Journalisation et événements système dans NSX

Mise à jour 5
Modifié le 16 novembre 2017
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

Journalisation et événements système dans NSX

Le document *Journalisation et événements système dans NSX* décrit les messages, événements et alarmes de journalisation dans le système VMware NSX® for vSphere® à l'aide de l'interface utilisateur NSX Manager et de vSphere Web Client.

Public visé

Ce manuel est destiné à toute personne souhaitant utiliser NSX ou résoudre un problème lié à ce système 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.

Événements système, alarmes et journaux

1

Vous pouvez utiliser les événements système, alarmes et journaux pour surveiller la santé et la sécurité de l'environnement NSX et résoudre les problèmes.

Ce chapitre contient les rubriques suivantes :

Événements système

Les événements système sont des enregistrements des actions du système. Chaque événement a un niveau de gravité, par exemple, informatif ou critique, qui indique la gravité de l'événement. Les événements système sont également émis sous forme d'interruptions SNMP, de sorte que tout logiciel de gestion SNMP peut surveiller les événements système NSX.

Afficher le rapport d'événements système

À partir de vSphere Web Client, vous pouvez afficher les événements système pour tous les composants gérés par NSX Manager.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Networking & Security**, puis, sous **Inventaire de mise en réseau et de sécurité**, cliquez sur **Instances de NSX Manager**.
3. Cliquez sur un dispositif NSX Manager dans la colonne **Nom**, puis cliquez sur l'onglet **Surveiller**.
4. Cliquez sur l'onglet **Événements système**.

   Vous pouvez cliquer sur les flèches dans les en-têtes de colonne pour trier les événements ou utiliser la zone de texte **Filtrer** pour filtrer les événements.

Format d'un événement système

Si vous spécifiez un serveur syslog, NSX Manager envoie l'ensemble des événements système au serveur syslog.

Ces messages ont un format similaire au message affiché ci-dessous :

```
Jan 8 04:35:00 NSXMGR 2017-01-08 04:35:00.422 GMT+00:00
INFO TaskFrameworkExecutor-18 SystemEventDaoImpl:133 -
[SystemEvent] Time:'Tue Nov 08 04:35:00.410 GMT+00:00 2016',
Severity:'High', Event Source:'Security Fabric', Code:'250024',
Event Message:'The backing EAM agency for this deployment could not be found.
It is possible that the VC services may still be initializing.
Please try to resolve the alarm to check existence of the agency.
In case you have deleted the agency manually, please delete the deployment
 entry from NSX.', Module:'Security Fabric', Universal Object:'false
```

L'événement système contient les informations suivantes.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Event Message: Text containing detailed information about the event.
Module: Event component. May be the same as event source.
Universal Object: Value displayed is True or False.
```

Alarmes

Les alarmes sont des notifications activées en réponse à un événement, un groupe de conditions ou l'état d'un objet. Les alarmes, ainsi que d'autres alertes, sont affichées sur le tableau de bord de NSX et d'autres écrans de l'interface utilisateur de vSphere Web Client.

Vous pouvez utiliser l'API `GET api/2.0/services/systemalarms` pour consulter les alarmes sur les objets NSX.

NSX prend en charge deux méthodes de gestion d'alarme :

- L'alarme correspond à un système et est associée à un résolveur qui tentera de résoudre le problème à l'origine de l'alarme. Cette approche est conçue pour le déploiement d'infrastructure réseau et de sécurité (par exemple, service EAM, bus de messages, plug-in de déploiement) ; elle est également prise en charge par Service Composer. Ces alarmes utilisent le code d'événement en tant que code d'alarme. Pour plus d'informations, reportez-vous au document *Journalisation et événements système dans NSX*.

- Les alarmes de notification Edge sont structurées sous la forme d'une paire d'alarmes de déclenchement et de résolution. Cette méthode est prise en charge par plusieurs fonctions Edge, notamment le réseau virtuel IPSec, l'équilibrage de charge, la haute disponibilité, la vérification de l'intégrité, le système de fichiers Edge et la réservation de ressources. Ces alarmes utilisent un code d'alarme unique qui se distingue du code d'événement. Pour plus d'informations, reportez-vous au document *Journalisation et événements système dans NSX*.

En général, une alarme est supprimée automatiquement par le système lorsque la condition d'erreur est corrigée. Certaines alarmes ne sont pas effacées automatiquement à l'occasion d'une mise à jour de la configuration. Une fois le problème résolu, vous devez désactiver les alarmes manuellement.

Voici l'exemple de l'API que vous pouvez utiliser pour effacer les alarmes.

Vous pouvez obtenir les alarmes d'une source spécifique, par exemple, un cluster, un hôte, un pool de ressources, un groupe de sécurité ou NSX Edge. Afficher les alarmes d'une source par *ID source* :

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}
```

Résoudre toutes les alarmes d'une source par *ID source* :

```
POST https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}?action=resolve
```

Vous pouvez afficher les alarmes NSX, notamment les alarmes du bus de messages, du plug-in de déploiement, de Service Composer et les alarmes Edge :

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms
```

Vous pouvez afficher une alarme NSX spécifique par *ID d'alarme* :

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
```

Vous pouvez résoudre une alarme NSX spécifique par *ID d'alarme* :

```
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

Pour plus d'informations sur l'API, consultez le *Guide de NSX API*.

Format d'une alarme

Vous pouvez afficher le format d'une alarme via l'API.

Le format d'une alarme contient les informations suivantes.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
```

```
Message: Text containing detailed information about the event.
Alarm ID: ID of an alarm.
Alarm Code: Event code which uniquely identifies the system alarm.
Alarm Source: Source where you should look to resolve the reported event.
```

Alarmes Guest Introspection

Les alarmes signalent à l'administrateur du serveur vCenter Server des événements d'introspection de Guest Introspection exigeant son attention. Les alarmes sont annulées automatiquement si l'état d'alarme n'existe plus.

Les alarmes de vCenter Server peuvent être affichées sans plug-in vSphere. Reportez-vous au *Guide d'administration du serveur vCenter Server* pour les événements et alarmes.

En plus de s'inscrire en tant qu'extension du serveur vCenter Server, NSX Manager définit les règles qui créent et suppriment les alarmes, à partir des événements provenant des trois composants de Guest Introspection : SVM, module Guest Introspection et agent léger. Les règles peuvent être personnalisées. Pour savoir comment créer des règles personnalisées pour les alarmes, voir la documentation de vCenter Server. Dans certains cas, les alarmes peuvent avoir des causes multiples. Les tableaux ci-dessous donnent la liste des causes possibles avec des actions correspondantes pouvant être entreprises pour y remédier.

Alarmes d'hôte

Les alarmes d'hôte sont générées par des événements concernant l'état de bon fonctionnement du module Guest Introspection.

Tableau 1-1. Erreurs (repérées en rouge)

Cause possible	Action
Le module Guest Introspection a été installé sur l'hôte, mais il ne signale plus d'état à NSX Manager.	1 Assurez-vous que Guest Introspection est en cours d'exécution en vous connectant à l'hôte et en tapant la commande `/etc/init.d/vShield-Endpoint-Mux start`. 2 Assurez-vous que le réseau est correctement configuré de sorte que Guest Introspection puisse se connecter à NSX Manager. 3 Redémarrez NSX Manager.

Alarmes SVM

Les alarmes SVM sont générées par des événements qui affectent l'intégrité des SVM.

Tableau 1-2. Alarmes SVM rouges

Problème	Action
Il existe une discordance de version de protocole avec le module Guest Introspection	Vérifiez que le module Guest Introspection et la SVM utilisent des protocoles mutuellement compatibles.
Guest Introspection n'a pas pu établir une connexion à la SVM	Vérifiez que la SVM est sous tension et que le réseau est configuré correctement.
La SVM ne communique pas son état, même si les clients sont connectés.	Erreur interne. Contactez le représentant du support technique de VMware.

Définition du niveau de journalisation des composants de NSX

Vous pouvez définir le niveau de journalisation de chaque composant de NSX.

Les niveaux pris en charge varient selon le composant, comme indiqué ici.

```
nsxmgr> set
  hardware-gateway  Show Logical Switch Commands
  PACKAGE-NAME      Set log level
  controller        Show Logical Switch Commands
  host              Show Logical Switch Commands

nsxmgr> set hardware-gateway agent 10.1.1.1 logging-level
  ERROR
  WARN
  INFO
  DEBUG
  TRACE

nsxmgr-01a> set <package-name> logging-level
  OFF
  FATAL
  ERROR
  WARN
  INFO
  DEBUG
  TRACE

nsxmgr> set controller 192.168.110.31
  java-domain    Set controller node log level
  native-domain  Set controller node log level

nsxmgr> set controller 192.168.110.31 java-domain logging-level
  OFF
  FATAL
  ERROR
  WARN
  INFO
  DEBUG
  TRACE
```

```
nsxmgr> set controller 192.168.110.31 native-domain logging-level
  ERROR
  WARN
  INFO
  DEBUG
  TRACE

nsxmgr> set host host-28
  netcpa  Set host node log level by module
  vdl2    Set host node log level by module
  vdr     Set host node log level by module

nsxmgr> set host host-28 netcpa logging-level
  FATAL
  ERROR
  WARN
  INFO
  DEBUG

nsxmgr> set host host-28 vdl2 logging-level
  ERROR
  INFO
  DEBUG
  TRACE

nsxmgr> set host host-28 vdr logging-level
  OFF
  ERROR
  INFO
```

Activer la journalisation pour VPN IPSec

Vous pouvez activer la journalisation de l'ensemble du trafic VPN IPSec.

Par défaut, la journalisation est activée et est définie sur le niveau AVERTISSEMENT.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Mise en réseau et sécurité (Networking & Security)**, puis sur **Dispositifs NSX Edge (NSX Edges)**.
3. Double-cliquez sur une instance de NSX Edge.
4. Cliquez sur l'onglet **Gérer (Manage)**, puis sur l'onglet **VPN**.
5. Cliquez sur **VPN IPSec (IPSec VPN)**.
6. Cliquez sur ▶ en regard de **Stratégie de journalisation (Logging Policy)**, puis sur **Activer la journalisation (Enable logging)** pour journaliser le trafic entre le sous-réseau local et le sous-réseau homologue et sélectionnez le niveau de journalisation.
7. Sélectionnez le niveau de journal et cliquez sur **Publier les modifications (Publish Changes)**.

Journaux VPN-Plus SSL

Les journaux de la passerelle VPN-Plus SSL sont envoyés au serveur syslog configuré sur le dispositif NSX Edge. Les journaux client VPN-Plus SSL sont stockés dans le répertoire suivant sur l'ordinateur de l'utilisateur distant : `%PROGRAMFILES%/VMWARE/SSL VPN Client/`.

Modifier les journaux du client VPN-Plus SSL et le niveau de journal

1 Dans l'onglet **VPN-Plus SSL (SSL VPN-Plus)**, cliquez sur **Paramètres du serveur (Server Settings)** dans le panneau de gauche.

2 Accédez à la section Stratégie de journalisation et développez la section pour afficher les paramètres actuels.

3 Cliquez sur **Modifier (Change)**.

4 Cochez la case **Activer la journalisation (Enable logging)** pour activer la journalisation.

OU

Décochez la case **Activer la journalisation (Enable logging)** pour désactiver la journalisation.

5 Sélectionnez le niveau de journal requis.

Note Les journaux du client VPN-Plus SSL sont activés par défaut et le niveau de journal est défini sur REMARQUE.

6 Cliquez sur **OK**.

journaux d'audit

Les journaux d'audit enregistrent toutes les actions des utilisateurs qui se connectent à NSX Manager.

Afficher le journal d'audit

L'onglet **Journaux d'audit** fournit une vue des actions effectuées par tous les utilisateurs de NSX Manager. NSX Manager conserve jusqu'à 100 000 journaux d'audit.

Procédure

1 Connectez-vous à vSphere Web Client.

2 Cliquez sur **Networking & Security**, puis, sous **Inventaire de mise en réseau et de sécurité**, cliquez sur **Instances de NSX Manager**.

3 Dans la colonne **Nom**, cliquez sur un serveur NSX puis sur l'onglet **Surveiller**.

4 Cliquez sur l'onglet **Journaux d'audit**.

5 Lorsque les détails sont disponibles pour un journal d'audit, le texte dans la colonne **Opération** pour ce journal est cliquable. Pour afficher les détails d'un journal d'audit, cliquez sur le texte dans la colonne **Opération**.

6 Dans les **Détails des modifications du journal d'audit**, sélectionnez **Rangées modifiées** pour afficher uniquement les propriétés dont les valeurs ont changé pour cette opération du journal d'audit.

Configuration d'un serveur Syslog

Un serveur Syslog peut être configuré pour servir de référentiel des journaux des composants NSX et des hôtes.

Configurer un serveur Syslog pour NSX Manager

Si vous spécifiez un serveur Syslog, NSX Manager envoie l'ensemble de ses journaux d'audit et événements système au serveur Syslog.

Les données syslog sont particulièrement utiles pour la résolution des problèmes et la révision des données journalisées pendant l'installation et la configuration.

NSX Edge prend en charge deux serveurs Syslog. NSX Manager et NSX Controller prennent en charge un serveur Syslog.

Procédure

1 Connectez-vous au dispositif virtuel NSX Manager.

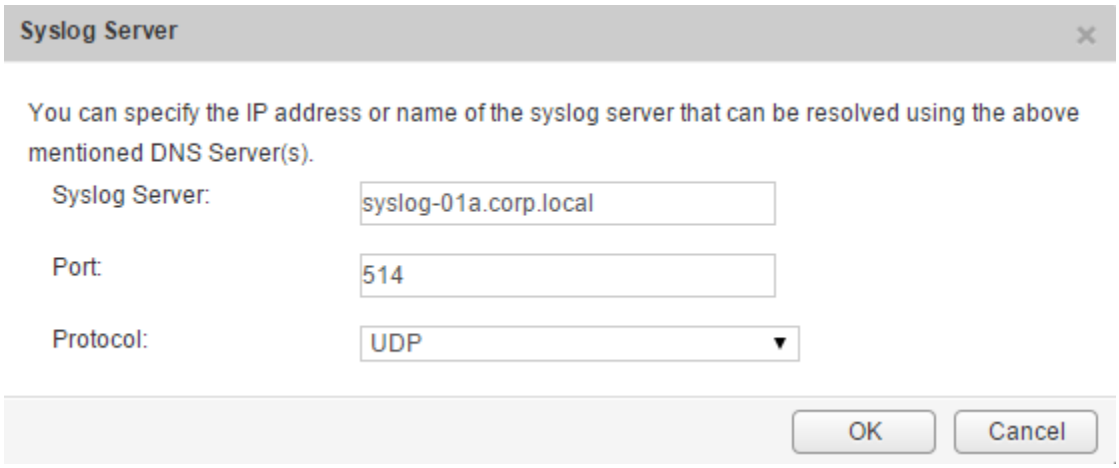
Dans un navigateur Web, accédez à l'interface utilisateur graphique du dispositif NSX Manager à l'adresse https://<nsx-manager-ip> ou https://<nsx-manager-hostname> et connectez-vous en tant qu'administrateur avec le mot de passe que vous avez configuré pendant l'installation de NSX Manager.

2 Dans la page d'accueil, cliquez sur **Gérer les paramètres des dispositifs (Manage Appliance Settings) > Général (General)**.

3 Cliquez sur **Modifier (Edit)** en regard de **Serveur syslog (Syslog Server)**.

4 Tapez l'adresse IP ou le nom d'hôte, le port et le protocole du serveur syslog.

Par exemple :



5 Cliquez sur **OK**.

La journalisation à distance de NSX Manager est activée et les fichiers journaux sont stockés dans votre serveur Syslog autonome.

Configurer les serveurs Syslog pour NSX Edge

Vous pouvez configurer un ou deux serveurs syslog distants. Les événements et les journaux NSX Edge associés aux événements du pare-feu qui circulent à partir des dispositifs NSX Edge sont envoyés aux serveurs syslog.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Mise en réseau et sécurité (Networking & Security)**, puis sur **Dispositifs NSX Edge (NSX Edges)**.
3. Double-cliquez sur un dispositif NSX Edge.
4. Cliquez sur l'onglet **Gérer**, puis sur l'onglet **Paramètres**.
5. Dans le panneau **Détails**, cliquez sur **Modifier** en regard des serveurs Syslog.
6. Entrez l'adresse IP de deux serveurs syslog distants et sélectionnez le protocole.
7. Cliquez sur **OK** pour enregistrer la configuration.

Configuration d'un serveur Syslog pour NSX Controller

Si vous configurez un serveur Syslog pour des contrôleurs NSX, NSX Manager envoie l'ensemble de ses journaux d'audit et événements système au serveur Syslog. Les données Syslog sont particulièrement utiles pour la résolution des problèmes et la révision des données journalisées pendant l'installation et la configuration. La seule méthode prise en charge pour la configuration du serveur Syslog sur les contrôleurs NSX implique NSX API. VMware recommande l'utilisation d'UDP comme protocole pour Syslog.

Procédure

1. Pour activer Syslog sur NSX Controller, utilisez la NSX API suivante. Celle-ci ajoute le programme d'exportation Syslog du contrôleur et configure un programme d'exportation Syslog sur le nœud du contrôleur spécifié.

```
Request
POST https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Request Body:
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

2 Vous pouvez interroger le programme d'exportation Syslog du contrôleur et récupérer les détails concernant le programme d'exportation Syslog configuré sur le nœud du contrôleur spécifié à l'aide de la NSX API suivante.

```
Request
GET https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Response Body:
<?xml version="1.0" encoding="UTF-8"?>
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

3 Si le programme d'exportation Syslog du contrôleur n'est pas nécessaire, vous pouvez le supprimer sur le nœud du contrôleur spécifié à l'aide de la NSX API suivante.

```
Request
DELETE https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
```

Étape suivante

Pour plus d'informations sur l'API, consultez *Guide de NSX API*.

