Eventos del sistema y de registro de NSX

Actualización 4
Modificado el 10 de agosto de 2017
VMware NSX for vSphere 6.3

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

https://docs.vmware.com/es/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Eventos del sistema y de registro de NSX

En el documento *Eventos del sistema y de registro de NSX* se describen los mensajes de registro, los eventos y las alarmas del sistema VMware NSX® for vSphere® mediante la interfaz de usuario de NSX Manager y vSphere Web Client.

Público objetivo

Este manual está destinado a quienes deseen utilizar NSX o solucionar los problemas relacionados en un entorno de VMware vCenter. La información de este manual está escrita para administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos. En este manual se da por sentado que está familiarizado con VMware vSphere, incluidos VMware ESXi, vCenter Server y vSphere Web Client.

Glosario de publicaciones técnicas de VMware

Publicaciones técnicas de VMware proporciona un glosario de términos que podrían resultarle desconocidos. Si desea ver las definiciones de los términos que se utilizan en la documentación técnica de VMware, acceda a la página http://www.vmware.com/support/pubs.

Eventos del sistema, alarmas y registros 1

Puede usar los eventos del sistema, las alarmas y los registros para supervisar el estado y la seguridad del entorno de NSX y solucionar problemas.

Este capítulo cubre los siguientes temas:

Eventos del sistema

Los eventos del sistema son registros de las acciones del sistema. Cada evento tiene un nivel de gravedad, como informativo o crítico, para indicar la importancia del evento. Los eventos del sistema también se envían como capturas SNMP para que cualquier software de administración SNMP pueda supervisar los eventos del sistema de NSX.

Ver el informe de eventos del sistema

Desde vSphere Web Client puede ver los eventos del sistema para todos los componentes administrados por NSX Manager.

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Inventario de redes y seguridad** (Networking & Security Inventory), haga clic en **NSX Managers**.

3 Haga clic en una instancia de NSX Manager en la columna **Nombre** (Name) y, a continuación, en la pestaña **Supervisar** (Monitor).

4 Haga clic en la pestaña **Eventos del sistema** (System Events).

Puede hacer clic en las flechas de los encabezados de las columnas para ordenar eventos, o utilizar el cuadro de texto **Filtrar** (Filter) para filtrar eventos.

Formato de un evento del sistema

Si especifica un servidor syslog, NSX Manager envía todos los eventos del sistema al servidor syslog.

Estos mensajes tienen un formato similar al mensaje que se muestra a continuación:

```
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
```

El evento del sistema incluye la información siguiente.

```
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.
```

Alarmas

Las alarmas son notificaciones que se activan en respuesta a un evento, a un conjunto de condiciones o al estado de un objeto. En el panel de control de NSX y en otras pantallas de la interfaz de usuario de vSphere Web Client se muestran alarmas así como otras alertas.

La API `GET api/2.0/services/systemalarms` permite ver las alarmas de los objetos de NSX.

NSX admite dos métodos para utilizar una alarma:

- La alarma corresponde a un evento del sistema y tiene una resolución asociada que intentará solucionar el problema que activa la alarma. Este enfoque está diseñado para la implementación de tejido de red y seguridad (por ejemplo, EAM, bus de mensajería, complemento de implementación) y también es compatible con Service Composer. Estas alarmas utilizan el código de evento como código de alarma. Para obtener más información detallada, consulte el documento *Eventos del sistema y de registro de NSX*.
- Las alarmas de notificaciones de Edge tienen la estructura de par de alarma de activación y resolución. Este método es compatible con varias funciones de Edge, entre ellas, VPN de IPsec, equilibrador de carga, alta disponibilidad, comprobación de estado, sistema de archivos de Edge y reserva de recursos. Estas alarmas utilizan un código de alarma único que no es el mismo que el código de evento. Para obtener más información detallada, consulte el documento *Eventos del sistema y de registro de NSX*.

Por lo general, el sistema elimina automáticamente una alarma si la condición de error se rectifica. Algunas alarmas no se borran automáticamente al actualizar la configuración. Una vez resuelto el problema, deberá borrar las alarmas de forma manual.

A continuación se muestra un ejemplo de la API que puede utilizar para borrar las alarmas.

Puede obtener alarmas para un origen específico, por ejemplo, un clúster, un host, un grupo de recursos, un grupo de seguridad o NSX Edge. Puede ver las alarmas para un origen mediante *sourceId*:

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

Puede resolver todas las alarmas para un origen mediante *sourceId*:

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

Puede ver las alarmas de NSX, entre ellas, el bus de mensajería, el complemento de implementación, Service Composer y las alarmas de Edge:

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

Puede ver una alarma específica de NSX mediante *alarmId*:

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

Puede resolver una alarma específica de NSX mediante *alarmId*:

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

Para obtener más información sobre la API, consulte la *Guía de NSX API*.

Formato de una alarma

El formato de una alarma se puede ver a través de una API.

El formato de una alarma incluye la información siguiente.

```
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.
```

Alarmas de Guest Introspection

Las alarmas indican al administrador de vCenter Server los eventos de Guest Introspection que requieren atención. Las alarmas se cancelan automáticamente en caso de que el estado de la alarma ya no esté presente.

Las alarmas de vCenter Server pueden mostrarse sin un complemento personalizado de vSphere. Consulte la *Guía de administración de vCenter Server* sobre eventos y alarmas.

Tras registrarse como una extensión de vCenter Server, NSX Manager define las reglas que crean y eliminan alarmas, en función de los eventos provenientes de los tres componentes de Guest Introspection: SVM, módulo de Guest Introspection y Thin Agent. Las reglas pueden personalizarse. Para obtener instrucciones sobre cómo crear nuevas reglas personalizadas para las alarmas, consulte la documentación de vCenter Server. En algunos casos, hay varias causas posibles para la alarma. En las tablas que figuran a continuación se enumeran las posibles causas y las acciones correspondientes para corregirlas.

Alarmas de host

Los eventos que afectan el estado de mantenimiento del módulo Guest Introspection generan alarmas de host.

Tabla 1-1. Errores (marcados en rojo)

Causa posible	Acción
El módulo Guest Introspection se instaló en el host, pero ya no informa el estado a NSX Manager.	1 Asegúrese de que Guest Introspection se esté ejecutando. Para ello, inicie sesión en el host y escriba el comando `/etc/init.d/vShield-Endpoint-Mux start`. 2 Asegúrese de que la red se haya configurado correctamente para que Guest Introspection pueda conectarse a NSX Manager. 3 Reinicie NSX Manager.

Alarmas de SVM

Las alarmas de SVM son generadas por eventos que afectan el estado de mantenimiento de SVM.

Tabla 1-2. Alarmas rojas de SVM

Problema	Acción
No coincide la versión del protocolo con el módulo de Guest Introspection.	Asegúrese de que el módulo de Guest Introspection y SVM tengan un protocolo compatible con cada uno.
Guest Introspection no pudo establecer una conexión con SVM.	Asegúrese de que SVM esté encendida y que la red esté configurada correctamente.
La SVM no informa su estado aunque los invitados están conectados.	Error interno. Póngase en contacto con su representante de soporte técnico de VMware.

Registros de los hosts y de NSX

Puede usar los registros que se encuentran en varios componentes de NSX y en los hosts para detectar y solucionar problemas.

Para obtener la lista de los archivos de registro de los hosts y de NSX, consulte la sección sobre la preparación de la infraestructura en la *Guía para solucionar problemas de NSX*.

Registros de auditoría

En los registros de auditoría se encuentran todas las acciones de los usuarios que inician sesión en NSX Manager.

Ver el registro de auditoría

La pestaña **Registros de auditoría** (Audit Logs) proporciona una vista de las acciones realizadas por todos los usuarios de NSX Manager. NSX Manager conserva hasta 100.000 de registros de auditoría.

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Inventario de redes y seguridad** (Networking & Security Inventory), haga clic en **NSX Managers**.

3 En la columna **Nombre** (Name), haga clic en un servidor NSX y, a continuación, en la pestaña **Supervisar** (Monitor).

4 Haga clic en la pestaña **Registros de auditoría** (Audit Logs).

5 Cuando hay detalles disponibles sobre un registro de auditoría, se puede hacer clic en el texto de la columna **Operación** (Operation) de ese registro. Para ver los detalles de un registro de auditoría, haga clic en el texto de la columna **Operación** (Operation).

6 En **Detalles de cambios en los registros de auditoría** (Audit Log Change Details), seleccione **Filas con cambios** (Changed Rows) para ver solo aquellas propiedades cuyos valores cambiaron en la operación de este registro de auditoría.

Configurar un servidor syslog

Puede configurar un servidor syslog para que sea un repositorio de los registros de los hosts y los componentes de NSX.

Configurar un servidor syslog para NSX Manager

Si especifica un servidor syslog, NSX Manager envía todos los registros de auditoría y los eventos del sistema al servidor syslog.

Los datos de Syslog son útiles para solucionar problemas y revisar los datos registrados durante la instalación y la configuración.

NSX Edge es compatible con dos servidores syslog. NSX Manager y las instancias de NSX Controller son compatibles con un servidor syslog.

Procedimiento

1 Inicie sesión en el dispositivo virtual NSX Manager.

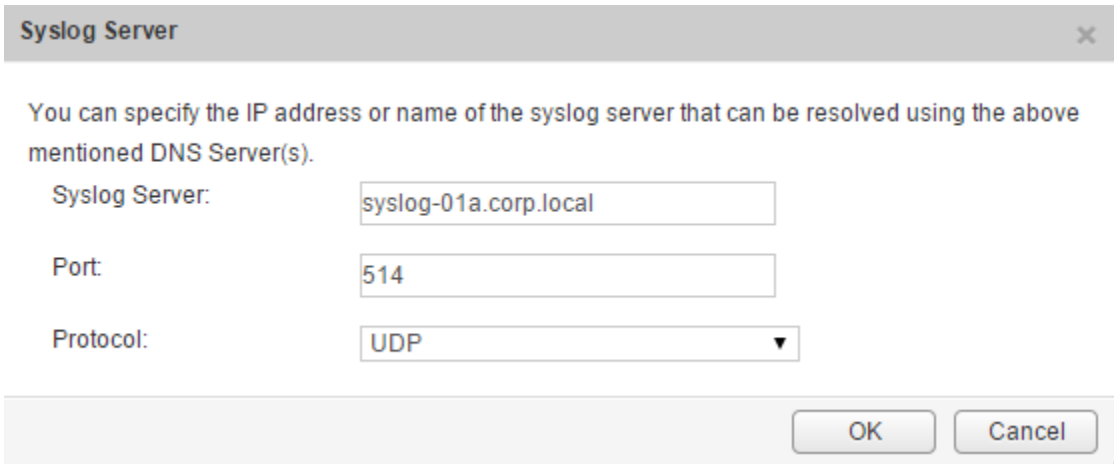
En un explorador web, desplácese hasta la GUI del dispositivo NSX Manager en https://<nsx-manager-ip> o https://<nsx-manager-hostname> e inicie sesión como administrador con la contraseña que configuró al instalar NSX Manager.

2 En la página de inicio, haga clic en **Administrar configuración de dispositivos (Manage Appliance Settings) > General (General)**.

3 Haga clic en **Editar** (Edit) junto a **Servidor syslog** (Syslog Server).

4 Escriba el nombre del host o la dirección IP, el puerto y el protocolo del servidor syslog.

Por ejemplo:



5 Haga clic en **Aceptar** (OK).

Se habilita el registro remoto en NSX Manager y los registros se almacenan en el servidor syslog independiente.

Configure los servidores de Syslog para NSX Edge

Puede configurar uno o dos servidores Syslog remotos. Los eventos y registros de NSX Edge relacionados con eventos de firewall que circulan desde dispositivos NSX Edge son enviados a los servidores Syslog.

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Instancias de NSX Edge** (NSX Edges).

3 Haga doble clic en una instancia de NSX Edge.

4 Haga clic en la pestaña **Administrar** (Manage) y seleccione la pestaña **Configuración** (Settings).

5 En el panel **Detalles** (Details), haga clic en **Cambiar** (Change) junto a los servidores Syslog.

6 Escriba la dirección IP de ambos servidores Syslog remotos y seleccione el protocolo.

7 Haga clic en **Aceptar** (OK) para guardar la configuración.

Recopilar los registros de soporte técnico

En algunas ocasiones, es posible que necesite recopilar los registros de soporte técnico de los hosts y los componentes de NSX para informar a VMware sobre algún problema.

Para recopilar registros de soporte técnico de los hosts, ejecute el comando `export host-tech-support` (consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*).

Descargar registros de soporte técnico para NSX

Es posible descargar los registros del sistema NSX Manager y de Web Manager en el escritorio.

Procedimiento

1 Inicie sesión en el dispositivo virtual de NSX Manager.

2 En Administración de dispositivos (Appliance Management), haga clic en **Administrar configuración de dispositivos** (Manage Appliance Settings).

3 Haga clic en  y, a continuación, en **Descargar registro de soporte técnico** (Download Tech Support Log).

4 Haga clic en **Descargar** (Download).

5 Una vez listo el registro, haga clic en **Guardar** (Save) para descargar el registro en el escritorio.

Se comprime el registro y tiene la extensión de archivo `.gz`.

Qué hacer a continuación

Puede abrir el registro con una utilidad de descompresión; para ello, busque **Todos los archivos** (All Files) en el directorio en el que guardó el archivo.

Descargar registros de soporte técnico para NSX Controller

Puede descargar los registros de soporte técnico para cada instancia de NSX Controller. Estos registros específicos del producto contienen información de diagnóstico para su análisis.

Para recopilar registros de NSX Controller:

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).

3 En **Administración** (Management), seleccione el controlador de la que quiera descargar los registros.

4 Haga clic en **Descargar registros de soporte técnico** (Download tech support logs).

5 Haga clic en **Descargar** (Download).

NSX Manager comienza a descargar el registro de NSX Controller y adquiere el bloqueo.

NOTA: Descargue los registros de NSX Controller de uno en uno. Una vez que descargara el primero, comience a descargar el otro. Si descarga registros de varios controladores al mismo tiempo, podría producirse un error.

---

6 Una vez listo el registro, haga clic en **Guardar** (Save) para descargar el registro en el escritorio.

El registro se comprime y tiene la extensión de archivo `.gz`.

Ahora puede analizar los registros descargados.

Qué hacer a continuación

Si quiere actualizar la información de diagnóstico para el soporte técnico de VMware, consulte el artículo 2070100 de la Knowledge Base.

Descargar registros de soporte técnico para NSX Edge

Puede descargar los registros de soporte técnico para cada instancia de NSX Edge. Si está habilitado el modo de alta disponibilidad para la instancia de NSX Edge, se descargan los registros de soporte de ambas máquinas virtuales de NSX Edge.

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **Instancias de NSX Edge** (NSX Edges).