Collecte des journaux de support technique

Dans certaines circonstances, vous pouvez avoir besoin de collecter les journaux de support technique des composants NSX et des hôtes pour signaler un problème à VMware.

Pour collecter les journaux de support technique des hôtes, exécutez la commande `export host-tech-support` (reportez-vous à la section « Dépannage du pare-feu distribué » du *Guide de dépannage de NSX*).

Télécharger les journaux de support technique pour NSX

Vous pouvez télécharger sur votre bureau les journaux système de NSX Manager et les journaux de Web Manager.

Procédure

1 Connectez-vous au dispositif virtuel NSX Manager.

2 Sous Gestion des dispositifs, cliquez sur **Gérer les paramètres des dispositifs**.

3 Cliquez sur  , puis sur **Télécharger les journaux de support technique**.

4 Cliquez sur **Télécharger**.

5 Lorsque le journal est prêt, cliquez sur **Enregistrer** pour télécharger le journal sur votre bureau.

Le journal est compressé et il porte l'extension de fichier `.gz`.

Étape suivante

Vous pouvez ouvrir le journal à l'aide d'un utilitaire de décompression en recherchant **Tous les fichiers** dans le répertoire où vous avez enregistré le fichier.

Télécharger les journaux du support technique de NSX Edge

Vous pouvez télécharger les journaux du support technique pour chaque instance NSX Edge. Si la haute disponibilité est activée pour l'instance NSX Edge, les journaux du support des deux machines virtuelles NSX Edge sont téléchargés.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Mise en réseau et sécurité (Networking & Security)**, puis sur **Dispositifs NSX Edge (NSX Edges)**.
3. Sélectionnez une instance de NSX Edge.
4. Cliquez sur **Actions** ( ) et sélectionnez **Télécharger les journaux de support technique**.
5. Après avoir généré les journaux du support technique, cliquez sur **Télécharger**.

Télécharger les journaux de support technique pour NSX Controller

Vous pouvez télécharger les journaux du support technique pour chaque instance NSX Controller. Ces journaux spécifiques au produit contiennent des informations de diagnostic pour l'analyse.

Pour collecter des journaux NSX Controller :

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Networking & Security**, puis sur **Installation**.
3. Sous **Gestion**, sélectionnez le contrôleur à partir duquel vous voulez télécharger des journaux.
4. Cliquez sur **Télécharger les journaux de support technique**.
5. Cliquez sur **Télécharger**.

   NSX Manager commence à télécharger le journal NSX Controller et acquiert le verrouillage.

   Note Téléchargez un journal NSX Controller à la fois. Une fois le premier terminé, lancez le téléchargement de l'autre. Une erreur peut se produire si vous téléchargez des journaux à partir de plusieurs contrôleurs simultanément.

6. Lorsque le journal est prêt, cliquez sur **Enregistrer** pour télécharger le journal sur votre bureau.

   Le journal est compressé et comporte l'extension de fichier `.gz`.

Vous pouvez maintenant analyser les journaux téléchargés.

Étape suivante

Pour télécharger des informations de diagnostic pour le support technique VMware, consultez l'article de la base de connaissances 2070100.

Journaux de NSX et des hôtes 2

Vous pouvez utiliser les journaux des différents composants de NSX et des hôtes pour détecter et résoudre les problèmes.

Ce chapitre contient les rubriques suivantes :

À propos des journaux NSX

Vous pouvez configurer le serveur Syslog et afficher les journaux de support technique de chaque composant NSX. Les journaux du plan de gestion sont disponibles dans NSX Manager et les journaux du plan de données sont disponibles dans vCenter Server. C'est pourquoi nous vous recommandons de spécifier le même serveur Syslog pour le composant NSX et pour vCenter Server, afin d'obtenir une image complète lorsque vous affichez des journaux sur le serveur Syslog.

Pour plus d'informations sur la configuration d'un serveur Syslog pour les hôtes gérés par un vCenter Server, consultez la version appropriée de la documentation de vSphere à l'adresse https://docs.vmware.com.

Note Les serveurs Syslog ou de saut utilisés pour collecter des journaux et accéder à une VM de contrôle du DLR (routeur logique distribué) NSX ne peuvent pas se trouver sur le même commutateur logique qui est directement lié aux interfaces logiques de ce DLR.

Tableau 2-1. Journaux de NSX

Composant	Description
Journaux d'ESXi	Ces journaux sont collectés dans le cadre du bundle de support de VM généré depuis vCenter Server. Pour plus d'informations sur les fichiers journaux d'ESXi, consultez la documentation de vSphere.
Journaux de NSX Edge	Utilisez la commande `show log [follow | reverse]` dans l'interface de ligne de commande de NSX Edge. Téléchargez le bundle de journaux de support technique via l'interface utilisateur de NSX Edge.
Journaux de NSX Manager	Utilisez la commande de l'interface de ligne de commande `show log` dans l'interface de ligne de commande de NSX Manager. Téléchargez le bundle de journaux de support technique via l'interface utilisateur du dispositif virtuel NSX Manager.
Journaux de routage	Consultez le guide *Journalisation et événements système dans NSX*.
Journaux de pare-feu	Reportez-vous à la section Journaux de pare-feu.
Journaux de Guest Introspection	Reportez-vous à la section Journaux de Guest Introspection.

NSX Manager

Pour spécifier un serveur Syslog, reportez-vous à la section Configurer un serveur Syslog pour NSX Manager.

Pour télécharger les journaux de support technique, reportez-vous à la section Télécharger les journaux de support technique pour NSX

NSX Edge

Pour spécifier un serveur Syslog, reportez-vous à la section Configurer les serveurs Syslog pour NSX Edge.

Pour télécharger les journaux de support technique, reportez-vous à la section Télécharger les journaux du support technique de NSX Edge

NSX Controller

Pour spécifier un serveur Syslog, reportez-vous à la section Configuration d'un serveur Syslog pour NSX Controller.

Pour télécharger les journaux de support technique, reportez-vous à la section Télécharger les journaux de support technique pour NSX Controller

Pare-feu

Pour plus d'informations, consultez Journaux de pare-feu.

Journaux de pare-feu

Le pare-feu génère et conserve des fichiers journaux, tels que des journaux d'audit, des journaux de messages relatifs aux règles et des journaux des événements système. Vous devez configurer un serveur Syslog pour chaque cluster ayant activé le pare-feu. Le serveur Syslog est spécifié dans l'attribut `Syslog.global.logHost`.

Le pare-feu génère des journaux comme décrit dans le tableau suivant.

Tableau 2-2. Journaux de pare-feu

Type de journal	Description	Emplacement
Journaux de messages relatifs aux règles	Incluent toutes les décisions d'accès (comme le trafic autorisé ou refusé) pour chaque règle si la journalisation a été activée pour cette règle. Contient des journaux de paquet DFW pour les règles pour lesquelles la journalisation a été activée.	/var/log/dfwpktlogs.log
Journaux d'audit	Incluent les journaux d'administration et les modifications apportées à la configuration du pare-feu distribué.	/home/secureall/secureall/logs/vsm.log
Journaux des événements système	Incluent la configuration appliquée au pare-feu distribué, les filtres créés, supprimés ou en échec et les machines virtuelles ajoutées aux groupes de sécurité, etc.	/home/secureall/secureall/logs/vsm.log
Journaux de plan de données/VMKernel	Capturent les activités liées à un module de noyau de pare-feu (VSIP). Il inclut les entrées de journal pour les messages générés par le système.	/var/log/vmkernel.log
Journaux du client du bus de messages/VSFWD	Capturent les activités d'un agent de pare-feu.	/var/log/vsfwd.log

Note Le fichier *vsm.log* est accessible en exécutant la commande `show log manager` à partir de l'interface de ligne de commande de NSX Manager et en effectuant *grep* pour le mot-clé *vsm.log*. Seul l'utilisateur ou le groupe d'utilisateurs disposant du privilège *racine* peut accéder à ce fichier.

Journaux de messages relatifs aux règles

Les journaux de messages relatifs aux règles incluent toutes les décisions d'accès (comme le trafic autorisé et celui refusé) pour chaque règle si la journalisation a été activée pour cette règle. Ces journaux sont stockés sur chaque hôte dans `/var/log/dfwpktlogs.log`.

Voici des exemples de messages de journal de pare-feu :

```
 # more /var/log/dfwpktlogs.log
2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138->192.168.110.255/138
```

```
# more /var/log/dfwpktlogs.log
2017-04-11T21:09:59.877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST
10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070
```

Autres exemples :

```
2017-10-19T22:38:05.586Z 58734 INET match PASS domain-c8/1006 OUT 84 ICMP 172.18.8.121->172.18.8.119
RULE_TAG
2017-10-19T22:38:08.723Z 58734 INET match PASS domain-c8/1006 OUT 60 TCP 172.18.8.121/36485-
>172.18.8.119/22 S RULE_TAG
2017-10-19T22:38:18.785Z 58734 INET TERM domain-c8/1006 OUT ICMP 8 0 172.18.8.121->172.18.8.119 2/2
168/168 RULE_TAG
2017-10-19T22:38:20.789Z 58734 INET TERM domain-c8/1006 OUT TCP FIN 172.18.8.121/36484-
>172.18.8.119/22 44/33 4965/5009 RULE_TAG
```

Dans l'exemple suivant :

- 1002 correspond à l'ID de la règle du pare-feu distribué.
- domain-c7 correspond à l'ID du cluster dans le MOB (Managed Object Browser) de vCenter.
- 192.168.110.10/138 correspond à l'adresse IP source.
- 192.168.110.255/138 correspond à l'adresse IP de destination.
- *RULE_TAG* est un exemple du texte que vous ajoutez dans la zone de texte **Balise** lors de l'ajout ou de la modification de la règle de pare-feu.

L'exemple suivant présente le résultat d'un test ping entre 192.168.110.10 et 172.16.10.12.

```
 # tail -f /var/log/dfwpktlogs.log | grep 192.168.110.10

2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
```

Les tableaux suivants expliquent les zones de texte incluses dans le message de journal de pare-feu.

Tableau 2-3. Composants d'une entrée de fichier journal

Composant	Valeur de l'exemple
Horodatage	2017-04-11T21:09:59
Partie spécifique au pare-feu	877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST 10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070

Tableau 2-4. Partie spécifique au pare-feu de l'entrée de fichier journal

Entité	Valeurs possibles
Hachage de filtre	Numéro permettant d'obtenir le nom du filtre et d'autres informations.
Valeur AF	INET, INET6

Tableau 2-4. Partie spécifique au pare-feu de l'entrée de fichier journal (Suite)

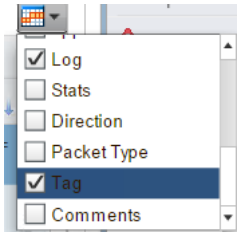
Entité	Valeurs possibles
Raison	■ match : le paquet correspond à une règle. ■ bad-offset : erreur interne de chemin de données lors de l'obtention du paquet. ■ fragment : fragments qui ne sont pas en premier après leur assemblage pour former le premier fragment. ■ short : paquet trop court (par exemple, pas encore terminé pour inclure un en-tête Adresse IP ou un en-tête TCP/UDP). ■ normalize : paquets mal formés sans en-tête correct ou sans section de configuration. ■ memory : mémoire insuffisante du chemin de données. ■ bad-timestamp : horodatage TCP incorrect. ■ proto-cksum : total de contrôle de protocole incorrect. ■ state-mismatch : paquets TCP qui ne transmettent pas la vérification de machine d'état TCP. ■ state-insert : une connexion en double est détectée. ■ state-limit : le nombre maximal d'états qu'un chemin de données peut suivre a été atteint. ■ SpoofGuard : paquets abandonnés par SpoofGuard. ■ TERM : une connexion est terminée.
Action	■ PASS : acceptez le paquet. ■ DROP : abandonnez le paquet. ■ NAT : règle SNAT. ■ NONAT : correspond à la règle SNAT, mais ne peut pas convertir l'adresse. ■ RDR : règle DNAT. ■ NORDR : correspond à la règle DNAT, mais ne peut pas convertir l'adresse. ■ PUNT : envoyez le paquet à une VM de service en cours d'exécution sur le même hyperviseur que la VM actuelle. ■ REDIRECT : envoyez le paquet au service réseau en cours d'exécution sur l'hyperviseur de la VM actuelle. ■ COPY : acceptez le paquet et faites une copie sur une VM de service en cours d'exécution sur le même hyperviseur que la VM actuelle. ■ REJECT : refusez le paquet.
Ensemble de règles et ID de règle	*rule set*/*rule ID*
Direction	IN, OUT
Longueur de paquet	*length*
Protocole	TCP, UDP, ICMP ou PROTO (numéro de protocole) Pour les connexions TCP, la raison réelle pour laquelle une connexion est terminée est indiquée après le mot-clé TCP. Si TERM est la raison d'une session TCP, une explication supplémentaire s'affiche sur la ligne PROTO. Les raisons possibles de l'arrêt d'une connexion TCP sont : RST (paquet TCP RST), FIN (paquet TCP FIN) et TIMEOUT (inactif depuis trop longtemps) Dans l'exemple ci-dessus, il s'agit de *RST*. Par conséquent, cela signifie qu'il existe un paquet *RST* dans la connexion qui doit être réinitialisée. Pour les connexions non-TCP (UDP, ICMP ou autres protocoles), la raison de l'arrêt d'une connexion est uniquement TIMEOUT.
Adresse IP et port sources	*IP address*/*port*

Tableau 2-4. Partie spécifique au pare-feu de l'entrée de fichier journal (Suite)

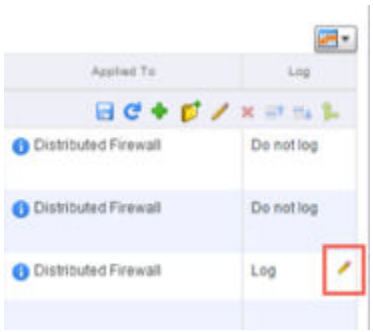
Entité	Valeurs possibles
Adresse IP et port de destination	*IP address/port*
Indicateurs TCP.	S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)
Nombre de paquets	Nombre de paquets. 22/14 : paquets entrants/paquets sortants
Nombre d'octets	Nombre d'octets. 7 684/1 070 : octets entrants/octets sortants

Pour activer un message relatif aux règles, connectez-vous à vSphere Web Client :

1 Activez la colonne **Journal** sur la page **Networking & Security > Pare-feu**.



2 Activez la journalisation pour une règle en passant votre souris au-dessus de la cellule correspondante dans le tableau de journalisation et en cliquant sur l'icône en forme de crayon.



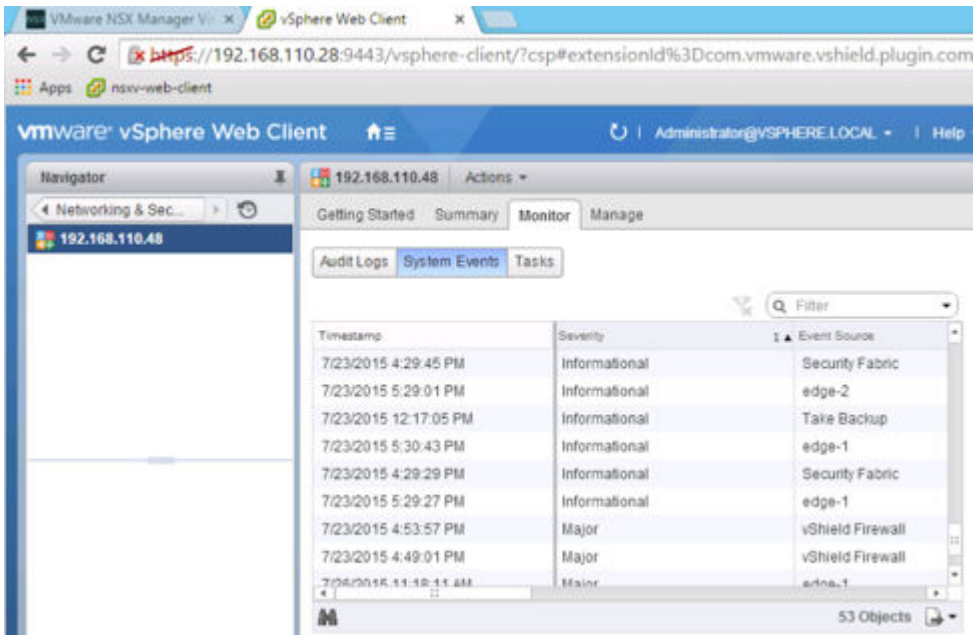
Note Si vous voulez que du texte personnalisé s'affiche dans le message de journal de pare-feu, vous pouvez activer la colonne **Balise** et ajouter le texte requis en cliquant sur l'icône de crayon.

Journaux d'audit et journaux des événements système

Les journaux d'audit incluent les journaux d'administration et les modifications apportées à la configuration du pare-feu distribué. Ils sont stockés dans `/home/secureall/secureall/logs/vsm.log`.

Les journaux des événements système incluent la configuration appliquée au pare-feu distribué, les filtres créés, supprimés ou en échec et les machines virtuelles ajoutées aux groupes de sécurité, etc. Ces journaux sont stockés dans `/home/secureall/secureall/logs/vsm.log`.

Pour consulter les journaux d'audit et les journaux des événements système dans l'interface utilisateur, accédez à **Mise en réseau et sécurité > Installation > Gestion**, puis double-cliquez sur l'adresse IP de l'instance de NSX Manager. Cliquez ensuite sur l'onglet **Surveiller**.



Pour plus d'informations, reportez-vous à la section *Journalisation et événements système dans NSX*.

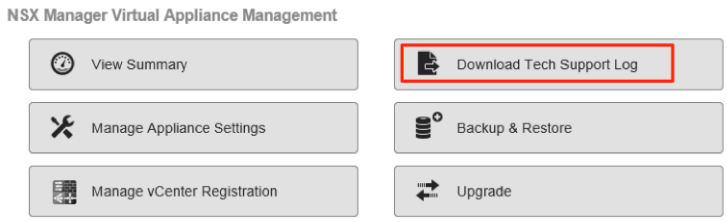
Journaux de NSX applicables au routage

Il est recommandé de configurer tous les composants de NSX pour qu'ils envoient leurs journaux à un collecteur centralisé, où ils peuvent être examinés dans un seul emplacement.

Si nécessaire, vous pouvez modifier le niveau de journal de composants NSX. Pour plus d'informations, reportez-vous à la section « Définition du niveau de journalisation des composants de NSX » dans *Journalisation et événements système dans NSX*.

Journaux de NSX Manager

- `show log` dans l'interface de ligne de commande de NSX Manager
- Bundle de journaux du support technique, collecté via l'interface utilisateur de NSX Manager



Le journal de NSX Manager contient des informations liées au plan de gestion, qui couvre les opérations Créer, Lire, Mettre à jour et Supprimer (CLMS).

Journaux du contrôleur

Les contrôleurs contiennent plusieurs modules, beaucoup disposant de leurs propres fichiers journaux. Les journaux de contrôleur sont accessibles à l'aide de la commande `show log <log file> [ filtered-by <string> ]`. Les fichiers journaux applicables au routage sont les suivants :

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log` : ce journal gère la configuration et le serveur API interne.
- `cloudnet/cloudnet.nsx-controller.log` : il s'agit du journal du processus principal du contrôleur.
- `cloudnet/cloudnet_cpp.log.nsx-controller.log` : ce journal gère le clustering et le démarrage.
- `cloudnet/cloudnet_cpp.log.ERROR` : ce fichier est présent si une erreur se produit.

Les journaux de contrôleur sont détaillés et, dans la plupart des cas, ils ne sont requis que lorsque les ingénieurs de VMware sont sollicités pour résoudre des cas plus difficiles.

En plus de l'interface de ligne de commande `show log`, des fichiers journaux individuels peuvent être consultés en temps réel lors de leur mise à jour, à l'aide de la commande `watch log <logfile> [ filtered-by <string> ]`.

Les journaux sont inclus dans le bundle de support du contrôleur qui peut être généré et téléchargé en sélectionnant un nœud de contrôleur dans l'interface utilisateur de NSX et en cliquant sur l'icône **Télécharger les journaux de support technique (Download tech support logs)**.

Journaux de l'hôte ESXi

Les composants de NSX exécutés sur les hôtes ESXi écrivent plusieurs fichiers journaux :

- Journaux VMkernel : `/var/log/vmkernel.log`
- Journaux de l'agent de plan de contrôle : `/var/log/netcpa.log`
- Journaux du client de bus de messages : `/var/log/vsfwd.log`

Les journaux peuvent également être collectés dans le cadre du bundle de support de VM généré depuis vCenter Server. Seuls les utilisateurs ou les groupes d'utilisateurs disposant du privilège *racine* peuvent accéder aux fichiers journaux.

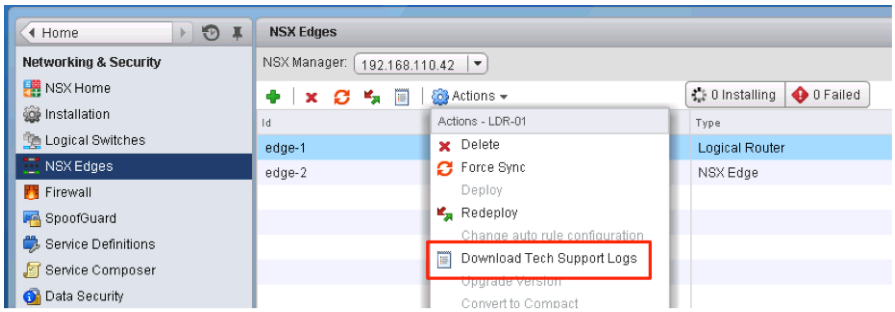
Journaux de la passerelle ESG/VM de contrôle du DLR

Il existe deux façons d'accéder aux fichiers journaux sur la passerelle ESG et les VM de contrôle du DLR : les afficher à l'aide d'une interface de ligne de commande ou télécharger le bundle de support technique à l'aide de l'interface de ligne de commande ou de l'interface utilisateur.

La commande CLI pour afficher les journaux est `show log [ follow | reverse ]`.

Pour télécharger le bundle de support technique :

- À partir de l'interface de ligne de commande, passez en mode `enable`, puis exécutez la commande `export tech-support <[ scp | ftp ]> <URI>`.
- À partir de vSphere Web Client, sélectionnez l'option **Télécharger les journaux de support technique (Download Tech Support Logs)** dans le menu **Actions**.



Autres fichiers utiles et leurs emplacements

Bien qu'il ne s'agisse pas purement de journaux, plusieurs fichiers peuvent être utiles pour comprendre et résoudre le routage NSX.

- La configuration de l'agent de plan de contrôle `/etc/vmware/netcpa/config-by-vsm.xml` contient les informations sur les composants suivants :
  - Adresses IP des contrôleurs, ports TCP, empreintes numériques de certificat, activer/désactiver SSL
  - dvUplinks sur le DVS activé avec VXLAN (stratégie d'association, noms, UUID)
  - Instances du DLR que l'hôte connaît (ID du DLR, nom)
- La configuration de l'agent de plan de contrôle `/etc/vmware/netcpa/netcpa.xml` contient diverses options de configuration pour netcpa, notamment le niveau de journalisation (qui par défaut est **info**).
- Fichiers de certificat du plan de contrôle : `/etc/vmware/ssl/rui-for-netcpa.*`
  - Deux fichiers : certificat de l'hôte et clé privée de l'hôte
  - Utilisés pour l'authentification des connexions d'hôte aux contrôleurs

Tous ces fichiers sont créés par l'agent du plan de contrôle à l'aide des informations qu'il reçoit de la part de NSX Manager via la connexion du bus de messages fournie par vsfwd.

Journaux de Guest Introspection

Il existe plusieurs journaux différents que vous pouvez capturer afin de les utiliser lors du dépannage de Guest Introspection.

Journaux de module ESX GI (MUX)

Si des machines virtuelles sur un hôte ESXi ne fonctionnent pas avec Guest Introspection, ou s'il existe des alarmes sur un hôte concernant la communication avec le SVA, il peut y avoir un problème avec le module ESX GI sur l'hôte ESXi.

Chemin du journal et exemple de message

Chemin du journal MUX
/var/log/syslog
var/run/syslog.log

Les messages du module ESX GI (MUX) suivent le format <timestamp>EPSecMUX<[ThreadID]>: <message>

Par exemple :

```
2017-07-16T05:44:49Z EPSecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

Dans l'exemple ci-dessus :

- [ERROR] est le type de message. Les autres types peuvent être [DEBUG], [INFO]
- (EPSEC) indique que les messages sont relatifs à Endpoint Security

Activation et affichage des fichiers journaux

Pour afficher la version du VIB du module ESX GI installé sur l'hôte, exécutez la commande `#esxcli software vib list | grep epsec-mux`.

Pour activer la journalisation complète, effectuez ces étapes sur le shell de commande d'hôte ESXi :

1 Exécutez la commande ps -c |grep Mux pour rechercher les processus du module ESX GI en cours d'exécution.

   Par exemple :

   ```
   ~ # ps -c | grep Mux
   192223 192223 sh  /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t
   1000000 /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
   192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
   192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
   ```

2 Si le service n'est pas en cours d'exécution, vous pouvez le redémarrer avec la commande `/etc/init.d/vShield-Endpoint-Mux start` ou `/etc//init.d/vShield-Endpoint-Mux restart`.

3 Pour arrêter les processus en cours d'exécution du module ESX GI, notamment le processus watchdog.sh, exécutez la commande ~ # kill –9 192223 192233 192236 .

   Notez que deux processus du module ESX GI sont générés.

4 Démarrez un module ESX GI avec une nouvelle option –d. Notez que l'option -d n'existe pas pour les builds epsec-mux 5.1.0-01255202 et 5.1.0-01814505 ~ # /usr/lib/vmware/vShield–Endpoint–Mux –d 900 –c 910

5 Affichez les messages de journaux du module ESX GI dans le fichier /var/log/syslog.log sur l'hôte ESXi. Vérifiez que les entrées correspondant aux solutions globales, à l'ID de solution et au numéro de port sont correctement spécifiés.

Exemple :Exemple de fichier muxconfig.xml

```
<?xml version="1.0" encoding="UTF–8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371–3630–47b0–8796–f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00–609186d9/EndpointService (216)/EndpointService
(216).vmx</vmxPath>

    </Solution>

    <Solution>

      <id>102</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48651</port>

      <uuid>423839c4–c7d6–e92e–b552–79870da05291</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00–609186d9/apoon/EndpointSVM–alpha–01/EndpointSVM–
alpha–01.vmx</vmxPath>

    </Solution>
```

```
    <Solution>
      <id>6341068275337723904</id>
      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>
      <listenOn>ip</listenOn>
      <port>48655</port>
      <uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>
      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>
    </Solution>
  </InstalledSolutions>
  <DefaultSolutions/>
  <GlobalSolutions>
    <solution>
      <id>100</id>
      <tag></tag>
      <order>0</order>
    </solution>
    <solution>
      <id>102</id>
      <tag></tag>
      <order>10000</order>
    </solution>
    <solution>
      <id>6341068275337723904</id>
      <tag></tag>
      <order>10001</order>
    </solution>
```

```
  </GlobalSolutions>

</EndpointConfig>
```

Journaux de l'agent léger GI

L'agent léger est installé sur le système d'exploitation invité de machine virtuelle et détecte les détails de l'ouverture de session utilisateur.

Chemin du journal et exemple de message

L'agent léger se compose de pilotes GI : vsepflt.sys, vnetflt.sys, vnetwfp.sys (Windows 10 et versions ultérieures).

Les journaux de l'agent léger se trouvent sur l'hôte ESXi, dans le cadre du bundle de journaux vCenter. Le chemin du journal est `/vmfs/volumes/<datastore>/<vmname>/vmware.log`. Par exemple : `/vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log`

Les messages de l'agent léger suivent le format <timestamp> <VM Name><Process Name><[PID]>: <message>.

Dans l'exemple de journal ci-dessous, `Guest: vnet or Guest:vsep` indique les messages de journal liés aux pilotes GI respectifs, suivis de messages de débogage.

Par exemple :

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
 vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

Exemple :Activation de la journalisation du pilote d'agent léger vShield Guest Introspection

Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Cette procédure vous oblige à modifier le Registre Windows. Avant de modifier le Registre, veillez à en faire une sauvegarde. Pour plus d'informations sur la sauvegarde et la restauration du Registre, consultez l'article 136393 de la base de connaissances de Microsoft.

Pour activer la journalisation de débogage pour le pilote d'agent léger :

1 Cliquez sur **Démarrer > Exécuter (Start > Run)**. Entrez regedit et cliquez sur **OK**. La fenêtre Éditeur du Registre s'ouvre. Pour plus d'informations, consultez l'article 256986 de la base de connaissances de Microsoft.

2 Créez cette clé à l'aide de l'éditeur du Registre : `HKEY_LOCAL_Machine\SYSTEM\CurrentControlSet\services\vsepflt\parameters`.

3 Sous la clé de paramètre qui vient d'être créée, créez ces valeurs de type DWORD. Assurez-vous que hexadécimal est sélectionné lorsque vous entrez ces valeurs :

```
Name: log_dest
Type: DWORD
Value: 0x2

Name: log_level
Type: DWORD
Value: 0x10
```

Autres valeurs pour la clé de paramètre `log level` :

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

4 Ouvrez une invite de commande en tant qu'administrateur. Exécutez ces commandes pour décharger et recharger le mini-pilote du système de fichiers vShield Endpoint :

- `fltmc unload vsepflt`
- `fltmc load vsepflt`

Les entrées de journal se trouvent dans le fichier vmware.log situé dans la machine virtuelle.

Activation de la journalisation du pilote d'introspection réseau vShield GI

Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Cette procédure vous oblige à modifier le Registre Windows. Avant de modifier le Registre, veillez à en faire une sauvegarde. Pour plus d'informations sur la sauvegarde et la restauration du Registre, consultez l'article 136393 de la base de connaissances de Microsoft.

1 Cliquez sur **Démarrer > Exécuter (Start > Run)**. Entrez regedit et cliquez sur **OK**. La fenêtre Éditeur du Registre s'ouvre. Pour plus d'informations, consultez l'article 256986 de la base de connaissances de Microsoft.

2 Modifiez le Registre :

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest"  = DWORD: 0x00000001
```

3 Redémarrez la machine virtuelle.

Emplacement des fichiers journaux vsepflt.sys et vnetflt.sys

Avec les paramètres de Registre log_dest DWORD:0x00000001, le pilote de l'agent léger de point de terminaison se connecte au débogueur. Exécutez le débogueur (DbgView depuis SysInternals ou windbg) pour capturer la sortie de débogage.

Vous pouvez également définir le paramètre de Registre log_dest sur DWORD:0x000000002. Dans ce cas, les journaux de pilote seront imprimés dans le fichier vmware.log, qui se trouve dans le dossier de machine virtuelle correspondant sur l'hôte ESXi.

Activation de la journalisation d'UMC

Le composant en mode utilisateur (UMC) Guest Introspection s'exécute dans le service VMware Tools sur la machine virtuelle protégée.

1 Sous Windows XP et Windows Server 2003, créez un fichier `tools config`, s'il n'existe pas dans le chemin suivant :`C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf`.

2 Sous Windows Vista, Windows 7 et Windows Server 2008, créez un fichier `tools config`, s'il n'existe pas dans le chemin suivant : `C:\ProgramData\VMWare\VMware Tools\tools.conf`

3 Ajoutez ces lignes dans le fichier `tools.conf` pour activer la journalisation de composant UMC.

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

Avec le paramètre `vsep.handler = vmx` , le composant UMC se connecte au fichier `vmware.log` , qui se trouve dans le dossier de machine virtuelle correspondant sur l'hôte ESXi.

Avec les journaux de paramètre suivants, les journaux de composant UMC sont imprimés dans le fichier journal spécifié.

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

Journaux EPSecLib et SVM GI

EPSecLib reçoit des événements du module ESX GI (MUX) de l'hôte ESXi.

Chemin du journal et exemple de message

Chemin du journal EPSecLib
/var/log/syslog
var/run/syslog

Les messages EPSecLib suivent le format <timestamp> <VM Name><Process Name><[PID]>: <message>

Dans l'exemple ci-dessous, [ERROR] est le type de message et (EPSEC) indique que les messages sont relatifs à Guest Introspection.

Par exemple :

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
 [7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

Collecte des journaux

Pour activer la journalisation de débogage de la bibliothèque EPSec, qui est un composant de la SVM GI :

1 Connectez-vous à la SVM GI en obtenant le mot de passe de console auprès de NSX Manager.

2 Créez le fichier `/etc/epseclib.conf` et ajoutez :

`ENABLE_DEBUG=TRUE`

`ENABLE_SUPPORT=TRUE`

3 Modifiez les autorisations en exécutant la commande `chmod 644 /etc/epseclib.conf`.

4 Redémarrez le processus GI-SVM en exécutant la commande `/usr/local/sbin/rcusvm restart`.

   Cela active la journalisation de débogage pour EPSecLib sur la SVM GI et les journaux de débogage sont disponibles dans les messages /var/log/messages applicables à NSX for vSphere 6.2.x et 6.3.x. Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Journaux de SVM GI

Avant de capturer les journaux, déterminez l'ID de l'hôte ou le MOID de l'hôte :

- Exécutez les commandes `show cluster all` et `show cluster <cluster ID>` dans NSX Manager.

  Par exemple :

```
nsxmgr-01a> show cluster all

No.  Cluster Name       Cluster Id              Datacenter Name   Firewall Status
1    RegionA01-COMP01   domain-c26              RegionA01         Enabled
2    RegionA01-MGMT01   domain-c71              RegionA01         Enabled

nsxmgr-01a> show cluster  domain-c26

Datacenter: RegionA01
Cluster: RegionA01-COMP01
No.  Host Name            Host Id                 Installation Status
1    esx-01a.corp.local   host-29                 Ready
2    esx-02a.corp.local   host-31                 Ready
```

1 Pour déterminer l'état actuel de journalisation, exécutez cette commande :

   `GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm`

   `GET https://nsxmanager/api/1.0/usvmlogging/host-##/root`

2 Pour modifier l'état actuel de journalisation, exécutez cette commande :

   `POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel`

```
## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

<?xml version="1.0" encoding="UTF-8" ?>
```

```
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>
```

3 Pour générer des journaux, exécutez cette commande :

`GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs`

Sélectionnez `Send` et `Download`.

Notez que cette commande génère des journaux de SVM GI et enregistre le fichier sous `techsupportlogs.log.gz`. Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Événements système 3

Tous les composants de NSX signalent des événements système. Ces événements permettent de surveiller la santé et la sécurité de l'environnement, et peuvent aider à résoudre les problèmes.

Chaque message d'événement contient les informations suivantes :

- Code d'événement unique
- Niveau de gravité
- Description de l'événement et, le cas échéant, des actions recommandées.

Collecte des journaux de support technique et contact de l'assistance VMware

Pour certains événements, il est recommandé de collecter les journaux de support technique et de contacter l'assistance VMware.

- Pour collecter les journaux de support technique de NSX Manager, reportez-vous à la section Télécharger les journaux de support technique pour NSX.
- Pour collecter les journaux de support technique de NSX Edge, reportez-vous à la section Télécharger les journaux du support technique de NSX Edge.
- Pour collecter les journaux de support technique des hôtes, exécutez la commande `export host-tech-support` (reportez-vous à la section « Dépannage de Pare-feu distribué » du *Guide de dépannage de NSX*).
- Pour contacter l'assistance VMware, reportez-vous à l'article indiquant comment soumettre une demande de support dans My VMware (http://kb.vmware.com/kb/2006985).