3 Seleccione una instancia de NSX Edge.

4 Haga clic en el icono **Más acciones** (More Actions) () y seleccione **Descargar registros de soporte técnico** (Download Tech Support Logs).

5 Una vez generados los registros de soporte técnico, haga clic en **Descargar** (Download).

6 En el cuadro de diálogo Seleccionar ubicación para la descarga (Select location for download), desplácese hasta el directorio en el que desea guardar el archivo de registro.

7 Haga clic en **Guardar** (Save).

8 Haga clic en **Cerrar** (Close).

Eventos del sistema 2

Todos los componentes de NSX notifican eventos del sistema. Estos eventos pueden ayudar a supervisar el estado y la seguridad del entorno, así como a solucionar problemas.

Cada mensaje de evento tiene la siguiente información:

- Código de evento único
- Nivel de gravedad
- Descripción del evento y, si se aplican, acciones recomendadas.

Recopilar los registros de soporte técnico y ponerse en contacto con el soporte de VMware

En algunos eventos, la acción recomendada incluye recopilar los registros de soporte técnico y ponerse en contacto con el equipo de soporte de VMware.

- Para recopilar los registros de soporte técnico de NSX Manager, consulte "Descargar registros de soporte técnico para NSX," página 12.
- Para recopilar los registros de soporte técnico de NSX Edge, consulte "Descargar registros de soporte técnico para NSX Edge," página 13.
- Para recopilar los registros de soporte técnico de los hosts, ejecute el comando `export host-tech-support` (consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*).
- Para ponerse en contacto con el soporte de VMware, consulte cómo registrar una solicitud de soporte en My VMware (http://kb.vmware.com/kb/2006985).

Realizar una sincronización forzada en NSX Edge

En algunos eventos, la acción recomendada incluye realizar una sincronización forzada en NSX Edge. Para obtener más información, consulte cómo forzar la sincronización de NSX Edge con NSX Manager en la *Guía de administración de NSX*. La sincronización forzada es una operación interruptora y reinicia la máquina virtual de NSX Edge.

Nivel de gravedad de los eventos del sistema

Cada evento tiene uno de los siguientes niveles de gravedad:

- Informativo
- Bajo
- Mediano

- Importante
- Crítica
- Alta

En los siguientes temas se documentan los mensajes de eventos del sistema que tienen una gravedad alta, crítica o importante y proceden de varios componentes.

Este capítulo cubre los siguientes temas:

Eventos del sistema de seguridad

En la tabla se explican los mensajes de eventos del sistema para la seguridad de gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
11002	Crítica	No	Unable to connect to vCenter Server. Bad username / password.	Error al configurar vCenter Server. Acción: compruebe que la configuración de vCenter Server sea adecuada y que se proporcionen las credenciales correctas. Consulte cómo registrar vCenter Server con NSX Manager en la *Guía de administración de NSX* y cómo conectar NSX Manager a vCenter Server en la *Guía para solucionar problemas de NSX*.
11006	Crítica	No	Lost vCenter Server connectivity.	Se perdió la conexión a vCenter Server. Acción: investigue los problemas de conectividad con vCenter Server. Consulte los apartados sobre cómo conectar NSX Manager a vCenter Server y sobre cómo solucionar los problemas de NSX Manager en la *Guía para solucionar problemas de NSX*.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
230000	Crítica	No	SSO Configuration Task on NSX Manager failed.	Error en la configuración de Single Sign-On (SSO). Las razones incluyen credenciales no válidas, una configuración no válida o que el tiempo de espera de la sincronización expiró. Acción: revise el mensaje de error y vuelva a configurar el SSO. Consulte "Configurar inicio de sesión único" en *Guía de administración de NSX*. Consulte también "Error al configurar el servicio de búsqueda de SSO" en la *Guía para solucionar problemas de NSX*.
230002	Crítica	No	SSO STS Client disconnected.	Se produjo un error al registrar NSX Manager en el servicio SSO o se perdió la conectividad a dicho servicio. Acción: busque problemas de conectividad, como credenciales no válidas, problemas por falta de sincronización y problemas de conectividad a la red. Este evento también puede suceder debido a problemas técnicos de VMware. Consulte los artículos de la KB "Los certificados SSL del servicio STS no se pueden verificar" (http://kb.vmware.com/kb/2121696) y "Error al registrar NSX Manager al servicio de búsqueda con el controlador externo del servicio de plataforma (PSC) con el siguiente error: no se verificó la cadena de certificados del servidor (server certificate chain not verified)" (http://kb.vmware.com/kb/2132645).
240000	Crítica	No	Added an entry {0} to authentication black list.	Un usuario con una dirección IP específica intenta iniciar 10 veces seguidas la sesión y, al no conseguirlo en ningún intento, se bloquea durante 30 minutos. Acción: investigue si existe algún problema de seguridad.

Eventos del sistema del firewall distribuido

En la tabla se explican los mensajes de eventos del sistema del firewall distribuido que tienen una gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301001	Crítica	No	Filter config update failed on host.	Se produjo un error en el host al recibir o analizar la configuración del filtro o al abrir el dispositivo */dev/dvfiltertbl*. Acción: consulte el par clave-valor para obtener más contexto y la razón del error, que podría ser, entre otras, que la versión de VIB no coincide entre NSX Manager y los hosts preparados, y que existen problemas de actualización inesperados. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301002	Importante	No	Filter config not applied to vnic.	No se pudo aplicar la configuración del filtro a vNIC. Posible causa: error al abrir, analizar o actualizar la configuración del filtro. Este error no debería ocurrir con el firewall distribuido, pero puede suceder en escenarios Network Extensibility (NetX). Acción: recopile los paquetes de soporte técnico de ESXi y NSX Manager, y póngase en contacto con el equipo de soporte técnico de VMware.
301031	Crítica	No	Firewall config update failed on host.	No se pudo recibir, analizar ni actualizar la configuración del firewall. El valor clave tendrá información de contexto, como el número de generación y otro tipo de información de depuración. Acción: verifique que se realizó el procedimiento de preparación del host. Inicie sesión en el host y recopile el archivo `/var/log/vsfwd.log` y, a continuación, fuerce la sincronización de la configuración del firewall con la API `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` (consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*). Si se sigue produciendo un error al actualizar la configuración del firewall distribuido en el host, recopile los registros de soporte técnico del host y de NSX Manager, y póngase en contacto con el soporte técnico de VMware.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301032	Importante	No	Failed to apply firewall rule to vnic.	No se pudo aplicar la regla del firewall a vNIC. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware. Compruebe que los registros del host (*vmkernel.log* y *vsfwd.log*) incluyan el periodo de tiempo en el que se aplicó la configuración del firewall a la vNIC.
301041	Crítica	No	Container configuration update failed on host.	Se produjo un error en una operación relacionada con la configuración del contenedor de seguridad y de red. El valor clave tendrá información de contexto, como el nombre del contenedor y el número de generación. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware. Compruebe que los registros del host (*vmkernel.log* y *vsfwd.log*) incluyan el periodo de tiempo en el que se aplicó la configuración del contenedor a la vNIC.
301051	Importante	No	Flow missed on host.	La información del flujo de una o varias sesiones desde y hacia las máquinas virtuales protegidas se descartó, se produjo un error al leerla, o bien al enviarla a NSX Manager. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre y que el consumo de memoria vsfwd esté dentro de los límites del recurso (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301061	Crítica	No	Spoofguard config update failed on host.	Error en una operación de configuración relacionada con SpoofGuard. Acción: verifique que se realizó el procedimiento de preparación del host. Inicie sesión en el host y recopile el archivo `/var/log/vsfwd.log` y, a continuación, fuerce la sincronización de la configuración del firewall con la API `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` (consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*). Si se siguen produciendo errores en la configuración de Spoofguard, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware. Asegúrese de que los registros incluyan el periodo de tiempo durante el cual el host recibió la configuración de Spoofguard.
301062	Importante	No	Failed to apply spoofguard to vnic.	No se pudo aplicar SpoofGuard a una vNIC. Acción: verifique que se realizó el procedimiento de preparación del host. Inicie sesión en el host y recopile el archivo `/var/log/vsfwd.log` y, a continuación, fuerce la sincronización de la configuración del firewall con la API `https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>` (consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*). Si se siguen produciendo errores en la configuración de Spoofguard, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301064	Importante	No	Failed to disable spoofguard for vnic.	No se pudo deshabilitar SpoofGuard de una vNIC. Acción: recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301072	Crítica	No	Failed to delete legacy App service vm.	Se produjo un error al eliminar la máquina virtual del servicio vShield App para vCloud Networking and Security. Acción: verifique que se siguió el procedimiento descrito en el apartado sobre la actualización de vShield App al firewall distribuido en la *Guía de actualización de NSX*.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301080	Crítica	No	Firewall CPU threshold crossed.	Se superó el valor del umbral de uso de CPU vsfwd. Acción: consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*. Es posible que necesite reducir el uso de los recursos del host. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301081	Crítica	No	Firewall memory threshold crossed.	Se superó el valor del umbral de la memoria vsfwd. Acción: consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*. Es posible que necesite reducir el uso de recursos del host, acción que incluye reducir el número de reglas del firewall configuradas o los contenedores de seguridad y de red. Para reducir el número de reglas del firewall, use la capacidad `appliedTo`. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301082	Crítica	No	Firewall ConnectionsPerSecond threshold crossed.	Se traspasó el umbral de conexiones por segundo del firewall. Acción: consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*. Es posible que necesite reducir el uso de recursos del host, acción que incluye reducir el número de conexiones activas desde y hacia las máquinas virtuales del host.
301501	Crítica	No	Firewall configuration update version {version#} to host {hostID} timed out. Firewall configuration on host is synced upto version {version#}.	Un host tardó más de dos minutos en procesar una actualización de la configuración del firewall y expiró el tiempo de espera de la actualización. Acción: verifique que vsfwd esté funcionando y que esas reglas se van a publicar en los hosts. Consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301502	Crítica	No	Spoofguard configuration update number {number#} to host {hostID} timed out. Spoofguard configuration on host is synced upto version {version#}.	Un host tardó más de dos minutos en procesar una actualización de la configuración del Spoofguard y expiró el tiempo de espera de la actualización. Acción: verifique que vsfwd esté funcionando y que esas reglas se van a publicar en los hosts. Consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301503	Crítica	No	Failed to publish firewall configuration version {version#} to cluster {clusterID}. Refer logs for details.	Se produjo un error al publicar reglas del firewall en un clúster o en uno o varios hosts. Acción: consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301504	Crítica	No	Failed to publish container updates to cluster {clusterID}. Refer logs for details.	Se produjo un error al publicar las actualizaciones de los contenedores de seguridad y de red en un clúster o en uno o varios hosts. Acción: consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301505	Crítica	No	Failed to publish spoofguard updates to cluster {clusterID}. Refer logs for details.	Se produjo un error al publicar las actualizaciones de SpoofGuard en un clúster o en uno o varios hosts. Acción: consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301506	Crítica	No	Failed to publish exclude list updates to cluster {clusterID}. Refer logs for details.	Se produjo un error al publicar las actualizaciones de la lista de exclusión en un clúster o en uno o varios hosts. Acción: consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301508	Crítica	No	Failed to sync host {hostID}. Refer logs for details.	Error en la operación de sincronización forzada del firewall a través de la API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>`. Acción: consulte "Resolución de problemas del firewall distribuido" en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301510	Crítica	No	Force sync operation failed for the cluster.	Error en la operación de sincronización forzada del firewall a través de la API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` . Acción: recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301512	Importante	No	Firewall is installed on host {hostID}[{hostID}].	El firewall distribuido se instaló correctamente en un host. Acción: en vCenter Server, desplácese hasta **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y seleccione la pestaña Preparación del host (Host Preparation). Compruebe que el Estado del firewall (Firewall Status) aparece en color verde.
301513	Importante	No	Firewall is uninstalled on host {hostID}[{hostID}].	El firewall distribuido se desinstaló de un host. Si los componentes del firewall distribuido no se pueden desinstalar, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301514	Crítica	No	Firewall is enabled on cluster {clusterID}.	El firewall distribuido se instaló correctamente en un clúster. Acción: en vCenter Server, desplácese hasta **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y seleccione la pestaña Preparación del host (Host Preparation). Compruebe que el Estado del firewall (Firewall Status) aparece en color verde.
301515	Crítica	No	Firewall is uninstalled on cluster {clusterID}.	El firewall distribuido se desinstaló de un clúster. Acción: si los componentes del firewall distribuido no se pueden desinstalar, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301516	Crítica	No	Firewall is disabled on cluster {clusterID}.	El firewall distribuido se deshabilitó en todos los host de un clúster. Acción: ninguna.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301034	Importante	No	Failed to apply Firewall rules to host.	Se produjo un error al aplicar una sección de reglas de firewall distribuido. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301043	Crítica	No	Failed to apply container configuration to vnic.	Se produjo un error al aplicar una configuración del contenedor de seguridad o de red. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301044	Crítica	No	Failed to apply container configuration to host.	Se produjo un error al aplicar una configuración del contenedor de seguridad o de red. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.
301066	Importante	No	Failed to apply Spoofguard configuration to host.	No se pudo aplicar SpoofGuard a las vnics. Acción: verifique que las pilas del kernel vsip tengan suficiente memoria libre (consulte cómo comprobar los eventos del umbral de memoria y la CPU del firewall en la *Guía de administración de NSX*). Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301100	Crítica	No	Firewall timeout configuration update failed on host.	La configuración del tiempo de espera del temporizador de la sesión del firewall no se pudo actualizar. Acción: recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware. Después de recopilar los registros, realice una sincronización forzada de la configuración del firewall con la REST API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>`. También puede acceder a **Instalación (Installation) > Preparación del host (Host Preparation)** y, en **Acciones (Actions)**, seleccionar **Forzar servicios de sincronización (Force Sync Services)** para llevar a cabo esta acción.
301101	Importante	No	Failed to apply firewall timeout configuration to vnic.	La configuración del tiempo de espera del temporizador de la sesión del firewall no se pudo actualizar. Acción: recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware. Después de recopilar los registros, realice una sincronización forzada de la configuración del firewall con la REST API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>`. También puede acceder a **Instalación (Installation) > Preparación del host (Host Preparation)** y, en **Acciones (Actions)**, seleccionar **Forzar servicios de sincronización (Force Sync Services)** para llevar a cabo esta acción.
301103	Importante	No	Failed to apply firewall timeout configuration to host.	La configuración del tiempo de espera del temporizador de la sesión del firewall no se pudo actualizar. Acción: recopile los registros de soporte técnico de NSX Manager y del host, y póngase en contacto con el equipo de soporte técnico de VMware. Después de recopilar los registros, realice una sincronización forzada de la configuración del firewall con la REST API `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>`. También puede acceder a **Instalación (Installation) > Preparación del host (Host Preparation)** y, en **Acciones (Actions)**, seleccionar **Forzar servicios de sincronización (Force Sync Services)** para llevar a cabo esta acción.
301200	Importante	No	Application Rule Manager flow analysis started.	Comenzó el análisis de flujos del Administrador de reglas de aplicaciones (Application Rule Manager). Acción: ninguna.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
301201	Importante	No	Application Rule Manager flow analysis failed.	Se produjo un error en el análisis de flujos del Administrador de reglas de aplicaciones (Application Rule Manager). Acción: recopile los registros de soporte técnico de NSX Manager y póngase en contacto con el equipo de soporte técnico de VMware. Inicie una nueva sesión de supervisión para las mismas vNIC de la sesión en la que se produjo el error para intentar volver a realizar la operación.
301202	Importante	No	Application Rule Manager flow analysis completed.	Se completó el análisis de flujo de la herramienta Administrador de reglas de aplicaciones (Application Rule Manager). Acción: ninguna.