Exécution d'une synchronisation forcée sur NSX Edge

Pour certains événements, il peut être recommandé d'effectuer une synchronisation forcée sur NSX Edge. Pour plus d'informations, reportez-vous à la section « Forcer la synchronisation de NSX Edge avec NSX Manager » du *Guide d'administration de NSX*. Une synchronisation forcée est une opération perturbatrice qui entraîne le redémarrage de la machine virtuelle NSX Edge.

Niveau de gravité des événements système

Chaque événement est associé à l'un des niveaux de gravité suivants :

- Informatif
- Faible
- Moyenne
- Majeur
- Critique
- Élevé

Les rubriques suivantes répertorient les messages d'événement système dont le niveau de gravité est majeur, critique ou élevé, pour différents composants.

Ce chapitre contient les rubriques suivantes :

Événements système liés à la sécurité

Le tableau décrit les messages d'événement système liés à la sécurité dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
11002	Critique	Non	`Connexion impossible à vCenter Server. Nom d'utilisateur/mot de passe incorrect. (Unable to connect to vCenter Server. Bad username/password.)`	La configuration de vCenter Server a échoué. Action : vérifiez que la configuration de vCenter Server est correcte et que les informations d'identification correctes sont fournies. Reportez-vous à la section « Enregistrer vCenter Server dans NSX Manager » du *Guide d'administration de NSX* et à la section « Connexion de NSX Manager à vCenter Server » du *Guide de dépannage de NSX*.
11006	Critique	Non	`Perte de connectivité de vCenter Server. (Lost vCenter Server connectivity.)`	La connexion à vCenter Server a été perdue. Action : recherchez les problèmes de connectivité pouvant affecter vCenter Server. Reportez-vous aux sections « Connexion de NSX Manager à vCenter Server » et « Résolution des problèmes de NSX Manager » du *Guide de dépannage de NSX*.
230000	Critique	Non	`Échec de la tâche de configuration SSO sur NSX Manager. (SSO Configuration Task on NSX Manager failed.)`	La configuration de Single Sign On (SSO) a échoué. Le problème peut être lié à des informations d'identification non valides, une configuration non valide ou à l'expiration de la synchronisation. Action : examinez le message d'erreur et reconfigurez SSO. Reportez-vous à la section « Configurer Single Sign-On » du *Guide d'administration de NSX*. De plus, reportez-vous à la section « Échec de la configuration de NSX SSO Lookup Service » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
230002	Critique	Non	`Client SSO STS déconnecté. (SSO STS Client disconnected.)`	L'enregistrement de NSX Manager pour le service SSO a échoué ou la connectivité avec le service SSO a été perdue. Action : vérifiez qu'il n'y a pas de problèmes de configuration, tels que des informations d'identification non valides, des problèmes de synchronisation ou des problèmes de connectivité réseau. Cet événement peut également se produire en raison de problèmes techniques VMware spécifiques. Reportez-vous à l'article de la base de connaissances traitant du problème de vérification du certificat SSL sur le service STS (http://kb.vmware.com/kb/2121696) et à l'article relatif à l'échec de l'enregistrement de NSX Manager sur le service de recherche avec le contrôleur PSC (External Platform Service Controller), avec génération d'un message d'erreur indiquant que la chaîne de certificats du serveur n'a pas été vérifiée (http://kb.vmware.com/kb/2132645).
240000	Critique	Non	`Une entrée {0} a été ajoutée à la liste noire d'authentification. (Added an entry {0} to authentication black list.)`	Un utilisateur avec une adresse IP spécifique n'a pas pu se connecter 10 fois de suite et est bloqué pendant 30 minutes. Action : recherchez un éventuel problème de sécurité.

Événements système de Pare-feu distribué

Le tableau décrit les messages d'événement système de Pare-feu distribué dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301001	Critique	Non	`Échec de la mise à jour de la configuration sur l'hôte. (Filter config update failed on host.)`	L'hôte n'a pas pu recevoir/analyser la configuration du filtre ni ouvrir le périphérique */dev/dvfiltertbl* . Action : consultez la pair clé-valeur pour obtenir le contexte et la raison de l'échec. Le problème peut provenir d'une non-correspondance de versions VIB entre NSX Manager et les hôtes préparés, ou de problèmes de mise à niveau inattendus. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301002	Majeur	Non	`La configuration de filtre n'est pas appliquée à la vNIC. (Filter config not applied to vnic.)`	La configuration de filtre n'a pas pu être appliquée à la vNIC. Cause possible : échec de l'ouverture, de l'analyse ou de la mise à jour de la configuration de filtre. Cette erreur ne devrait pas se produire avec le pare-feu distribué, mais peut se produire dans des scénarios d'extensibilité du réseau (NetX). Action : collectez des bundles de support technique pour ESXi et NSX Manager, puis contactez le support technique VMware.
301031	Critique	Non	`Échec de la mise à jour de la configuration de pare-feu sur l'hôte. (Firewall config update failed on host.)`	Échec de la réception/analyse/mise à jour de la configuration de pare-feu. La valeur de clé comportera des informations sur le contexte, telles que le numéro de génération et d'autres informations de débogage. Action : vérifiez que la procédure de préparation de l'hôte a bien été suivie. Connectez-vous à l'hôte et collectez le fichier `/var/log/vsfwd.log`, puis forcez la synchronisation de la configuration du pare-feu avec l'API `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` (reportez-vous à la section « Dépannage de Pare-feu distribué » du *Guide de dépannage de NSX*). Si la mise à jour de la configuration du pare-feu distribué échoue toujours sur l'hôte, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez l'assistance technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301032	Majeur	Non	Échec de l'application de la règle de pare-feu à la vNIC. (Failed to apply firewall rule to vnic.)	Échec de l'application des règles de pare-feu à la vNIC. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware. Assurez-vous que les journaux des hôtes (*vmkernel.log* et *vsfwd.log*) incluent la période pendant laquelle la configuration de pare-feu a été appliquée à la vNIC.
301041	Critique	Non	Échec de la mise à jour de la configuration du conteneur sur l'hôte. (Container configuration update failed on host.)	Une opération liée la configuration du conteneur réseau et sécurité a échoué. La valeur de clé comportera des informations sur le contexte, telles que le nom du conteneur et le numéro de génération. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware. Assurez-vous que les journaux des hôtes (*vmkernel.log* et *vsfwd.log*) incluent la période pendant laquelle la configuration de conteneur a été appliquée à la vNIC.
301051	Majeur	Non	Le flux est absent de l'hôte. (Flow missed on host.)	Les données de flux d'une ou plusieurs sessions en provenance et à destination de machines virtuelles protégées ont été abandonnées ; leur lecture ou leur envoi à NSX Manager a échoué. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre et que la consommation de mémoire vsfwd se situe dans les limites des ressources (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301061	Critique	Non	`Échec de la mise à jour de la configuration de Spoofguard sur l'hôte. (Spoofguard config update failed on host.)`	Une opération de configuration liée à Spoofguard a échoué. Action : vérifiez que la procédure de préparation de l'hôte a bien été suivie. Connectez-vous à l'hôte et collectez le fichier `/var/log/vsfwd.log`, puis forcez la synchronisation de la configuration du pare-feu avec l'API `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` (reportez-vous à la section « Dépannage de Pare-feu distribué » du *Guide de dépannage de NSX*). Si la configuration de SpoofGuard échoue toujours, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware. Assurez-vous que les journaux incluent la période pendant laquelle l'hôte a reçu la configuration de SpoofGuard.
301062	Majeur	Non	`Échec de l'application de Spoofguard à la vNIC. (Failed to apply spoofguard to vnic.)`	L'application de Spoofguard à la vNIC a échoué. Action : vérifiez que la procédure de préparation de l'hôte a bien été suivie. Connectez-vous à l'hôte et collectez le fichier `/var/log/vsfwd.log`, puis forcez la synchronisation de la configuration du pare-feu avec l'API `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` (reportez-vous à la section « Dépannage de Pare-feu distribué » du *Guide de dépannage de NSX*). Si la configuration de SpoofGuard échoue toujours, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301064	Majeur	Non	`Impossible de désactiver Spoofguard pour la vNIC. (Failed to disable spoofguard for vnic.)`	La désactivation de Spoofguard pour la vNIC a échoué. Action : collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301072	Critique	Non	`Échec de la suppression de vm existante sur le service d'application. (Failed to delete legacy App service vm.)`	La machine virtuelle du service vShield App pour vCloud Networking and Security n'a pas pu être supprimée. Action : vérifiez que la procédure de mise à niveau de vShield App vers Distributed Firewall décrite dans le *Guide de mise à niveau de NSX* a bien été suivie.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301080	Critique	Non	`Seuil de CPU du pare-feu franchi. (Firewall CPU threshold crossed.)`	La valeur du seuil d'utilisation du CPU vsfwd a été dépassée. Action : reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*. Il vous sera peut-être nécessaire de réduire l'utilisation des ressources de l'hôte. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301081	Critique	Non	`Seuil de mémoire du pare-feu franchi. (Firewall memory threshold crossed.)`	La valeur du seuil de la mémoire vsfwd a été dépassée. Action : reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*. Il vous sera peut-être nécessaire de réduire l'utilisation des ressources de l'hôte, notamment le nombre de règles de pare-feu configurées ou de conteneurs réseau et sécurité. Pour réduire le nombre de règles de pare-feu, utilisez la fonctionnalité `appliedTo`. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301082	Critique	Non	`Seuil de ConnectionsPerSecond du pare-feu franchi. (Firewall ConnectionsPerSecond threshold crossed.)`	Le seuil pour les connexions de pare-feu par seconde a été dépassé. Action : reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*. Il vous sera peut-être nécessaire de réduire l'utilisation des ressources de l'hôte, notamment le nombre de connexions actives en provenance et à destination des machines virtuelles de l'hôte.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301501	Critique	Non	La mise à jour de la configuration du pare-feu vers la version {version#} sur l'hôte {hostID} a expiré. La configuration du pare-feu de l'hôte est synchronisée jusqu'à la version {version#}. (Firewall configuration update version {version#} to host {hostID} timed out. Firewall configuration on host is synced upto version {version#}.)	Un hôte a mis plus de deux minutes pour traiter la mise à jour d'une configuration du pare-feu, et la mise à jour a expiré. Action : vérifiez que vsfwd fonctionne et que les règles ont été publiées sur les hôtes. Reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301502	Critique	Non	La mise à jour de la configuration de Spoofguard vers le numéro {number#} sur l'hôte {hostID} a expiré. La configuration de Spoofguard de l'hôte est synchronisée jusqu'à la version {version#}. (Spoofguard configuration update number {number#} to host {hostID} timed out. Spoofguard configuration on host is synced upto version {version#}.)	Un hôte a mis plus de deux minutes pour traiter la mise à jour d'une configuration de SpoofGuard, et la mise à jour a expiré. Action : vérifiez que vsfwd fonctionne et que les règles ont été publiées sur les hôtes. Reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301503	Critique	Non	Échec de la publication de la version {version#} de la configuration de pare-feu sur le cluster {clusterID}. Reportez-vous aux journaux pour plus d'informations. (Failed to publish firewall configuration version {version#} to cluster {clusterID}. Refer logs for details.)	La publication des règles de pare-feu a échoué pour un cluster ou pour un ou plusieurs hôtes. Action : reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301504	Critique	Non	Échec de la publication des mises à jour de conteneur vers le cluster {clusterID}. Reportez-vous aux journaux pour plus d'informations. (Failed to publish container updates to cluster {clusterID}. Refer logs for details.)	La publication des mises à jour des conteneurs réseau et sécurité a échoué pour un cluster ou pour un ou plusieurs hôtes. Action : reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301505	Critique	Non	Échec de la publication des mises à jour de Spoofguard vers le cluster {clusterID}. Reportez-vous aux journaux pour plus d'informations. (Failed to publish spoofguard updates to cluster {clusterID}. Refer logs for details.)	La publication des mises à jour de Spoofguard a échoué pour un cluster ou pour un ou plusieurs hôtes. Action : reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301506	Critique	Non	Échec de la publication des mises à jour de liste d'exclusion vers le cluster {clusterID}. Reportez-vous aux journaux pour plus d'informations. (Failed to publish exclude list updates to cluster {clusterID}. Refer logs for details.)	La publication des mises à jour des listes d'exclusion a échoué pour un cluster ou pour un ou plusieurs hôtes. Action : reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301508	Critique	Non	Échec de la synchronisation de l'hôte {hostID}. Reportez-vous aux journaux pour plus d'informations. (Failed to sync host {hostID}. Refer logs for details.)	Une opération de synchronisation forcée du pare-feu via l'API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` a échoué. Action : reportez-vous à la section « Dépannage de Distributed Firewall » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301510	Critique	Non	Échec de la synchronisation forcée pour le cluster. (Force sync operation failed for the cluster.)	Une opération de synchronisation forcée du pare-feu via l'API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` a échoué. Action : collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301512	Majeur	Non	Le pare-feu est installé sur l'hôte {hostID}[{hostID}]. (Firewall is installed on host {hostID} [{hostID}].)	Le pare-feu distribué a été installé sur un hôte. Action : dans vCenter Server, accédez à **Accueil > Networking & Security > Installation**, puis sélectionnez l'onglet Préparation de l'hôte. Vérifiez que l'état du pare-feu s'affiche en vert.
301513	Majeur	Non	Le pare-feu est désinstallé sur l'hôte {hostID}[{hostID}]. (Firewall is uninstalled on host {hostID}[{hostID}].)	Le pare-feu distribué a été désinstallé d'un hôte. Si la désinstallation des composants du pare-feu distribué échoue toujours, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301514	Critique	Non	`Le pare-feu est activé sur le cluster {clusterID}. (Firewall is enabled on cluster {clusterID}.)`	Le pare-feu distribué a été installé sur un cluster. Action : dans vCenter Server, accédez à **Accueil > Networking & Security > Installation**, puis sélectionnez l'onglet Préparation de l'hôte. Vérifiez que l'état du pare-feu s'affiche en vert.
301515	Critique	Non	`Le pare-feu est désinstallé sur le cluster {clusterID}. (Firewall is uninstalled on cluster {clusterID}.)`	Le pare-feu distribué a été désinstallé d'un cluster. Action : si la désinstallation des composants du pare-feu distribué échoue toujours, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301516	Critique	Non	`Le pare-feu est désactivé sur le cluster {clusterID}. (Firewall is disabled on cluster {clusterID}.)`	Le pare-feu distribué a été désactivé sur tous les hôtes d'un cluster. Action : aucune action n'est nécessaire.
301034	Majeur	Non	`Échec de l'application des règles du pare-feu à l'hôte. (Failed to apply Firewall rules to host.)`	Une section de règles de pare-feu distribué n'a pas pu être appliquée. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301043	Critique	Non	`Échec de l'application de la configuration du conteneur à la vNIC. (Failed to apply container configuration to vnic.)`	L'application d'une configuration de conteneur réseau ou sécurité a échoué. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301044	Critique	Non	`Échec de l'application de la configuration du conteneur à l'hôte. (Failed to apply container configuration to host.)`	L'application d'une configuration de conteneur réseau ou sécurité a échoué. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301066	Majeur	Non	`Échec de l'application de la configuration de Spoofguard à l'hôte. (Failed to apply Spoofguard configuration to host.)`	L'application de Spoofguard aux vNIC a échoué. Action : vérifiez que les segments de mémoire du noyau vsip ont suffisamment de mémoire libre (reportez-vous à la section « Afficher les événements de seuil de CPU et de mémoire du pare-feu » du *Guide d'administration de NSX*.) Si le problème persiste, collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware.
301100	Critique	Non	`Échec de la mise à jour de la configuration du délai d'expiration du pare-feu sur l'hôte. (Firewall timeout configuration update failed on host.)`	La mise à jour de la configuration du délai d'expiration du temporisateur de la session du pare-feu a échoué. Action : collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez l'assistance VMware. Après avoir collecté les journaux, forcez la synchronisation de la configuration du pare-feu avec l'API REST `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` ou accédez à **Installation > Préparation de l'hôte** et, sous **Actions**, sélectionnez **Forcer les services de synchronisation**.
301101	Majeur	Non	`Échec de l'application de la configuration du délai d'expiration du pare-feu à la vNIC. (Failed to apply firewall timeout configuration to vnic.)`	La mise à jour de la configuration du délai d'expiration du temporisateur de la session du pare-feu a échoué. Action : collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware. Après avoir collecté les journaux, forcez la synchronisation de la configuration du pare-feu avec l'API REST `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` ou accédez à **Installation > Préparation de l'hôte** et, sous **Actions**, sélectionnez **Forcer les services de synchronisation**.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
301103	Majeur	Non	`Échec de l'application de la configuration du délai d'expiration du pare-feu à l'hôte. (Failed to apply firewall timeout configuration to host.)`	La mise à jour de la configuration du délai d'expiration du temporisateur de la session du pare-feu a échoué. Action : collectez les journaux de support technique pour NSX Manager et l'hôte, puis contactez le support technique VMware. Après avoir collecté les journaux, forcez la synchronisation de la configuration du pare-feu avec l'API REST `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` ou accédez à **Installation > Préparation de l'hôte** et, sous **Actions**, sélectionnez **Forcer les services de synchronisation**.
301200	Majeur	Non	`L'analyse des flux du gestionnaire de règles d'application a démarré. (Application Rule Manager flow analysis started.)`	L'analyse des flux du gestionnaire de règles d'application a démarré. Action : aucune action n'est nécessaire.
301201	Majeur	Non	`Échec de l'analyse des flux du gestionnaire de règles d'application. (Application Rule Manager flow analysis failed.)`	Échec de l'analyse des flux du gestionnaire de règles d'application. Action : collectez les journaux de support technique pour NSX Manager, puis contactez le support technique VMware. Démarrez une nouvelle session de surveillance sur les mêmes vNIC que celles de la session qui a échoué, pour tenter à nouveau l'opération.
301202	Majeur	Non	`L'analyse des flux du gestionnaire de règles d'application est terminée. (Application Rule Manager flow analysis completed.)`	L'analyse des flux du gestionnaire de règles d'application est terminée. Action : aucune action n'est nécessaire.

Événements systèmes de NSX Edge

Le tableau décrit les messages d'événement système de NSX Edge dont le niveau de gravité peut être majeur, critique ou élevé. Les événements système dont la gravité est Informatif sont répertoriés s'ils déclenchent l'alarme.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30011	Élevé	S/O	`Aucune VM NSX Edge n'est en service. La connexion au réseau est peut-être interrompue. (None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.)`	Les machines virtuelles NSX Edge doivent récupérer automatiquement de cet état. Recherchez une interruption dont le code d'événement est 30202 ou 30203. Action : reportez-vous à la section « Dépannage du dispositif Edge » du *Guide de dépannage de NSX*.
30013	Critique	130013	`NSX Manager indique que la VM NSX Edge (vmId : {#}) est défectueuse. Forcez la synchronisation. (NSX Manager found NSX Edge VM (vmId : {#}) in bad state. Needs a force sync.)`	La VM NSX Edge indique un état défectueux, alors qu'il est possible qu'elle ne fonctionne pas correctement. Action : une synchronisation forcée automatique est déclenchée lorsqu'un état problématique est détecté. Si la synchronisation forcée automatique échoue, essayez d'effectuer une synchronisation forcée manuelle.
30014	Majeur	S/O	`Impossible de communiquer avec la VM NSX Edge. (Failed to communicate with the NSX Edge VM.)`	NSX Manager communique avec NSX Edge via VIX ou le bus de messages. Le canal de communication est sélectionné par NSX Manager en fonction de l'état de la préparation de l'hôte (si celle-ci était ou non effectuée au moment du déploiement ou du redéploiement du dispositif Edge). Cet événement indique que NSX Manager a perdu la communication avec NSX Edge. Action : reportez-vous à la section « Dépannage du dispositif Edge » du *Guide de dépannage de NSX*.
30027	Informatif	130027	`La VM NSX Edge (vmId : {#}) est hors tension. (NSX Edge VM (vmId : {#}) is powered off.)`	La machine virtuelle NSX Edge a été mise hors tension. Action : événement informatif uniquement.
30032	Élevé	130032	`Le dispositif NSX Edge portant le vmId {#} est introuvable dans l'inventaire de vCenter. (NSX Edge appliance with vmId : {#} not found in the vCenter inventory.)`	La VM NSX Edge a probablement été supprimée directement à partir de vCenter Server. Cette opération n'est pas prise en charge, car les objets gérés par NSX doivent être ajoutés ou supprimés à partir de l'interface de vSphere Web Client pour NSX. Action : redéployez le dispositif Edge ou déployez un nouveau dispositif Edge.
30033	Élevé	130033	`VM NSX Edge (vmId : {#}) introuvable dans l'inventaire vCenter. (NSX Edge VM (vmId : {#}) not found in the vCenter inventory.)`	Impossible de trouver la machine virtuelle NSX Edge dans l'inventaire vCenter. Action : vérifiez si la machine virtuelle a été supprimée accidentellement. Dans l'affirmative, redéployez le dispositif Edge.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30034	Critique	130034	Aucune VM NSX Edge n'est en service. La connexion au réseau est peut-être interrompue. (None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.)	La VM Edge ne répond pas à la vérification de l'intégrité envoyée par NSX Manager. Action : vérifiez que la VM Edge est sous tension. Ensuite, collectez les journaux Edge et contactez le support technique VMware.
30037	Critique	S/O	La règle de pare-feu du dispositif Edge modifiée en {#} n'est plus disponible pour {#}. (Edge firewall rule modified as {#} is no longer available for {#}.)	Un GroupingObject non valide (IPSet, securityGroup, etc.) est présent dans la règle de pare-feu. Action : revoyez la règle de pare-feu et faites les mises à jour nécessaires.
30038	Critique	S/O	Dispositif NSX Edge sous tension : {EdgeId #}, {vmName #} enfreint la règle d'anti-affinité de machine virtuelle. (Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule.)	La fonction de haute disponibilité de NSX Edge applique automatiquement des règles d'anti-affinité aux hôtes vSphere, de sorte que les machines virtuelles Edge actives et en veille sont déployées sur des hôtes différents. Cet événement indique que ces règles d'anti-affinité ont été supprimées du cluster et que les deux machines virtuelles Edge s'exécutent sur le même hôte. Action : accédez à vCenter Server et vérifiez les règles d'anti-affinité.
30045	Critique	S/O	Échec du contrôle d'intégrité de la VM NSX Edge avec des erreurs critiques vix. Le contrôle d'intégrité est désactivé pour la VM. Pour le reprendre, redéployez la VM ou forcez sa synchronisation. (NSX Edge VM health check failing with critical vix errors. Further health check is disabled for vm. Please redeploy or forcesync vm to resume health check.)	L'environnement réseau est peut-être à l'origine d'erreurs de communication répétées de la machine virtuelle Edge sur le canal VIX. Action : collectez les journaux de support technique de NSX Manager et NSX Edge si NSX Edge est réactif. Effectuez ensuite une synchronisation forcée. Si le problème persiste, redéployez NSX Edge(reportez-vous à la section « Redéployer le dispositif NSX Edge » du *Guide d'administration de NSX*). **Note** Le redéploiement est une action perturbatrice. Il est recommandé de réaliser en premier lieu une synchronisation forcée et de procéder à un nouveau déploiement ensuite si le problème n'est pas résolu.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30046	Critique	S/O	La publication des règles préalables a échoué sur le dispositif Edge : {EdgeID#}, vm : {#} pour le numéro de génération {#}. Consultez les journaux pour plus de détails. Une synchronisation forcée peut s'avérer nécessaire. (Pre rules publish failed on edge: {EdgeID#}, vm: {#} for generation number {#}. Refer logs for detail. It may need forcesync.)	Les règles de pare-feu de NSX Edge sont peut-être désynchronisées. Cette erreur est générée si des règles préalables (configurées à partir de l'interface utilisateur DFW/l'API) échouent. Action : si le problème n'est pas résolu automatiquement par le processus de récupération intégré, effectuez une synchronisation forcée manuelle.
30100	Critique	S/O	La synchronisation de NSX Edge a été forcée. (NSX Edge was force synced.)	La machine virtuelle NSX Edge a été soumise à une synchronisation forcée. Action : si la synchronisation forcée ne résout pas le problème, collectez les journaux de support technique pour NSX Manager et NSX Edge, puis contactez le support technique VMware.
30102	Élevé	130102	NSX Edge (vmId : {IP Address}) est défectueux. Forcez la synchronisation. (NSX Edge (vmId : {IP Address}) is in Bad State. Needs a force sync.)	La machine virtuelle NSX Edge est affectée par une erreur interne. Action : si le problème n'est pas résolu automatiquement par le processus de récupération intégré, essayez de procéder à une synchronisation forcée manuelle.
30148	Critique	S/O	L'utilisation du processeur par NSX Edge a augmenté. Les {#} principaux processus sont : {#}. (NSX Edge CPU usage has increased. {#} Top processes are: {#}.)	L'utilisation du CPU de la machine virtuelle NSX Edge est élevée durant des périodes prolongées. Action : reportez-vous à la section « Dépannage du dispositif Edge » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et NSX Edge, puis contactez le support technique VMware.
30153	Majeur	S/O	Moteur de chiffrement AESNI activé. (AESNI crypto engine is up.)	Le moteur de chiffrement AESNI est activé. Action : aucune action n'est nécessaire.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30154	Majeur	S/O	Moteur de chiffrement AESNI désactivé. (AESNI crypto engine is down.)	Le moteur de chiffrement AESNI est désactivé. Action : aucune action n'est nécessaire. Cet état est normal.
30155	Élevé	130155	Ressources de CPU et de mémoire insuffisantes sur l'hôte ou le pool de ressources, lors de la réservation de ressources au moment du déploiement de NSX Edge. (Insufficient cient CPU and/or Memory Resources available on Host or Resource Pool, during resource reservation at the time of NSX Edge deployment.)	Ressources de CPU et/ou de mémoire insuffisantes sur l'hôte ou dans le pool de ressources. Vous pouvez afficher les ressources disponibles et les ressources réservées en accédant à la page **Accueil (Home) > Hôtes et clusters > [nom-du-cluster] (Hosts and Clusters > [Cluster-name])**> **Surveiller (Monitor) > Réservation des ressources (Resource Reservation)**. Après avoir vérifié les ressources disponibles, spécifiez de nouveau celles qui font partie de la configuration du dispositif de sorte que la limite de réservation des ressources soit acceptée.
30180	Critique	S/O	La mémoire du dispositif NSX Edge est insuffisante. Le dispositif Edge va redémarrer dans 3 secondes. Les 5 principaux processus sont : {#}. (NSX Edge is out of memory. The Edge is rebooting in 3 seconds. Top 5 processes are: {#}.)	La mémoire de la machine virtuelle NSX Edge est insuffisante. Un redémarrage a été effectué pour récupérer. Action : reportez-vous à la section « Dépannage du dispositif Edge » du *Guide de dépannage de NSX*. Si le problème persiste, collectez les journaux de support technique pour NSX Manager et NSX Edge, puis contactez le support technique VMware.
30181	Critique	130181	Le système de fichiers de nom de VM {#} de NSX Edge {EdgeID#} est en lecture seule. (NSX Edge {EdgeID#} VM name {#} file system is read only.)	Il existe un problème de connectivité avec le périphérique de stockage qui supporte la machine virtuelle NSX Edge. Action : corrigez tout problème de connectivité affectant la banque de données de sauvegarde. Il peut être nécessaire d'effectuer une synchronisation forcée manuelle après la résolution du problème de connectivité.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30202	Majeur	S/O	`Basculement de NSX Edge {EdgeID#} HighAvailability. La VM {#} avec le nom {#} est passée à l'état ACTIVE. (NSX Edge {EdgeID#} HighAvailability switch over happened. VM {#} name {#} has moved to ACTIVE state.)`	Un basculement d'Edge HA s'est produit et la machine virtuelle NSX Edge secondaire est passée de l'état STANDBY à l'état ACTIVE. Action : aucune action n'est nécessaire.
30203	Majeur	S/O	`Basculement de NSX Edge {EdgeID} HighAvailability. La VM {#} avec le nom {#} est passée à l'état STANDBY. (NSX Edge {EdgeID} HighAvailability switch over happened. VM {#} name {#} has moved to STANDBY state.)`	Un basculement d'Edge HA s'est produit et la machine virtuelle NSX Edge principale est passée de l'état ACTIVE à l'état STANDBY. Action : aucune action n'est nécessaire.
30205	Critique	130205	`Split Brain détecté pour NSX Edge {EdgeID} avec HighAvailability. (Split Brain detected for NSX Edge {EdgeID} with HighAvailability.)`	En raison d'une panne de réseau, les machines virtuelles NSX Edge configurées pour la haute disponibilité ne parviennent pas à déterminer si l'autre machine virtuelle est en ligne. Dans ce scénario, les deux machines virtuelles passent à l'état Actif, car elles estiment mutuellement qu'elles ne sont pas actives. Cela peut provoquer une interruption du réseau. Action : recherchez d'éventuels échecs et dysfonctionnements dans l'infrastructure de réseau (virtuel et physique), en particulier sur les interfaces et le chemin d'accès configuré pour la haute disponibilité.
30302	Critique	130302	`LoadBalancer virtualServer/pool : {virtualServerName]} Protocole : {#} serverIp : {IP Address} a remplacé l'état par Arrêté. (LoadBalancer virtualServer/pool : {virtualServerName]} Protocol : {#} serverIp : {IP Address} changed the state to down.)`	Un serveur virtuel ou un pool de l'équilibrage de charge de NSX Edge est arrêté. Action : reportez-vous à la section « Équilibrage de charge » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30303	Majeur	S/O	`LoadBalancer virtualServer/pool : {0} Protocole : {#} serverIp : {IP Address} a été modifié pour un état incorrect. (LoadBalancer virtualServer/pool : {0} Protocol : {#} serverIp : {IP Address} changed to a wrong state.)`	Un serveur virtuel ou un pool de l'équilibrage de charge de NSX Edge est affecté par une erreur interne. Action : reportez-vous à la section « Équilibrage de charge » du *Guide de dépannage de NSX*.
30304	Majeur	130304	`LoadBalancer pool : {0} Protocole : {#} serverIp : {IP address} a été modifié pour un état d'avertissement. (LoadBalancer pool : {0} Protocol : {#} serverIp : {IP address} changed to a warning state.)`	Un pool d'équilibrage de charge de NSX Edge est passé à l'état **avertissement (warning)**. Action : reportez-vous à la section « Équilibrage de charge » du *Guide de dépannage de NSX*.
30402	Critique	130402	`Le canal IPSEC de localIp : {IP address} à peerIp : {IP address} a remplacé l'état par Arrêté. (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down.)`	Un canal VPN IPSec de NSX Edge est arrêté. Action : reportez-vous à la section « Réseaux privés virtuels (VPN) » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30404	Critique	130404	TUNNEL EDGE IPSEC ARRÊTÉ : Le tunnel IPSEC de localSubnet : {subnet} à peerSubnet : {subnet} a remplacé l'état par Arrêté. (EDGE IPSEC TUNNEL DOWN : IPsec Tunnel from localSubnet : {subnet} to peerSubnet : {subnet} changed the status to down.)	Un canal VPN IPSec de NSX Edge est arrêté. Action : reportez-vous à la section « Réseaux privés virtuels (VPN) » du *Guide de dépannage de NSX*.
30405	Majeur	S/O	Le canal IPSEC de localIp : {IP address} en peerIp : {IP address} a modifié le statut en Inconnu. (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.)	L'état d'un canal VPN IPSec de NSX Edge ne peut pas être déterminé. Action : reportez-vous à la section « Réseaux privés virtuels (VPN) » du *Guide de dépannage de NSX*.
30406	Majeur	S/O	Le canal IPSEC de localIp : {IP address} en peerIp : {IP address} a modifié le statut en Inconnu. (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.)	L'état d'un canal VPN IPSec de NSX Edge ne peut pas être déterminé. Action : reportez-vous à la section « Réseaux privés virtuels (VPN) » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Code d'alarme	Message d'événement	Description
30701	Critique	S/O	`Le service de relais DHCP NSX Edge sur Edge {EdgeID} est désactivé, car aucun serveur DHCP externe n'est fourni. Vérifiez l'adresse IP du serveur ou l'objet de groupement référencé. (NSX Edge DHCP Relay service on edge {EdgeID} is disabled because there is no external DHCP server provided. Please check server IP or referenced grouping object.)`	Le service de relais DHCP de NSX Edge est désactivé. Raisons possibles : (1) Le processus de relais DHCP n'est pas en cours d'exécution. (2) Il n'y a pas de serveur DHCP externe. Ce problème peut provenir de la suppression d'objets de regroupement référencés par le relais. Action : reportez-vous à la section « Configuration du relais DHCP » du *Guide d'administration de NSX*.
30206	Critique	S/O	`Split Brain résolu pour NSX Edge {EdgeID} avec HighAvailability. (Resolved Split Brain for NSX Edge {EdgeID} with HighAvailability.)`	Les deux dispositifs NSX Edge HA peuvent communiquer l'un avec l'autre et ont renégocié leur état actif et en veille. Action : reportez-vous à l'article indiquant comment résoudre les problèmes de haute disponibilité dans NSX Edge : (http://kb.vmware.com/kb/2126560).
30207	Critique	S/O	`Tentative de résolution de Split Brain pour NSX Edge {EdgeID} avec le nombre {value}. (Attempted Split Brain resolution for NSX Edge {EdgeID} with count {value}.)`	Les deux dispositifs NSX Edge HA tentent de renégocier et de récupérer d'une condition de Split Brain. **Note** Le mécanisme de récupération signalé par cet événement se produit uniquement dans les versions de NSX Edge antérieures à la version 6.2.3. Action : reportez-vous à l'article indiquant comment résoudre les problèmes de haute disponibilité dans NSX Edge : (http://kb.vmware.com/kb/2126560).