Eventos del sistema de NSX Edge

En la tabla se explican los mensajes de eventos del sistema referentes a NSX Edge y que tienen una gravedad alta, crítica o importante. Los eventos del sistema de relevancia informativa se muestran si dichos eventos activan la alarma.

Código de evento	Gravedad del evento	Código de alarma	Mensaje del evento	Descripción
30011	Alta	N/C	None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.	Las máquinas virtuales de NSX Edge se deberían recuperar automáticamente de este estado. Busque una captura con los códigos de evento 30202 o 30203. Acción: consulte cómo solucionar los problemas de Edge en la *Guía para solucionar problemas de NSX*.
30013	Crítica	130013	NSX Manager found NSX Edge VM (vmId : {#}) in bad state. Needs a force sync.	La máquina virtual de NSX Edge informa sobre un estado incorrecto y es posible que no funcione correctamente. Acción: se activa una sincronización forzada cuando se detecta un estado problemático. Si se produce un error en la sincronización forzada automática, realice una sincronización forzada manual.
30014	Importante	N/C	Failed to communicate with the NSX Edge VM.	NSX Manager se comunica con NSX Edge a través de VIX o del bus de mensajería. NSX Manager selecciona el canal de comunicación dependiendo de si se realiza la preparación del host cuando se implementa o se vuelve a implementar Edge. Este evento indica que se perdió la comunicación entre NSX Manager y NSX Edge. Acción: consulte cómo solucionar los problemas de Edge en la *Guía para solucionar problemas de NSX*.
30027	Informativo	130027	NSX Edge VM (vmId : {#}) is powered off.	La máquina virtual NSX Edge se desconectó. Acción: evento únicamente informativo.
30032	Alta	130032	NSX Edge appliance with vmId : {#} not found in the vCenter inventory.	Probablemente, la máquina virtual de NSX Edge se eliminó directamente desde vCenter Server. No se admite esta operación, ya que los objetos administrados por NSX se deben agregar o eliminar desde la interfaz de vSphere Web Client para NSX. Acción: vuelva a implementar Edge o implemente uno nuevo.

Código de evento	Gravedad del evento	Código de alarma	Mensaje del evento	Descripción
30033	Alta	130033	NSX Edge VM (vmId : {#}) not found in the vCenter inventory.	La máquina virtual NSX Edge no se encuentra en el inventario de vCenter. Acción: compruebe si la máquina virtual se eliminó accidentalmente. Si se confirmó, vuelva a implementar el dispositivo edge.
30034	Crítica	130034	None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.	La máquina virtual de Edge no responde a las comprobaciones de estado que envía NSX Manager. Acción: confirme que la máquina virtual esté encendida. A continuación, recopile los registros de Edge y póngase en contacto con el equipo de soporte técnico de VMware.
30037	Crítica	N/C	Edge firewall rule modified as {#} is no longer available for {#}.	Un GroupingObject no válido (IPSet, securityGroup, etc.) está presente en la regla del firewall. Acción: vuelva a visitar la regla del firewall y realice las actualizaciones necesarias.
30038	Crítica	N/C	Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule.	NSX Edge High Availability aplica reglas de anticompatibilidad a los hosts de vSphere automáticamente para que las máquinas virtuales de Edge activas y en suspensión se implementen en hosts diferentes. Este evento indica que esas reglas de anticompatibilidad se eliminaron del clúster y que ambas máquinas virtuales de Edge se ejecutan en el mismo host. Acción: acceda a vCenter Server y compruebe las reglas de anticompatibilidad.
30045	Crítica	N/C	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.	El entorno de red puede estar causando errores de comunicación repetidos en la máquina virtual de Edge a través del canal VIX. Acción: recopile los registros de soporte técnico de NSX Manager y de NSX Edge si NSX Edge no responde. A continuación, realice una sincronización forzada. Si el problema continúa, vuelva a implementar NSX Edge (consulte "Volver a implementar NSX Edge" en la *Guía de administración de NSX*). **NOTA:** Volver a implementar es una acción disruptiva. Se recomienda realizar primero una sincronización forzada y, si el problema no se soluciona, entonces volver a implementar.
30046	Crítica	N/C	Pre rules publish failed on edge: {EdgeID#}, vm: {#} for generation number {#}. Refer logs for detail. It may need forcesync.	Las reglas del firewall de NSX Edge podrían no estar sincronizadas. Este error se genera a partir de un error en las reglas definidas previamente (que se configuraron desde DFW UI/API). Acción: si el proceso integrado de recuperación no soluciona automáticamente el problema, realice una sincronización manual.
30100	Crítica	N/C	NSX Edge was force synced.	Se realizó una sincronización forzada de la máquina virtual de NSX Edge. Acción: si la sincronización forzada no resuelve el problema, recopile los registro de soporte técnico de NSX Manager y de NSX Edge, y póngase en contacto con el equipo de soporte técnico de VMware.

Código de evento	Gravedad del evento	Código de alarma	Mensaje del evento	Descripción
30102	Alta	130102	NSX Edge (vmId : {IP Address}) is in Bad State. Needs a force sync.	La máquina virtual de NSX Edge tiene un error interno. Acción: si el proceso de recuperación integrado no soluciona automáticamente el problema, realice una sincronización manual.
30148	Crítica	N/C	NSX Edge CPU usage has increased. {#} Top processes are: {#}.	El uso de la CPU de la máquina virtual de NSX Edge es elevado durante periodos constantes. Acción: consulte cómo solucionar los problemas de Edge en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y de NSX Edge, y póngase en contacto con el equipo de soporte técnico de VMware.
30153	Importante	N/C	El motor de cifrado AESNI está activado.	El motor de cifrado AESNI está activado. Acción: ninguna.
30154	Importante	N/C	El motor de cifrado AESNI está desactivado.	El motor de cifrado AESNI está desactivado. Acción: ninguna. Este estado es el esperado.
30155	Alta	130155	No hay suficientes recursos de CPU y/o de memoria disponibles en el host o el grupo de recursos durante la reserva de recursos en el momento de la implementación de NSX Edge.	Recursos de CPU y/o de memoria insuficientes en el host o el grupo de recursos. Puede ver los recursos disponibles y los recursos reservados si se desplaza a la página **Inicio (Home) > Hosts y clústeres (Hosts and Clusters) > [Cluster-name]> Supervisar (Monitor) > Reserva de recursos (Resource Reservation**). Después de comprobar los recursos disponibles, vuelva a especificar los recursos como parte de la configuración del dispositivo, de esta forma la reserva de recursos se realiza correctamente.
30180	Crítica	N/C	NSX Edge is out of memory. The Edge is rebooting in 3 seconds. Top 5 processes are: {#}.	La máquina virtual de NSX Edge no tiene memoria. Comenzó un reinicio para recuperarse. Acción: consulte cómo solucionar los problemas de Edge en la *Guía para solucionar problemas de NSX*. Si el problema persiste, recopile los registros de soporte técnico de NSX Manager y de NSX Edge, y póngase en contacto con el equipo de soporte técnico de VMware.
30181	Crítica	130181	NSX Edge {EdgeID#} VM name {#} file system is read only.	Existe un problema de conectividad con el dispositivo de almacenamiento que respalda la máquina virtual de NSX Edge. Acción: compruebe y corrija cualquier problema de conectividad relacionado con el almacén de datos de respaldo. Es posible que necesite ejecutar una sincronización forzada manual después de solucionar el problema de conectividad.
30202	Importante	N/C	NSX Edge {EdgeID#} HighAvailability switch over happened. VM {#} name {#} has moved to ACTIVE state.	Se produjo un error de HA y la máquina virtual secundaria de NSX Edge cambió del estado de EN SUSPENSIÓN (STANDBY) a ACTIVA (ACTIVE). Acción: no se requiere ninguna acción.
30203	Importante	N/C	NSX Edge {EdgeID} HighAvailability switch over happened. VM {#} name {#} has moved to STANDBY state.	Se produjo un error de HA y la máquina virtual primaria de NSX Edge cambió del estado EN SUSPENSIÓN (STANDBY) a ACTIVA (ACTIVE). Acción: no se requiere ninguna acción.