Événements système liés à l'infrastructure

Le tableau décrit les messages des événements système liés à l'infrastructure.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250000	Informatif	Non	L'ancien statut opérationnel de l'unité de déploiement était {#}, le nouveau statut opérationnel est {#} et l'ancien état de progression était {#}, le nouvel état de progression est {#}. Consultez la chaîne d'alarme pour voir la cause d'origine. (Deployment unit old operational status was {#} , new operational status is {#} and old progress state was {#}, new progress state is {#}. Check alarm string for root cause.)	Événement informatif uniquement.
250001	Informatif	Non	Une unité de déploiement a été créée. (A deployment unit has been created.)	Événement informatif uniquement.
250002	Informatif	Non	Une unité de déploiement dans NSX a été mise à jour. Des services d'infrastructure seront mis à jour sur le cluster. (A deployment unit in NSX has been updated. Fabric services will be updated on the cluster.)	Événement informatif uniquement.
250003	Informatif	Non	Une unité de déploiement a été supprimée de NSX. (A deployment unit has been deleted from NSX.)	Événement informatif uniquement.
250004	Élevé	Oui	Échec du déploiement du service {#} sur l'hôte {#}, car la banque de données {#} n'est pas connectée à l'hôte. Vérifiez qu'elle est connectée ou fournissez une banque de données différente. (Failed to deploy service {#} on host {#} since datastore (#) is not connected to the host. Please verify that it is connected, or provide a different datastore.)	La banque de données dans laquelle vous stockez les machines virtuelles de sécurité pour l'hôte n'a pas pu être configurée. Action : vérifiez que l'hôte peut atteindre la banque de données.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250005	Élevé	Oui	`L'installation de l'unité de déploiement a échoué. Vérifiez que les URL OVF/VIB sont accessibles, que DNS est configuré et que les ports réseau requis sont ouverts. (Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)`	L'hôte ESXi n'a pas pu accéder aux bundles VIB/OVF depuis NSX lors de l'installation d'un service NSX sur l'hôte. Le tableau des événements système vCenter affiche le message d'événement suivant : `'L'installation de l'unité de déploiement a échoué. Vérifiez que les URL OVF/VIB sont accessibles, que DNS est configuré et que les ports réseau requis sont ouverts. (Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)', Module:'Security Fabric'`. Action : reportez-vous à la section *Guide de dépannage de NSX*.
250006	Informatif	Non	`L'agent d'infrastructure pour les services d'infrastructure réseau a été correctement installé sur un hôte. (The fabric agent for network fabric services installed successfully on a host.)`	Événement informatif uniquement.
250007	Informatif	Non	`L'agent d'infrastructure a été correctement supprimé d'un hôte. (The fabric agent was removed successfully from a host.)`	Événement informatif uniquement.
250008	Élevé	Oui	`L'emplacement des fichiers OVF/VIB a été modifié. Le service doit être redéployé. (Location of OVF / VIB files has changed. Service must be redeployed.)`	Les bundles VIB et OVF de NSX sont accessibles via une URL qui diffère selon la version de NSX. Pour trouver les bundles VIB adéquats, accédez à *https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties*. Si l'adresse IP de NSX Manager change, il peut être nécessaire de redéployer les bundles VIB ou OVF de NSX. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250009	Élevé	Oui	La mise à niveau de l'unité de déploiement a échoué. Vérifiez que les URL OVF/VIB sont accessibles, que DNS est configuré et que les ports réseau requis sont ouverts. (Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)	EAM n'a pas pu accéder aux bundles VIB/OVF depuis NSX pendant la mise à niveau d'un hôte. Le tableau des événements système vCenter affiche le message d'événement suivant : 'La mise à niveau de l'unité de déploiement a échoué. Vérifiez que les URL OVF/VIB sont accessibles, que DNS est configuré et que les ports réseau requis sont ouverts. (Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)', Module:'Security Fabric'. Action : reportez-vous à la section *Guide de dépannage de NSX*.
250012	Élevé	Oui	Les services suivants doivent être installés pour que le service {#} fonctionne : {#} (Following service(s) need to be installed successfully for Service {#} to function: {#}.)	Le service en cours d'installation dépend d'un autre service qui n'a pas encore été installé. Action : déployez le service nécessaire sur le cluster.
250014	Élevé	Oui	Erreur lors de l'envoi de la notification à la solution de sécurité avant la mise à niveau. La solution n'est peut-être pas accessible ou elle ne répond pas. Vérifiez que les URL de la solution sont accessibles depuis NSX. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera redéployé. (Error while notifying security solution before upgrade. The solution may not be reachable/responding. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be redeployed.)	Une erreur s'est produite lors de l'envoi de la notification à la solution de sécurité avant la mise à niveau. La solution n'est peut-être pas joignable ou elle ne répond pas. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme. Le service sera redéployé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250015	Élevé	Oui	N'a pas reçu de rappel de la solution de sécurité pour la notification de mise à niveau, même après le délai d'expiration. Vérifiez que les URL de la solution sont accessibles depuis NSX, et que NSX est accessible depuis la solution. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera redéployé. (Did not receive callback from security solution for upgrade notification even after timeout. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be redeployed.)	Aucun rappel de la solution de sécurité n'a été reçu pour la notification de mise à niveau, même après le délai d'expiration. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX et que NSX est joignable depuis la solution. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.
250016	Élevé	Non	La désinstallation du service a échoué. Vérifiez que les URL de la solution sont accessibles depuis NSX, et que NSX est accessible depuis la solution. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera supprimé. (Uninstallation of service failed. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.)	La désinstallation du service a échoué. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX et que NSX est joignable depuis la solution. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250017	Élevé	Oui	`Erreur lors de l'envoi de la notification à la solution de sécurité avant la désinstallation. Résolvez pour envoyer de nouveau la notification ou supprimez pour désinstaller sans envoyer de notification. Vérifiez que les URL de la solution sont accessibles depuis NSX, et que NSX est accessible depuis la solution. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera supprimé. (Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.)`	Erreur lors de l'envoi de la notification à la solution de sécurité avant la désinstallation. Cliquez sur Résoudre pour renvoyer la notification ou sur Supprimer pour désinstaller sans envoyer de notification. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX et que NSX est joignable depuis la solution. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.
250018	Élevé	Oui	`Erreur lors de l'envoi de la notification à la solution de sécurité avant la désinstallation. Résolvez pour envoyer de nouveau la notification ou supprimez pour désinstaller sans envoyer de notification. Vérifiez que les URL de la solution sont accessibles depuis NSX, et que NSX est accessible depuis la solution. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera supprimé. (Error while notifying security solution before uninstall.Resolve to notify once again, or delete to uninstall without notification. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.)`	Erreur lors de l'envoi de la notification à la solution de sécurité avant la désinstallation. Cliquez sur Résoudre pour renvoyer la notification ou sur Supprimer pour désinstaller sans envoyer de notification. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX et que NSX est joignable depuis la solution. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250019	Élevé	Oui	`Le serveur a redémarré alors que la notification de la solution de sécurité pour la désinstallation était en cours d'envoi. Vérifiez que les URL de la solution sont accessibles depuis NSX. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera désinstallé. (Server rebooted while security solution notification for uninstall was going on. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be uninstalled.)`	Le serveur a redémarré alors que la notification pour la désinstallation était en cours d'envoi à la solution de sécurité. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme. Le service sera désinstallé.
250020	Élevé	Oui	`Le serveur a redémarré alors que la notification de la solution de sécurité pour la mise à niveau était en cours d'envoi. Vérifiez que les URL de la solution sont accessibles depuis NSX. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera redéployé. (Server rebooted while security solution notification for upgrade was going on. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be redeployed.)`	Le serveur a redémarré alors que la notification pour la mise à niveau était en cours d'envoi à la solution de sécurité. Action : assurez-vous que les URL de la solution sont accessibles depuis NSX. Utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme. Le service sera redéployé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250021	Critique	Non	NSX Manager repose sur le service EAM dans vCenter pour déployer/surveiller des VIB NSX sur ESX. La connexion à ce service EAM s'est arrêtée. Cela peut être dû au service EAM ou au redémarrage/arrêt de vCenter ou à un problème dans le service EAM. Vérifiez que vCenter est actif et que le service EAM dans vCenter est en cours d'exécution. De plus, nous pouvons consulter le mob d'EAM pour vérifier qu'EAM fonctionne comme prévu. (NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX vibs on ESX. The connection to this EAM service has gone down. This could be due to EAM service or vCenter restart/stop or an issue in the EAM service. Verify that vCenter is up, and the EAM service in vCenter is running. Further, we can look at EAM mob to verify that EAM is functioning as expected.)	NSX Manager repose sur le service EAM dans vCenter pour déployer/surveiller des VIB NSX sur ESX. La connexion à ce service EAM est arrêtée. Cela peut être dû au service EAM, au redémarrage/arrêt de vCenter ou à un problème dans le service EAM. Action : vérifiez que vCenter est activé et que le service EAM dans vCenter est en cours d'exécution. Vérifiez que l'URL du MOB d'EAM **`http://{vCenter_IP}/eam/mob/`** est accessible et qu'EAM fonctionne comme prévu. Pour plus d'informations, reportez-vous à la section « Préparation de l'infrastructure » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250022	Critique	Non	`NSX Manager repose sur le service EAM dans VC pour déployer/surveiller des VIB NSX sur ESX. La connexion à ce service EAM s'est arrêtée. Cela peut être dû au service EAM ou au redémarrage/arrêt de VC ou à un problème dans le service EAM. Vérifiez que VC est actif et que le service EAM dans VC est en cours d'exécution. De plus, nous pouvons consulter le mob d'EAM pour vérifier qu'EAM fonctionne comme prévu. (NSX Manager relies on the EAM service in VC for deploying/monitoring NSX vibs on ESX. The connection to this EAM service has gone down. This could be due to EAM service or VC restart/stop or an issue in the EAM service. Verify that VC is up, and the EAM service in VC is running. Further, we can look at EAM mob to verify that EAM is functioning as expected.)`	NSX Manager repose sur le service EAM dans vCenter pour déployer/surveiller des VIB NSX sur ESX. La connexion à ce service EAM est arrêtée. Cela peut être dû au service EAM, au redémarrage/arrêt de vCenter ou à un problème dans le service EAM. Action : vérifiez que vCenter est activé et que le service EAM dans vCenter est en cours d'exécution. Vérifiez que l'URL du MOB d'EAM **`http://{vCenter_IP}/eam/mob/`** est accessible et qu'EAM fonctionne comme prévu. Pour plus d'informations, reportez-vous à la section « Préparation de l'infrastructure » du *Guide de dépannage de NSX*.
250023	Élevé	Oui	`Échec du nettoyage préalable à la désinstallation. Utilisez l'API de résolution pour résoudre l'alarme. Le service sera supprimé. (Pre Uninstall cleanup failed. Use resolve API to resolve the Alarm. Service will be removed.)`	Les tâches de nettoyage interne préalables à la désinstallation ont échoué. Action : utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme. Le service sera supprimé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
250024	Élevé	Oui	L'agence EAM de sauvegarde de cette unité de déploiement est introuvable. Il est possible que les services VC soient toujours en cours d'initialisation. Essayez de résoudre l'alarme pour vérifier l'existence de l'agence. Au cas où vous avez supprimé l'agence manuellement, supprimez l'entrée de déploiement de NSX. (The backing EAM agency for this deployment unit could not be found. It is possible that the VC services may still be initializing. Please try to resolve the alarm to check existence of the agency. In case you have deleted the agency manually, please delete the deployment unit entry from NSX.)	EAM déploie des VIB sur des hôtes ESXi. Une agence EAM est installée sur chaque cluster préparé pour NSX. Si cette agence est introuvable, cela signifie que les services vCenter Server sont peut-être en cours d'initialisation ou que l'agence a été supprimée manuellement par erreur.
250025	Élevé	Oui	Cet événement est généré lors d'une tentative de mise à niveau ou de désinstallation des VIB NSX sur un hôte sans état à l'aide d'EAM. Tous les hôtes sans état doivent être préparés à l'aide de la fonctionnalité de déploiement automatique. Corrigez la configuration avec la fonctionnalité de déploiement automatique et utilisez l'API de résolution pour résoudre l'alarme. (This event is generated when an attempt is made to upgrade or uninstall NSX vibs on stateless host using EAM. All stateless host should be prepared using the auto deploy feature. Fix configuration using auto deploy feature, and use the resolve API to resolve the alarm.)	Cet événement est généré lors de la tentative de mise à niveau ou de désinstallation des VIB NSX sur l'hôte sans état, à l'aide d'EAM. Tous les hôtes sans état doivent être préparés à l'aide de la fonction Auto Deploy. Action : corrigez la configuration à l'aide de la fonctionnalité de déploiement automatique et utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Événements système liés au plug-in de déploiement

Le tableau décrit les messages d'événement système liés au plug-in de déploiement dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
280000	Élevé	Oui	`Alarme de dépassement du pool IP du plug-in de déploiement. (Deployment Plugin IP pool exhausted alarm.)`	Une adresse IP n'a pas pu être attribuée à la machine virtuelle d'un service NSX, car le pool d'adresses IP sources était épuisé. Action : ajoutez des adresses IP dans le pool.
280001	Élevé	Oui	`Alarme générique de plug-in de déploiement. (Deployment Plugin generic alarm.)`	Chaque service, tel que Guest Introspection, possède un ensemble de plug-ins pour configurer le service sur chaque hôte. Tout problème au niveau du code du plug-in est signalé par une alarme générique. L'état du service passe au vert uniquement lorsque tous les plug-ins qui y sont rattachés ne présentent plus aucun problème. Cet événement capture un sous-ensemble d'exceptions possibles. Action : utilisez l'API `resolve` pour résoudre l'alarme. Le service sera déployé.
280004	Élevé	Oui	`Alarme d'exception générique de plug-in de déploiement. (Deployment Plugin generic exception alarm.)`	Chaque service, tel que Guest Introspection, possède un ensemble de plug-ins pour configurer le service sur chaque hôte. Tout problème au niveau du code du plug-in est signalé par une alarme d'exception générique. L'état du service passe au vert uniquement lorsque tous les plug-ins qui y sont rattachés ne présentent plus aucun problème. Cet événement capture toutes les exceptions possibles. Action : utilisez l'API `resolve` pour résoudre l'alarme. Le service sera déployé.
280005	Élevé	Oui	`La VM doit être redémarrée pour que certains changements soient effectués/appliqués. (VM needs to be rebooted for some changes to be made/take effect.)`	La VM doit être redémarrée pour que certains changements soient effectués ou appliqués. Action : utilisez l'API `resolve` pour résoudre l'alarme. Cette action va redémarrer la machine virtuelle.

Événements système liés à la messagerie

Le tableau décrit les messages d'événement système liés à la messagerie dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
390001	Élevé	Oui	`Échec de la configuration de messagerie d'hôte. (Host messaging configuration failed.)`	Le bus de messages NSX est configuré après la préparation de l'hôte, une fois qu'ESX Agent Manager (EAM) a notifié NSX que les bundles VIB de NSX avaient été installés sur un hôte ESXi. Cet événement indique un échec de la configuration du bus de messages sur l'hôte. À partir de la version 6.2.3 de NSX, une icône d'erreur rouge s'affiche en regard de l'hôte concerné sous l'onglet **Installation > Préparation de l'hôte**. Action : pour les étapes de dépannage, reportez-vous au *Guide de dépannage de NSX*.
390002	Élevé	Oui	`Échec de reconfiguration de connexion de messagerie d'hôte. (Host messaging connection reconfiguration failed.)`	Dans certaines situations, lorsque NSX découvre que les informations du broker RMQ ont changé, NSX tente d'envoyer à l'hôte les nouvelles informations du broker RMQ. Si NSX ne parvient pas à envoyer les informations, cette alarme est déclenchée. Action : pour les étapes de dépannage, reportez-vous au *Guide de dépannage de NSX*.
390003	Élevé	Oui	`La configuration de la messagerie d'hôte a échoué et les notifications ont été ignorées. (Host messaging configuration failed and notifications were skipped.)`	NSX tentera à nouveau de configurer le canal de messagerie lorsqu'un hôte préparé se connectera à vCenter Server. Cet événement indique que la configuration a échoué et que les autres modules NSX qui dépendent du canal de messagerie n'ont pas été notifiés. Action : pour les étapes de dépannage, reportez-vous au *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
391002	Critique	Non	`Infrastructure de messagerie en bas sur l'hôte. (Messaging infrastructure down on host.)`	Plusieurs messages de pulsation entre NSX Manager et un hôte NSX ont été manqués. Action : pour les étapes de dépannage, reportez-vous au *Guide de dépannage de NSX*.
321100	Critique	Non	`Désactivation du compte de messagerie {account #}. Le mot de passe a expiré. (Disabling messaging account {account #}. Password has expired.)`	Un hôte ESXi, une machine virtuelle NSX Edge ou une machine virtuelle de service universelle (USVM) jouant le rôle de client du bus de messages n'a pas modifié son mot de passe Rabbit MQ dans les délais prévus, à savoir deux heures après le déploiement initial ou la préparation de l'hôte. Action : tentez d'identifier tout problème de communication entre NSX Manager et le client du bus de messages. Vérifiez que le client est en cours d'exécution. Avant de procéder à une resynchronisation ou à un redéploiement, collectez les journaux appropriés. Pour les étapes de dépannage, reportez-vous au *Guide de dépannage de NSX*.