Código de evento	Gravedad del evento	Código de alarma	Mensaje del evento	Descripción
30205	Crítica	130205	Split Brain detected for NSX Edge {EdgeID} with HighAvailability.	Debido a un error de red, las máquinas virtuales de NSX Edge configuradas para HA no pueden determinar si la otra máquina virtual está en línea. En tal caso, las máquinas virtuales de ambos lados piensan que la otra máquina no está en línea y pasan al estado ACTIVA (ACTIVE). Esto puede causar la interrupción de la red. Acción: compruebe la infraestructura de red (virtual y física) para buscar cualquier tipo de error, sobre todo en las interfaces y la ruta configurada para HA.
30302	Crítica	130302	LoadBalancer virtualServer/pool : {virtualServerName]} Protocol : {#} serverIp : {IP Address} changed the state to down.	Un grupo o un servidor virtual del equilibrador de carga de NSX Edge están fuera de servicio. Acción: consulte la sección sobre el equilibrador de carga de la *Guía para solucionar problemas de NSX*.
30303	Importante	N/C	LoadBalancer virtualServer/pool : {0} Protocol : {#} serverIp : {IP Address} changed to a wrong state.	Un grupo o un servidor virtual del equilibrador de carga de NSX Edge tienen un error interno. Acción: consulte la sección sobre el equilibrador de carga de la *Guía para solucionar problemas de NSX*.
30304	Importante	130304	LoadBalancer pool : {0} Protocol : {#} serverIp : {IP address} changed to a warning state.	El estado de grupo de equilibradores de carga de NSX Edge cambió a **advertencia (warning)**. Acción: consulte la sección sobre el equilibrador de carga de la *Guía para solucionar problemas de NSX*.
30402	Crítica	130402	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down.	Un canal VPN de IPsec de NSX Edge está fuera de servicio. Acción: consulte la sección "Redes privadas virtuales (VPN)" en la *Guía para solucionar problemas de NSX*.
30404	Crítica	130404	EDGE IPSEC TUNNEL DOWN : IPsec Tunnel from localSubnet : {subnet} to peerSubnet : {subnet} changed the status to down.	Un canal VPN de IPsec de NSX Edge está fuera de servicio. Acción: consulte la sección "Redes privadas virtuales (VPN)" en la *Guía para solucionar problemas de NSX*.
30405	Importante	N/C	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.	El estado del canal de VPN de IPsec de NSX Edge no se puede determinar. Acción: consulte la sección "Redes privadas virtuales (VPN)" en la *Guía para solucionar problemas de NSX*.
30406	Importante	N/C	IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.	El estado del canal de VPN de IPsec de NSX Edge no se puede determinar. Acción: consulte la sección "Redes privadas virtuales (VPN)" en la *Guía para solucionar problemas de NSX*.
30701	Crítica	N/C	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.	El servicio de NSX Edge DHCP Relay está deshabilitado. Posibles causas: (1) El proceso DHCP Relay no se está ejecutando. (2) No existen servidores DHCP externos. La eliminación de los objetos de agrupamiento por parte de la retransmisión puede causar esta condición. Acción: consulte cómo configurar DHCP Relay en la *Guía de administración de NSX*.

Código de evento	Gravedad del evento	Código de alarma	Mensaje del evento	Descripción
30206	Crítica	N/C	Resolved Split Brain for NSX Edge {EdgeID} with HighAvailability.	Los dos dispositivos de NSX Edge HA se pueden comunicar y renegociaron los estados de suspensión y activo. Acción: consulte cómo solucionar los problemas de NSX Edge High Availability (HA): (http://kb.vmware.com/kb/2126560).
30207	Crítica	N/C	Attempted Split Brain resolution for NSX Edge {EdgeID} with count {value}.	Los dos dispositivos de NSX Edge HA intentan renegociar y recuperarse de una condición de cerebro dividido. **NOTA:** : El mecanismo de recuperación notificado por este evento solo tiene lugar en versiones anteriores a la 6.2.3 de NSX Edge. Acción: consulte cómo solucionar los problemas de NSX Edge High Availability (HA): (http://kb.vmware.com/kb/2126560).

Eventos del sistema del tejido

En la tabla se explican los mensajes de eventos del sistema referentes al tejido y que tienen una gravedad alta, crítica o importante.

A continuación, se explican algunos términos relacionados con los eventos del sistema del tejido:

- El tejido es una capa de software en NSX Manager que interactúa con ESX Agent Manager (EAM) para instalar los servicios de seguridad y de redes en el host. Una vez que NSX recibe la confirmación por parte de EAM de que los VIB de NSX se instalaron correctamente en el host, la capa de tejido activa la configuración del bus de mensajería. Puede consultar más información sobre el tejido de NSX usando la API `/api/2.0/nwfabric/`.
- La agencia ESX Agent Manager (EAM) es la base de datos de NSX Manager de las unidades de implementación. La base de datos EAM de vCenter de las agencias EAM debe estar sincronizada. Una agencia EAM es el objeto que se crea en la base de datos EAM de vCenter para definir un servicio NSX que se base en EAM para la implementación. En raras ocasiones, las dos bases de datos no se sincronizan y NSX proporciona eventos y alarmas para notificar la condición.

En la siguiente tabla se documentan los mensajes de eventos del sistema que tienen una gravedad alta, crítica o importante para los eventos del sistema del tejido.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
250004	Alta	Sí	Datastore {#} could not be configured on host, probably its not connected.	El almacén de datos en el que almacena las máquinas virtuales de seguridad para el host podría no estar configurado. Acción: confirme que el host pueda acceder al almacén de datos.
250005	Alta	Sí	Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.	El host ESXi no pudo acceder a VIB/OVF desde NSX durante una instalación del servicio de NSX en el host. En la tabla de eventos del sistema vCenter, puede ver: `Event Message:'Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.', Module:'Security Fabric'`. Acción: consulte cómo solucionar problemas de vSphere ESX Agent Manager (EAM) con NSX (http://kb.vmware.com/kb/2122392).
250008	Alta	Sí	Service will need to be redeployed as the location of the OVF / VIB bundles to be deployed has changed.	Los VIB y OVF de NSX están disponibles a través de una URL que es diferente según las versiones de NSX. Para encontrar los VIB adecuados, acceda a *https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties*. Si la dirección IP de NSX Manager cambia, es posible que sea necesario volver a implementar el VIB o el OVF de NSX. Acción: para resolver la alarma, haga clic en el vínculo **Resolver (Resolve)** en la pestaña **Instalación (Installation) > Preparación del host (Host preparation)** o use la API `resolve` para resolver la alarma.
250009	Alta	Sí	Upgrade of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.	EAM no pudo acceder a VIB/OVF desde NSX durante una actualización del host. En la tabla de eventos del sistema vCenter, puede ver: `Event Message:'Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.', Module:'Security Fabric'`. Acción: consulte cómo solucionar problemas de vSphere ESX Agent Manager (EAM) con NSX (http://kb.vmware.com/kb/2122392).
250012	Alta	Sí	Following service(s) need to be installed successfully for Service {#} to function: {#}.	El servicio que se está instalando depende de otro servicio que aún no se instaló. Acción: implemente el servicio necesario en el clúster.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
250014	Alta	Sí	Error while notifying security solution before upgrade.	Se produjo un error al notificar una solución de seguridad antes de actualizar. Es posible que no se pueda acceder a la solución o que esta no responda. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución. Use la API `resolve` para resolver la alarma. El servicio se volverá a implementar.
250015	Alta	Sí	Did not receive callback from security solution for upgrade notification even after timeout.	No se recibió la devolución de la llamada desde la solución de seguridad para actualizar la notificación incluso después del tiempo de espera. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución y de que la solución pueda acceder a NSX. Use la API `resolve` para resolver la alarma. El servicio se volverá a implementar.
250016	Alta	No	Did not receive callback from security solution for uninstall notification even after timeout.	Se produjo un error al desinstalar el servicio. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución y de que la solución pueda acceder a NSX. Use la API `resolve` para resolver la alarma. Se eliminará el servicio.
250017	Alta	Sí	Se produjo un error al desinstalar el servicio.	Se produjo un error al notificar una solución de seguridad antes de realizar la desinstalación. Resolve to notify once again, or delete to uninstall without notification. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución y de que la solución pueda acceder a NSX. Use la API `resolve` para resolver la alarma. Se eliminará el servicio.
250018	Alta	Sí	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification.	Se produjo un error al notificar una solución de seguridad antes de realizar la desinstalación. Resolve to notify once again, or delete to uninstall without notification. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución y de que la solución pueda acceder a NSX. Use la API `resolve` para resolver la alarma. Se eliminará el servicio.
250019	Alta	Sí	Server rebooted while security solution notification for uninstall was going on.	Se reinició el servidor mientras se ejecutaba la notificación de la solución de seguridad para realizar la desinstalación. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución. Use la API `resolve` para resolver la alarma. Se desinstalará el servicio.
250020	Alta	Sí	Server rebooted while security solution notification for upgrade was going on.	Se reinició el servidor mientras se ejecutaba la notificación de la solución de seguridad para realizar la desinstalación. Acción: asegúrese de que NSX pueda acceder a las URL de esa solución. Use la API de resolución para resolver la alarma. El servicio se volverá a implementar.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
250021	Crítica	No	Connection to EAM server failed.	La conexión entre NSX Manager y el servicio EAM de vCenter está inactiva. Acción: verifique que vCenter esté activo y que el servicio EAM se esté ejecutando. Verifique que se pueda acceder a la URL **`http://{VC_IP}/eam/mob/`**. Para obtener más información, consulte la sección "Preparación de la infraestructura" en la *Guía para solucionar problemas de NSX*.
250023	Alta	Sí	Pre Uninstall cleanup failed.	No se pudieron completar las tareas de limpieza interna previas a la desinstalación. Acción: use la API `POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve` con el cuerpo de solicitud `SystemAlarmsDto` para solucionar la alarma y eliminar el servicio.
250024	Alta	Sí	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.	EAM implementa los VIB en los hosts ESXi. Una agencia EAM está instalada en cada clúster preparado con NSX. Si no se puede encontrar esta agencia, los servicios de vCenter Server se pueden estar inicializando o la agencia se eliminó de forma manual por error.
250025	Alta	Sí	El VIB requiere una instalación manual.	Este evento se genera cuando se realiza un intento de actualizar o desinstalar NSX BITS en el host sin estado mediante EAM. Todos los hosts sin estado deben estar preparados mediante la función Auto Deploy. Acción: corrija la configuración mediante la función Auto Deploy y utilice la API `resolve` para resolver la alarma.

Eventos del sistema del complemento de implementación

En la tabla se explican los mensajes de los eventos del sistema del complemento de implementación que tienen una gravedad alta, crítica o importante.

A continuación, se explican algunos términos relacionados con los eventos del sistema del complemento de implementación:

- El complemento de implementación es un código adicional que se agrega al tejido de NSX para realizar acciones de preimplementación y de postimplementación.
- La unidad de implementación es un objeto creado en la base de datos de NSX Manager para cada clúster. Se debe crear una unidad de implementación antes de instalar los servicios de seguridad y de redes.

En la siguiente tabla se documentan los mensajes de eventos del sistema que tengan una gravedad alta, crítica o importante y que se refieran a los eventos del sistema del complemento de implementación.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
280000	Alta	Sí	Deployment Plugin IP pool exhausted alarm.	Se produjo un error al asignar una dirección IP a una máquina virtual del servicio de NSX, ya que el grupo de direcciones IP de origen está agotado. Acción: agregue direcciones IP al grupo.
280001	Alta	Sí	Deployment Plugin generic alarm.	Cada servicio, como Guest Introspection, tiene un grupo de complementos para configurar el servicio de cada host. Los problemas con el código del complemento se notifican como una alarma genérica. El servicio aparecerá en verde después de que todos los complementos del servicio sean los correctos. Este evento captura un subconjunto de excepciones posibles. Acción: use la API `resolve` para resolver la alarma. El servicio se implementará.
280004	Alta	Sí	Deployment Plugin generic exception alarm.	Cada servicio, como Guest Introspection, tiene un grupo de complementos para configurar el servicio de cada host. Los problemas relacionados con el código del complemento se notifican como una alarma genérica de excepción. El servicio aparecerá en verde después de que todos los complementos del servicio sean los correctos. Este evento captura todas excepciones posibles. Acción: use la API `resolve` para resolver la alarma. El servicio se implementará.
280005	Alta	Sí	VM needs to be rebooted for some changes to be made/take effect.	Se debe reiniciar la máquina virtual para que se apliquen o se realicen algunos cambios. Acción: use la API `resolve` para resolver la alarma. Esto reiniciará la máquina virtual.