Événements système liés à Service Composer

Le tableau décrit les messages d'événement système liés à Service Composer dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
300000	Critique	Oui	`La stratégie {#} a été supprimée suite à la suppression explicite du SecurityGroup dépendant. (Policy {#} is deleted as a result of explicit deletion of its dependent SecurityGroup.)`	Une stratégie de service a été supprimée lors de la suppression d'un groupe de sécurité dépendant. Action : envisagez de recréer la stratégie de sécurité.
300001	Élevé	Oui	`La stratégie est désynchronisée. (Policy is out of sync.)`	Une erreur s'est produite au niveau de Service Composer lors d'une tentative d'application des règles sur cette stratégie de service. Action : consultez le message d'erreur pour obtenir des indications sur les règles à modifier dans cette stratégie. Résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
300002	Élevé	Oui	`Les règles de pare-feu de cette stratégie sont désynchronisées. Aucun changement lié au pare-feu de cette stratégie ne sera émis, tant que cette alarme n'est pas résolue. (Firewall rules on this Policy are out of sync. No Firewall related changes from this policy will be pushed, until this alarm is resolved.)`	Cette erreur provient d'un problème au niveau de la configuration du pare-feu. Action : consultez le message d'erreur pour obtenir des détails sur la stratégie (et peut-être les règles) à l'origine de l'erreur. Assurez-vous que vous avez résolu l'alarme pour synchroniser la stratégie à l'aide de Service Composer ou de l'API `resolve`. Reportez-vous également à l'article indiquant comment résoudre les problèmes liés à Service Composer dans NSX 6.x (http://kb.vmware.com/kb/2132612).
300003	Élevé	Oui	`Les règles d'introspection réseau de cette stratégie sont désynchronisées. Aucun changement lié à l'introspection réseau de cette stratégie ne sera émis, tant que cette alarme n'est pas résolue. (Network Introspection rules on this Policy are out of sync. No Network Introspection related changes from this policy will be pushed, until this alarm is resolved.)`	Cette erreur provient d'un problème au niveau de la configuration d'Introspection réseau. Action : consultez le message d'erreur pour obtenir des détails sur la stratégie (et peut-être les règles) à l'origine de l'erreur. Assurez-vous que vous avez résolu l'alarme pour synchroniser la stratégie à l'aide de Service Composer ou du paramètre `action=resolve` dans l'API `systemalarms`. Reportez-vous également à l'article indiquant comment résoudre les problèmes liés à Service Composer dans NSX 6.x (http://kb.vmware.com/kb/2132612). Résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
300004	Élevé	Oui	`Les règles Guest Introspection de cette stratégie sont désynchronisées. Aucun changement lié à Guest Introspection de cette stratégie ne sera émis, tant que cette alarme n'est pas résolue. (Guest Introspection rules on this Policy are out of sync. No Guest Introspection related changes from this policy will be pushed, until this alarm is resolved.)`	Cette erreur provient d'un problème au niveau de la configuration de Guest Introspection. Action : consultez le message d'erreur pour obtenir des détails sur la stratégie (et peut-être les règles) à l'origine de l'erreur. Assurez-vous que vous avez résolu l'alarme pour synchroniser la stratégie à l'aide de Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms`. Reportez-vous également à l'article indiquant comment résoudre les problèmes liés à Service Composer dans NSX 6.x (http://kb.vmware.com/kb/2132612).
300005	Élevé	Oui	`Service Composer n'est pas synchronisé. Aucun changement de Service Composer ne sera émis vers le pare-feu/l'introspection réseau. (Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection.)`	Une erreur s'est produite au niveau de Service Composer lors de la synchronisation d'une stratégie. Aucune modification ne sera envoyée aux services d'introspection du pare-feu ou du réseau. Action : consultez le message d'erreur pour déterminer les stratégies et/ou les sections de pare-feu à modifier. Résolvez l'alarme via Service Composer ou à l'aide de l'API `resolve`.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
300006	Élevé	Oui	`Service Composer n'est pas synchronisé en raison de l'échec de la synchronisation lors de l'opération de redémarrage. (Service Composer is out of sync due to failure on sync on reboot operation.)`	Une erreur s'est produite au niveau de Service Composer lors de la synchronisation d'une stratégie au moment du redémarrage. Aucune modification ne sera envoyée aux services d'introspection du pare-feu ou du réseau. Action : consultez le message d'erreur pour déterminer les stratégies et/ou les sections de pare-feu à modifier. Résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.
300007	Élevé	Oui	`Service Composer n'est pas synchronisé en raison de la restauration de brouillons du pare-feu. Aucun changement de Service Composer ne sera émis vers le pare-feu/l'introspection réseau. (Service Composer is out of sync due to rollback of drafts from Firewall. No changes from Service Composer will be pushed to Firewall/Network Introspection.)`	Une erreur de synchronisation s'est produite au niveau de Service Composer lors du rétablissement d'ensembles de règles de pare-feu à une version antérieure. Aucune modification ne sera envoyée aux services d'introspection du pare-feu ou du réseau. Action : résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.
300008	Élevé	Oui	`Échec lors de la suppression de la section correspondant à la stratégie. (Failure while deleting section corresponding to the Policy.)`	Une erreur s'est produite au niveau de Service Composer lors de la suppression de la section de règles de pare-feu de la stratégie. Ce problème survient lorsque le gestionnaire d'un service tiers avec insertion de services NSX n'est pas joignable. Action : recherchez les problèmes au niveau de la connexion au gestionnaire de service tiers. Résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
300009	Élevé	Oui	`Échec lors de la réorganisation de la section pour refléter la modification de la priorité. (Failure while reordering section to reflect precedence change.)`	Une erreur s'est produite au niveau de Service Composer lors de la synchronisation d'une stratégie au moment du redémarrage. Aucune modification ne sera envoyée aux services d'introspection du pare-feu ou du réseau. Action : consultez le message d'erreur pour déterminer les stratégies et/ou les sections de pare-feu à modifier. Résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.
300010	Élevé	Oui	`Échec lors de l'initialisation du paramètre d'enregistrement automatique des brouillons. (Failure while initializing auto save drafts setting.)`	Une erreur s'est produite au niveau de Service Composer lors de l'initialisation des paramètres d'enregistrement automatique des brouillons. Action : consultez le message d'erreur pour déterminer les stratégies et/ou les sections de pare-feu à modifier. Résolvez l'alarme via Service Composer ou utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Événements système liés à la SVM GI

Le tableau décrit les messages d'événement système liés aux opérations de VM de service universel Guest Introspection (SVM GI) dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
295002	Majeur			NSX Manager ne reçoit aucun signal de pulsation de la part de l'USVM Guest Introspection. Action : collectez les journaux de support technique de NSX Manager et de l'USVM et ouvrez une demande de support technique.
295003	Informatif			NSX Manager reçoit des signaux de pulsation de la part de l'USVM. Action : la récupération de l'événement après l'événement 295002 est signalée.
295010	Informatif			La connexion entre l'USVM et le module hôte Guest Introspection est établie. Action : événement informatif uniquement. Aucune action n'est requise.

Événements système liés aux opérations SVM

Le tableau décrit les messages d'événement système liés aux opérations de VM de service (SVM) dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
280002	Élevé	Oui	NSX a manqué certains événements de cet agent, probablement en raison d'un redémarrage ou d'une perte de connexion temporaire avec vCenter Server. Avertissement : la résolution de cette alarme entraînera la suppression de la VM et l'émission d'une nouvelle alarme indiquant que la VM agent est manquante. Si vous la résolvez de la même manière, la VM sera redéployée. (Some of the events for this agent were missed by NSX. Probably reason could be reboot or temporary connectivity loss with vCenter Server. Warning: Resolving the alarm will delete the VM and raise another indicating agent VM is missing. Resolving same will redeploy the VM.)	Une erreur interne s'est produite au niveau d'une machine virtuelle de service déployée. Action : résolvez l'alarme en supprimant la machine virtuelle. Une seconde alarme concernant la suppression est alors générée. La résolution de la seconde alarme réinstalle la machine virtuelle. Si le redéploiement de la machine virtuelle échoue, l'alarme originale est à nouveau déclenchée. Si l'alarme réapparaît, collectez les journaux SVM en suivant la procédure décrite dans l'article de la base de connaissances http://kb.vmware.com/kb/2144624, puis contactez le support technique VMware.
280003	Élevé	Oui	NSX a manqué certains des événements de cet agent, probablement à cause d'un redémarrage ou d'une perte de connexion temporaire avec vCenter Server. Avertissement : la correction de cette alarme entraînera le redémarrage de la	Une machine virtuelle de service déployée a été redémarrée. Action : résolvez l'alarme en redémarrant la machine virtuelle. Si le redémarrage échoue, l'alarme réapparaît. Collectez les journaux SVM en suivant la procédure décrite dans l'article de la base de connaissances http://kb.vmware.com/kb/2144624, puis contactez le support technique VMware.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
			`VM. (Some of the events for this agent were missed by NSX. Probably reason could be reboot or temporary connectivity loss with vCenter Server. Warning: Resolving the alarm will restart the VM.)`	
280006	Élevé	Oui	`Échec de l'indication de l'agent comme disponible. (Failed to mark agent as available.)`	Une erreur interne s'est produite lorsque la machine virtuelle de l'agent ESX a été marquée comme disponible. Action : résolvez l'alarme à l'aide du paramètre `action=resolve` dans l'API `systemalarms`. Si l'alarme ne peut pas être résolue, collectez les journaux SVM en suivant la procédure décrite dans l'article de la base de connaissances http://kb.vmware.com/kb/2144624, puis contactez le support technique VMware.

Événements système liés à la réplication - synchronisation universelle

Le tableau décrit les messages d'événement système liés à la réplication - synchronisation universelle dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
310001	Critique	Non	`Échec de la synchronisation complète pour le type d'objet {#} sur NSX Manager {#}. (Full sync failed for object type {#} on NSX Manager {#}.)`	La synchronisation complète d'objets universels a échoué sur une instance secondaire de NSX Manager. Action : collectez les journaux de support technique pour NSX Manager, puis contactez le support technique VMware.
310003	Critique	Non	`Échec de l'opération de synchronisation universelle pour l'entité {#} sur NSX Manager {#}. (Universal sync operation failed for the entity {#} on NSX Manager {#}.)`	La synchronisation d'un objet universel vers une instance secondaire de NSX Manager dans un environnement cross-vCenter a échoué. Action : collectez les journaux de support technique pour NSX Manager, puis contactez le support technique VMware.

Événements système liés à la gestion de NSX

Le tableau décrit les messages d'événement système liés à la gestion de NSX dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
320001	Critique	Non	`L'adresse IP de NSX Manager a été attribuée à une autre machine avec l'adresse MAC. (The NSX Manager IP has been assigned to another machine with the MAC Address.)`	L'adresse IP de gestion de NSX Manager a été attribuée à une machine virtuelle qui se trouve sur le même réseau. Avant la version 6.2.3, les adresses IP en double de NSX Manager n'étaient pas détectées ou évitées. La présence de ces adresses peut engendrer des problèmes au niveau du chemin de données. Dans la version 6.2.3 et les versions ultérieures, cet événement est déclenché lorsqu'une adresse en double est détectée. Action : résolvez le problème d'adresse en double.

Événements système liés au réseau logique

Le tableau décrit les messages d'événement système liés à la mise en réseau logique.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
814	Critique	Non	`Le commutateur logique {#} n'est plus correctement configuré, certains des groupes de ports virtuels distribués de sauvegarde ayant été modifiés et/ou supprimés. (Logical Switch {#} is no longer properly configured since some of the backing distributed virtual port groups were modified and/or removed.)`	Un ou plusieurs groupes de ports DVS de sauvegarde d'un commutateur logique NSX ont été modifiés ou supprimés, ou la modification du mode du plan de contrôle du commutateur logique a échoué. Action : si l'événement a été déclenché par la suppression ou la modification d'un groupe de ports, une erreur s'affichera sur la page Commutateurs logiques de vSphere Web Client. Cliquez sur l'erreur pour créer les groupes de ports DVS manquants. Si l'événement a été déclenché en raison de l'échec de la modification du mode du plan de contrôle, effectuez à nouveau la mise à jour. Reportez-vous à la section « Mise à jour des zones de transport et des commutateurs logiques » du *Guide de mise à niveau de NSX*.
1900	Critique	Non	`Échec de l'initialisation de VXLAN sur l'hôte {0}. (VXLAN initialization failed on the host.)`	L'initialisation du VXLAN a échoué en raison de l'échec de la configuration des cartes réseau VMkernel pour le nombre de VTEP requis. NSX prépare les DVS sélectionnés par l'utilisateur pour le VXLAN et crée un groupe de ports DV destiné à être utilisé par les cartes réseau VMkernel des VTEP. L'association, la méthode d'équilibrage de charge, le MTU et l'ID VLAN sont choisis lors de la configuration de VXLAN. Les méthodes d'association et d'équilibrage de charge doivent correspondre à la configuration du DVS sélectionné pour le VXLAN. Action : examinez le fichier `vmkernel.log`. Reportez-vous également à la section « Préparation de l'infrastructure » du *Guide de dépannage de NSX*.
1901	Critique	Non	`L'initialisation du port VXLAN a échoué sur l'hôte {0}. (VXLAN port initialization failed on the host.)`	VXLAN n'a pas pu être configuré sur le port DV associé et le port a été déconnecté. NSX prépare les DVS sélectionnés par l'utilisateur pour le VXLAN et crée un groupe de ports DV destinés à être utilisés par chaque commutateur logique configuré. Action : examinez le fichier `vmkernel.log`. Reportez-vous également à la section « Préparation de l'infrastructure » du *Guide de dépannage de NSX*.
1902	Critique	Non	`L'instance VXLAN n'existe pas sur l'hôte {0}. (VXLAN instance does not exist on the host.)`	La configuration VXLAN a été reçue pour un port DV alors que le DVS sur l'hôte ESXI n'était pas encore activé pour le VXLAN. Action : examinez le fichier `vmkernel.log`. Reportez-vous également à la section « Préparation de l'infrastructure » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
1903	Critique	Non	`Le commutateur logique {#} ne peut pas fonctionner correctement, car l'interface IP de sauvegarde n'a pas pu rejoindre un groupe de multidiffusion spécifique. (Logical Switch {#} can't work properly since the backing IP interface couldn't join specific multicast group.)`	L'interface VTEP n'a pas pu rejoindre le groupe multidiffusion spécifié. Le trafic sur certains hôtes va être affecté tant que le problème n'est pas résolu. NSX utilise un mécanisme de nouvel essai (toutes les cinq secondes) pour rejoindre un groupe de multidiffusion. Action : examinez le fichier `vmkernel.log`. Reportez-vous également à la section « Préparation de l'infrastructure » du *Guide de dépannage de NSX*.
1905	Critique	Non	`La zone de transport ne doit pas être utilisée, car l'interface IP de sauvegarde ne parvient pas à acquérir une adresse IP correcte. (Transport Zone may not be used since the backing IP interface can't acquire correct IP Address.)`	Une adresse IP valide n'a pas pu être attribuée à la carte réseau VMkernel de VTEP. Tout le trafic VXLAN passant par la carte réseau VMkernel va être abandonné. Action : confirmez que DHCP est disponible sur les VLAN de transport de VXLAN si vous utilisez DHCP pour attribuer des adresses IP à des VMKNic. Reportez-vous à l'article traitant de l'échec de la préparation de l'hôte NSX avec un message d'erreur indiquant que le nombre d'adresses IP du pool d'adresses IP est insuffisant (http://kb.vmware.com/kb/2137025).
1906	Critique	Non	`La classe de superposition VXLAN est manquante sur DVS. (VXLAN overlay class is missing on DVS.)`	Les bundles VIB de NSX n'étaient pas installés lorsque le DVS a été configuré pour le VXLAN. Aucune interface VXLAN ne parviendra à se connecter au DVS. Action : reportez-vous à l'article traitant des problèmes de connectivité réseau après une mise à niveau dans l'environnement NSX/VCNS (http://kb.vmware.com/kb/2107951).
1920	Critique	Non	`Le contrôleur VXLAN {#} a été supprimé du fait de l'impossibilité de créer la connexion. Vérifiez la configuration de l'adresse IP du contrôleur et redéployez. (VXLAN Controller {#} has been removed due to the connection can't be built, please check controller IP configuration and deploy again.)`	Le déploiement du contrôleur a échoué. Action : vérifiez que l'adresse IP attribuée est joignable. Reportez-vous également à la section « NSX Controller » du *Guide de dépannage de NSX*.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
1930	Critique	Non	`Le contrôleur {#} ne peut pas établir la connexion au nœud {#} (actif={#}). État de connexion actuel = {#}. (The controller {#} cannot establish the connection to the node {#}(active={#}). Current connection status = {#}.)`	Deux nœuds de contrôleur sont déconnectés, ce qui affecte la communication entre les contrôleurs Action : reportez-vous à la section « NSX Controller » du *Guide de dépannage de NSX*.
1935	Critique	Non	`Les informations de l'hôte {#} n'ont pas pu être envoyées aux contrôleurs, car ils sont tous inactifs. La synchronisation des contrôleurs peut être nécessaire une fois qu'ils sont activés. (Host {#} information could not be sent to controllers as all controllers are inactive. Controller synchronization may be needed once controllers become active.)`	Les informations du certificat de l'hôte n'ont pas pu être envoyées au cluster de NSX Controller. Le canal de communication entre l'hôte et le cluster de contrôleurs peut se comporter de manière inattendue. Action : confirmez que l'état du cluster de NSX Controller est défini sur Normal avant de préparer un hôte ESXi. Utilisez l'API `controller sync` pour résoudre ce problème.
1937	Critique	Non	`VXLAN vmknic {#} [PortGroup = {#}] est manquant ou supprimé de l'hôte {#}. (VXLAN vmknic {#} [PortGroup = {#}] is missing or deleted from host {#}.)`	La carte réseau VMkernel de VXLAN est manquante ou a été supprimée de l'hôte. Le trafic à destination et en provenance de l'hôte va être affecté. Action : pour résoudre le problème, cliquez sur le bouton **Résoudre** dans l'onglet **Installation > Préparation du réseau logique > Transport VXLAN**.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
1939	Critique	Non	`VXLAN vmknic {#} [PortGroup = {#}] a peut-être été supprimé de l'hôte {#} ou la connexion entre l'hôte et vCenter peut rencontrer des problèmes. (VXLAN vmknic {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues.)`	NSX Manager a détecté qu'une carte réseau VMkernel de VXLAN était manquante sur Virtual Center. Cela peut être dû à des problèmes de communication entre vCenter Server et les hôtes. Par ailleurs, lorsque vCenter Server ou un hôte est redémarré, un bref laps de temps s'écoule durant lequel NSX Manager n'est pas en mesure de détecter la carte réseau VMkernel de VXLAN et marque cet événement. Après le redémarrage de vCenter Server et de l'hôte, NSX Manager vérifie à nouveau les cartes réseau VMkernel de VXLAN et efface l'événement si tout est en ordre. Action : résolvez ce problème, s'il n'est pas transitoire, en cliquant sur le bouton **Résoudre** sous l'onglet **Installation > Préparation du réseau logique > Transport VXLAN**.
1941	Critique	Non	`État de connexion de l'hôte modifié : Code d'événement : {#}, Hôte : {#} (ID : {#}), NSX Manager – Agent de pare-feu : {#}, NSX Manager – Agent de plan de contrôle : {#}, Agent de plan de contrôle – Contrôleurs : {#}. (Host Connection Status Changed: Event Code: {#}, Host: {#} (ID: {#}), NSX Manager – Firewall Agent: {#}, NSX Manager – Control Plane Agent: {#}, Control Plane Agent – Controllers: {#}.)`	NSX Manager a détecté un état défaillant pour l'une des connexions suivantes : de NSX Manager à l'agent de pare-feu de l'hôte, de NSX Manager à l'agent du plan de contrôle de l'hôte ou de l'agent de plan de contrôle de l'hôte à NSX Controller. Action : si la connexion de NSX Manager à l'agent de pare-feu de l'hôte est défaillante, consultez le journal de NSX Manager et de l'agent de pare-feu (*/var/log/vsfwd.log*) ou envoyez l'appel de l'API REST POST `https://NSX-Manager-IP-Address/api/2.0/nwfabric/configure?action=synchronize` afin de synchroniser de nouveau la connexion. Si la connexion de NSX Manager à l'agent du plan de contrôle de l'hôte est défaillante, examinez le journal de NSX Manager et de l'agent du plan de contrôle (*/var/log/netcpa.log*). Si la connexion de l'agent du plan de contrôle de l'hôte à NSX Controller est défaillante, accédez à **Networking & Security > Installation** et vérifiez l'état de la connexion de l'hôte.
1942	Critique	Non	`Le groupe de ports de sauvegarde [moid = {#}] de LogicalSwitch {#} est marqué comme manquant. (The backing portgroup [moid = {#}] of LogicalSwitch {#} is marked as missing.)`	NSX Manager a détecté que le groupe de ports de sauvegarde DV d'un commutateur logique NSX était manquant dans VirtualCenter. Action : cliquez sur le bouton **Résoudre** sous l'onglet **Installation > Préparation du réseau logique > Transport VXLAN** ou utilisez REST API (POST `https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate`) pour recréer le groupe de ports.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
1945	Critique	Non	`L'alerte de latence de disque est activée sur le périphérique {#} sur le contrôleur {#}. (The device {#} on controller {#} has the disk latency alert on.)`	NSX Manager a détecté une latence de disque élevée pour NSX Controller. Action : reportez-vous à la section « NSX Controller » du *Guide de dépannage de NSX*.
1946	Informatif	Non	`Toutes les alertes de latence de disque sur le contrôleur {0} sont désactivées. (All disk latency alerts on controller {0} are off.)`	NSX Manager ne détecte plus la latence de disque élevée sur un contrôleur. Action : événement informatif uniquement. Aucune action n'est requise.
1947	Critique	Non	`Le contrôleur de la machine virtuelle est hors tension sur vCenter. (Controller Virtual Machine is powered off on vCenter.)`	NSX Manager a détecté qu'une VM NSX Controller a été mise hors tension à partir de Virtual Center. L'état du cluster de contrôleurs peut passer à Déconnecté, ce qui affecte toutes les opérations nécessitant un cluster en état de fonctionnement. Action : cliquez sur le bouton **Résoudre** pour le contrôleur sous l'onglet **Installation > Gestion** ou appelez l'API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` pour mettre la VM du contrôleur sous tension.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
1948	Critique	Non	`Le contrôleur de la machine virtuelle est supprimé de vCenter. (Controller Virtual Machine is deleted from vCenter.)`	NSX Manager a détecté qu'une VM NSX Controller a été supprimée de Virtual Center. L'état du cluster de contrôleurs peut passer à Déconnecté, ce qui affecte toutes les opérations nécessitant un cluster en état de fonctionnement. Action : cliquez sur le bouton **Résoudre** pour le contrôleur sous l'onglet **Installation > Gestion** ou appelez l'API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` pour supprimer l'état du contrôleur dans la base de données NSX Manager.
1952	Critique	Non	`Le groupe de ports VXLAN [moid = dvportgroup-xx] et le DVS associé ont des stratégies d'association différentes. (The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies.)`	NSX Manager a détecté qu'une stratégie d'association d'un groupe de ports VXLAN était différente de la stratégie d'association du DVS associé. Cela peut entraîner un comportement imprévisible. Action : reconfigurez le groupe de ports VXLAN ou DVS, afin qu'ils aient la même stratégie d'association.

Événements système liés au pare-feu d'identité

Le tableau décrit les messages d'événement système liés au pare-feu d'identité (IDFW) dont le niveau de gravité peut être majeur, critique ou élevé.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
395000	Critique	Non	`Le journal SecurityLog du serveur du journal des événements du contrôleur de domaine est plein. (SecurityLog on Domain Controller Eventlog Server is Full.)`	Le journal de sécurité du serveur de journaux des événements Active Directory est plein. IDFW cessera de fonctionner s'il est configuré pour utiliser les données récupérées dans les journaux. Action : contactez l'administrateur du serveur Active Directory et augmentez la taille du journal de sécurité, effacez le journal de sécurité ou archivez-le.

Événements système liés à la préparation de l'hôte

Le tableau décrit tous les messages d'événement système liés à la préparation de l'hôte.

Note Plusieurs événements ESX Agent Manager mappent à un événement unique sur NSX.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Informatif	Oui	`Un module VIB a été téléchargé vers l'hôte {hostID}, mais ne sera pas entièrement installé tant que l'hôte {hostID} n'est pas placé en mode de maintenance. (A VIB module has been uploaded to the host {hostID}, but will not be fully installed until the host {hostID} has been put in maintenance mode.)`	ESX Agent Manager place l'hôte en mode de maintenance. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Critique	Oui	`Une machine virtuelle d'agent doit être déployée sur un hôte, mais elle ne peut pas être déployée, car vSphere ESX Agent Manager ne parvient pas à accéder au module OVF pour l'agent. Cela se produit généralement, car le serveur Web fournissant le module OVF est arrêté. Le serveur Web est souvent interne à la solution qui a créé l'agence. (An agent virtual machine is expected to be deployed on a host, but the agent virtual machine cannot be deployed because the vSphere ESX Agent Manager is unable to access the OVF package for the agent. This typically happens because the Web server providing the OVF package is down. The`	ESX Agent Manager redéploie l'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
			Web server is often internal to the solution that created the Agency.)	
270000	Critique	Oui	Un module VIB d'agent doit être déployé sur un hôte, mais le module VIM ne peut pas être déployé, car vSphere ESX Agent Manager ne parvient pas à accéder au module VIB pour l'agent. Cela se produit généralement, car le serveur Web fournissant le module VIB est arrêté. Le serveur Web est souvent interne à la solution qui a créé l'agence. (An agent VIB module is expected to be deployed on a host, but the VIM module cannot be deployed because the vSphere ESX Agent Manager is unable to access the VIB package for the agent. This typically happens because the Web server providing the VIB package is down. The Web server is often internal to the solution that created the Agency.)	ESX Agent Manager réinstalle le module VIB. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent n'a pas pu être déployé, car il n'était pas compatible avec l'hôte {hostID}. (An agent virtual machine is expected to be deployed on a host, but the agent could not be deployed because it was incompatible with the host {hostID}.)`	vSphere ESX Agent Manager redéploie l'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme. Toutefois, le problème est susceptible de durer tant que vous ne mettez pas à niveau l'hôte ou la solution, de sorte que l'agent devienne compatible avec l'hôte.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être mise sous tension, mais il n'y a aucune adresse IP libre dans le pool d'adresses IP de machine virtuelle de l'agent. (An agent virtual machine is expected to be powered on, but there are no free IP addresses in the agent's pool of virtual machine IP addresses.)`	Action : pour résoudre le problème, libérez des adresses IP ou ajoutez davantage d'adresses IP au pool d'adresses IP, puis utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être déployée sur un hôte, mais elle n'a pas pu être déployée, car l'hôte {hostID} ne dispose pas de ressources de CPU ou de mémoire libres suffisantes. (An agent virtual machine is expected to be deployed on a host, but the agent virtual machine could not be deployed because the host {hostID} does not have enough free CPU or memory resources.)`	ESX Agent Manager redéploie la machine virtuelle d'agent. Toutefois, le problème est susceptible de durer tant que suffisamment de ressources de CPU et de mémoire ne sont pas mises à disposition. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être déployée sur un hôte, mais elle n'a pas pu être déployée, car la banque de données d'agent de l'hôte agent ne disposait pas d'un espace libre suffisant. (An agent virtual machine is expected to be deployed on a host, but the agent virtual machine could not be deployed because the host's agent datastore did not have enough free space.)`	ESX Agent Manager redéploie la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme. Toutefois, le problème est susceptible de durer tant que : Vous ne libérez pas de l'espace sur la banque de données de machine virtuelle d'agent de l'hôte. -Ou- Vous ne configurez pas une nouvelle banque de données de machine virtuelle d'agent avec un espace libre suffisant.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être mise sous tension, mais elle est mise hors tension, car il n'y a aucune adresse IP définie sur le réseau de machine virtuelle de l'agent. (An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off because there are no IP addresses defined on the agent's virtual machine network.)`	Action : créez un pool d'adresses IP sur le réseau de machine virtuelle de l'agent et utilisez le paramètre `action=resolve` dans l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car la banque de données d'agent n'a pas été configurée sur l'hôte {hostID}. (An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host {hostID}.)	Action : vous devez configurer la banque de données de machine virtuelle d'agent sur l'hôte.
270000	Élevé	Oui	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car le réseau d'agent n'a pas été configuré sur l'hôte. (An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent network has not been configured on the host.)	Action : vous devez configurer le réseau de machine virtuelle d'agent sur l'hôte.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car le réseau d'agent n'a pas été configuré sur l'hôte. L'hôte doit être ajouté à l'un des réseaux répertoriés dans customAgentVmNetwork. (An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent network has not been configured on the host. The host needs to be added to one of the networks listed in customAgentVmNetwork.)	Action : vous devez ajouter un des réseaux *customAgentVmNetwork* à l'hôte.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car la banque de données d'agent n'a pas été configurée sur l'hôte. L'hôte doit être ajouté à l'une des banques de données répertoriées dans customAgentVmDatastore. (An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host. The host needs to be added to one of the datastores listed in customAgentVmDatastore.)`	Vous devez ajouter une des banques de données nommées *customAgentVmDatastore* à l'hôte.
270000	Élevé	Oui	`La solution qui a créé l'agence n'est plus enregistrée auprès de vCenter Server. (The solution that created the agency is no longer registered with the vCenter server.)`	ESX Agent Manager supprime l'agence. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Un commutateur dvFilter existe sur un hôte, mais aucun agent sur l'hôte ne dépend de dvFilter. Cela se produit généralement si un hôte est déconnecté lorsque la configuration d'une agence a été modifiée. (A dvFilter switch exists on a host but no agents on the host depend on dvFilter. This typically happens if a host is disconnected when an agency configuration changed.)`	ESX Agent Manager supprime *dvFilterSwitch*. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être provisionnée sur un hôte, mais elle a échoué, car le provisionnement du module OVF a échoué. Le provisionnement est peu susceptible d'aboutir tant que la solution qui fournit le module OVF n'est pas mise à niveau ou corrigée afin de fournir un module OVF valide pour la machine virtuelle d'agent. (An Agent virtual machine is expected to be provisioned on a host, but it failed to do so because the provisioning of the OVF package failed. The provisioning is unlikely to succeed until the solution that provides the OVF package has been upgraded or patched to provide a valid OVF package for the agent virtual machine.)`	ESX Agent Manager retente le provisionnement OVF. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être mise sous tension, mais une propriété OVF est manquante ou a une valeur non valide. (An agent virtual machine needs to be powered on, but an OVF property is either missing or has an invalid value.)`	Action : mettez à jour l'environnement OVF dans la configuration de l'agent utilisée pour provisionner la machine virtuelle d'agent.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent a été trouvée dans l'inventaire de vCenter qui n'appartient pas à aucune agence dans cette instance du serveur vSphere ESX Agent Manager. (An agent virtual machine has been found in the vCenter inventory that does not belong to any agency in this vSphere ESX Agent Manager server instance.)`	ESX Agent Manager se met hors tension (s'il est sous tension) et supprime la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Un module VIB requiert que l'hôte soit en mode de maintenance, mais vSphere ESX Agent Manager ne parvient pas à mettre l'hôte en mode de maintenance. Cela peut se produire si des machines virtuelles s'exécutant sur l'hôte ne peuvent pas être déplacées et doivent être arrêtées pour que l'hôte puisse entrer en mode de maintenance. (A VIB module requires the host to be in maintenance mode, but the vSphere ESX Agent Manager is unable to put the host in maintenance mode. This can happen if there are virtual machines running on the host that cannot be moved and must be stopped before the host can enter maintenance mode.)`	ESX Agent Manager tente de mettre l'hôte en mode de maintenance. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme. Toutefois, le problème est susceptible de durer tant que vous n'effectuez pas la mise hors tension ou le déplacement des machines virtuelles pour mettre l'hôte en mode de maintenance.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Critique	Oui	`Un module VIB doit être installé sur un hôte, mais l'installation ci a échoué, car le module VIB est dans un format non valide. L'installation est peu susceptible d'aboutir tant que la solution fournissant le bundle n'est pas été mise à niveau ou corrigée afin de fournir un module VIB valide. (A VIB module is expected to be installed on a host, but it failed to install since the VIB package is in an invalid format. The installation is unlikely to succeed until the solution providing the bundle has been upgraded or patched to provide a valid VIB package.)`	ESX Agent Manager retente l'installation du module VIB. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Un module VIB doit être installé sur un hôte, mais il n'a pas été installé. En général, un problème plus spécifique (une sous-classe de ce problème) indique la raison particulière de l'échec de l'installation du module VIB. (A VIB module is expected to be installed on a host, but it has not been installed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why the VIB module installation failed.)`	ESX Agent Manager retente l'installation du module VIB. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Informatif	Oui	`Un module VIB a été téléchargé vers l'hôte, mais ne sera pas activé tant que l'hôte n'est pas redémarré. (A VIB module has been uploaded to the host, but will not be activated until the host is rebooted.)`	ESX Agent Manager met l'hôte en mode de maintenance et le redémarre. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`L'installation d'un module VIB a échoué, car l'installation automatique par vSphere ESX Agent Manager n'est pas autorisée sur l'hôte. (A VIB module failed to install, but failed to do so because automatic installation by vSphere ESX Agent Manager is not allowed on the host.)`	Action : accédez à vSphere Update Manager et installez les bulletins requis sur l'hôte ou ajoutez les bulletins au profil d'image de l'hôte. Pour plus de détails, consultez la documentation de vSphere.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`La désinstallation d'un module VIB a échoué, car la désinstallation automatique par vSphere ESX Agent Manager n'est pas autorisée sur l'hôte. (A VIB module failed to uninstall, but failed to do so because automatic uninstallation by vSphere ESX Agent Manager is not allowed on the host.)`	Action : accédez à vSphere Update Manager et désinstallez les bulletins requis sur l'hôte ou ajoutez les bulletins au profil d'image de l'hôte. Pour plus de détails, consultez la documentation de vSphere.
270000	Élevé	Oui	`Une machine virtuelle d'agent est endommagée. (An agent virtual machine is corrupt.)`	ESX Agent Manager supprime et reprovisionne la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme. Pour résoudre le problème manuellement : résolvez le problème lié au fichier manquant et mettez la machine virtuelle d'agent sous tension.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être supprimée d'un hôte, mais elle n'a pas été supprimée. En général, un problème plus spécifique (une sous-classe de ce problème) indique la raison particulière pour laquelle vSphere ESX Agent Manager n'a pas pu supprimer la machine virtuelle d'agent, par exemple l'hôte est en mode de maintenance, hors tension ou en veille. (An agent virtual machine is expected to be removed from a host, but the agent virtual machine has not been removed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why vSphere ESX Agent Manager was unable to remove the agent virtual machine, such as the host is in maintenance mode, powered off or in standby mode.)`	ESX Agent Manager redéploie l'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Une machine virtuelle d'agent est un modèle de machine virtuelle. (An agent virtual machine is a virtual machine template.)`	ESX Agent Manager convertit le modèle de machine virtuelle d'agent en machine virtuelle. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être déployée sur un hôte, mais elle n'a pas été déployée. En général, un problème plus spécifique (une sous-classe de ce problème) indique la raison particulière pour laquelle vSphere ESX Agent Manager n'a pas pu déployer l'agent, par exemple impossible d'accéder au module OVF pour l'agent ou une configuration d'hôte est manquante. Ce problème peut également se produire si la machine virtuelle d'agent est supprimée explicitement de l'hôte. (An agent virtual machine is expected to be deployed on a host, but the agent virtual machine has not been deployed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why vSphere ESX Agent Manager was unable to deploy the agent, such as being unable to access the OVF package for the agent or a missing host configuration. This issue can also happen if the agent virtual machine is explicitly deleted from the host.)`	ESX Agent Manager redéploie la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être mise sous tension, mais elle est hors tension. ( An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off.)`	ESX Agent Manager met sous tension la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être mise hors tension, mais elle est hors tension. (An agent virtual machine is expected to be powered off, but the agent virtual machine is powered off.)`	ESX Agent Manager met hors tension la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit être mise sous tension, mais elle est interrompue. (An agent virtual machine is expected to be powered on, but the agent virtual machine is suspended.)`	ESX Agent Manager met sous tension la machine virtuelle d'agent. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Une machine virtuelle d'agent doit se trouver dans un dossier de machine virtuelle d'agent désigné, mais se trouve dans un autre dossier. (An agent virtual machine is expected to be located in a designated agent virtual machine folder, but is found in a different folder.)`	ESX Agent Manager replace la machine virtuelle d'agent dans le dossier d'agent désigné. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.

Code d'événement	Gravité de l'événement	Alarme déclenchée	Message d'événement	Description
270000	Élevé	Oui	`Une machine virtuelle d'agent doit se trouver dans un pool de ressources de machine virtuelle d'agent désigné, mais se trouve dans un pool de ressources différent. (An agent virtual machine is expected to be located in a designated agent virtual machine resource pool, but is found in a different resource pool.)`	ESX Agent Manager replace la machine virtuelle d'agent dans le pool de ressources d'agent désigné. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.
270000	Élevé	Oui	`Alarme EAM reçue. (EAM alarm received.)`	ESX Agent Manager a détecté un problème au niveau d'une installation ou d'une mise à niveau de NSX, en lien avec les modules VIB de NSX ou avec les machines virtuelles de service. Action : cliquez sur l'option **Résoudre (Resolve)** dans l'onglet **Préparation de l'hôte (Host Preparation)** ou utilisez le paramètre `action=resolve` de l'API `systemalarms` pour résoudre l'alarme.