Eventos del sistema de mensajes

En la tabla se explican los mensajes de eventos del sistema que tienen una gravedad alta, crítica o importante con relación a los mensajes.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
390001	Alta	Sí	Host messaging configuration failed.	El bus de mensajería de NSX se configuró después de la preparación del host, una vez que ESX Agent Manager (EAM) informó a NSX de que los VIB de NSX se instalaron correctamente en un host ESXi. Este evento indica que se produjo un error en la configuración del bus de mensajería. A partir de NSX 6.2.3, aparece un icono rojo junto al host afectado en la pestaña **Instalación (Installation) > Preparación del host (Host Preparation)**. Acción: consulte los pasos de solución de problemas que aparecen en el artículo sobre cómo entender y solucionar los problemas del bus de mensajería en VMware NSX for vSphere 6.x (http://kb.vmware.com/kb/2133897).
390002	Alta	Sí	Host messaging connection reconfiguration failed.	En algunas situaciones, cuando NSX detecta que los detalles del agente RMQ cambian, intenta enviar la información del agente RMQ más reciente al host. Si NSX no puede enviar la información, se activa la alarma. Acción: consulte los pasos de solución de problemas que aparecen en el artículo sobre cómo entender y solucionar los problemas del bus de mensajería en VMware NSX for vSphere 6.x (http://kb.vmware.com/kb/2133897).
390003	Alta	Sí	Host messaging configuration failed and notifications were skipped.	NSX intentará configurar el canal de mensajería de nuevo cuando un host preparado se vuelva a conectar a vCenter Server. Este evento indica que se produjo un error en la configuración y que no se notificó la presencia de otros módulos de NSX dependientes del canal de mensajería. Acción: consulte los pasos de solución de problemas que aparecen en el artículo sobre cómo entender y solucionar los problemas del bus de mensajería en VMware NSX for vSphere 6.x (http://kb.vmware.com/kb/2133897).
391002	Crítica	No	Messaging infrastructure down on host.	Faltan dos o más mensajes de latidos entre NSX Manager y un host de NSX. Acción: consulte los pasos de solución de problemas que aparecen en el artículo sobre cómo entender y solucionar los problemas del bus de mensajería en VMware NSX for vSphere 6.x (http://kb.vmware.com/kb/2133897).
321100	Crítica	No	Disabling messaging account {account #}. Password has expired.	Un host ESXi, una máquina virtual NSX Edge o USVM que actúa como cliente de bus de mensajería no cambiaron su contraseña rabbit MQ en las dos horas después de la implementación inicial o la preparación del host. Acción: investigue si existe algún problema de comunicación entre NSX Manager y el cliente del bus de mensajería. Verifique que el cliente se esté ejecutando. Antes de volver a realizar la sincronización o implementación, recopile los registros apropiados. Consulte los pasos de solución de problemas que aparecen en el artículo sobre cómo entender y solucionar los problemas del bus de mensajería en VMware NSX for vSphere 6.x (http://kb.vmware.com/kb/2133897).

Eventos del sistema de Service Composer

En la tabla se explican los mensajes de eventos del sistema de Service Composer que tienen una gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
300000	Crítica	Sí	Policy {#} is deleted as a result of explicit deletion of its dependent SecurityGroup.	Una directiva del servicio se eliminó al borrar un grupo de seguridad dependiente. Acción: vuelva a crear el grupo de seguridad.
300001	Alta	Sí	Policy is out of sync.	Se produjo un error en Service Composer al intentar aplicar las reglas en esta directiva de servicio. Acción: consulte el mensaje de error de las entradas de las reglas para cambiar la directiva. Use Service Composer o la API `resolve` para resolver esta alarma.
300002	Alta	Sí	Firewall rules on this Policy are out of sync. No Firewall related changes from this policy will be pushed, until this alarm is resolved.	Este error fue causado por un problema con la configuración del firewall. Acción: consulte el mensaje de error para obtener más detalles de la directiva y, posiblemente, las reglas que causaron el error. Asegúrese de resolver la alarma para sincronizar la directiva utilizando Service Composer o la API `resolve`. Consulte también cómo solucionar problemas con Service Composer en NSX 6.x (http://kb.vmware.com/kb/2132612).
300003	Alta	Sí	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.	Un problema con la configuración de la introspección de red causó este error. Acción: consulte el mensaje de error para obtener más detalles de la directiva y, posiblemente, las reglas que causaron el error. Asegúrese de resolver la alarma para sincronizar la directiva utilizando Service Composer o la API `resolve`. Consulte cómo solucionar problemas con Service Composer en NSX 6.x (http://kb.vmware.com/kb/2132612).
300004	Alta	Sí	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.	Un problema con la configuración de la introspección invitada causó este error. Acción: consulte el mensaje de error para obtener más detalles de la directiva y, posiblemente, las reglas que causaron el error. Asegúrese de resolver la alarma para sincronizar la directiva utilizando Service Composer o la API `resolve`. Consulte también cómo solucionar problemas con Service Composer en NSX 6.x (http://kb.vmware.com/kb/2132612).
300005	Alta	Sí	Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection.	Se produjo un error en Service Composer al sincronizar una directiva. No se enviará ningún cambio a los servicios de introspección de red o de firewall. Acción: consulte el mensaje de error para determinar las directivas o las secciones del firewall que se deben editar. Resuelva la alarma a través de Service Composer o a través de la API `resolve`.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
300006	Alta	Sí	Service Composer is out of sync due to failure on sync on reboot operation.	Se produjo un error en Service Composer al sincronizar una directiva durante el reinicio. No se enviará ningún cambio a los servicios de introspección de red o de firewall. Acción: consulte el mensaje de error para determinar las directivas o las secciones del firewall que se deben editar. Resuelva la alarma a través de Service Composer o a través de la API `resolve`.
300007	Alta	Sí	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.	Se produjo un error de sincronización en Service Composer al revertir la regla del firewall a un borrador anterior. No se enviará ningún cambio a los servicios de introspección de red o de firewall. Acción: resuelva la alarma a través de Service Composer o a través de la API `resolve`.
300008	Alta	Sí	Failure while deleting section corresponding to the Policy.	Se produjo un error en Service Composer al eliminar la sección de reglas de firewall de la directiva. Este problema ocurrirá cuando no se pueda acceder al administrador de un servicio de terceros con la inserción de servicios de NSX. Acción: compruebe si existe algún problema de conectividad con un Service Manager de terceros. Resuelva la alarma a través de Service Composer o a través de la API `resolve`.
300009	Alta	Sí	Failure while reordering section to reflect precedence change.	Se produjo un error en Service Composer al sincronizar una directiva durante el reinicio. No se enviará ningún cambio a los servicios de introspección de red o de firewall. Acción: consulte el mensaje de error para determinar las directivas o las secciones del firewall que se deben editar. Resuelva la alarma a través de Service Composer o a través de la API `resolve`.
300010	Alta	Sí	Failure while initializing auto save drafts setting.	Se produjo un error en Service Composer al inicializar la configuración de borradores autoguardados. Acción: consulte el mensaje de error para determinar las directivas o las secciones del firewall que se deben editar. Resuelva la alarma a través de Service Composer o a través de la API `resolve`.

Eventos del sistema de las operaciones de SVM

En la tabla se explican los mensajes de eventos del sistema de las operaciones de las máquinas virtuales de servicio (SVM) que tienen una gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
280002	Alta	Sí	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.	Se produjo un error interno en una máquina virtual del servicio implementada. Acción: al resolver la alarma, se elimina la máquina virtual y se notifica una segunda alarma sobre la eliminación. Al resolver la segunda alarma se vuelve a instalar la máquina virtual. Si se produce un error en la máquina virtual, la alarma original se vuelve a notificar. Si la alarma vuelve a aparecer, recopile los registros de las SVM siguiendo el procedimiento que aparece en la base de conocimientos http://kb.vmware.com/kb/2144624 y póngase en contacto con el soporte de VMware.
280003	Alta	Sí	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.	Se reinició una máquina virtual del servicio implementada. Acción: al resolver la alarma, se reinicia la máquina virtual. Si se produce un error en el reinicio, la alarma vuelve a aparecer. Recopile los registros de las máquinas virtuales del servicio siguiendo el procedimiento que aparece en la KB http://kb.vmware.com/kb/2144624 y póngase en contacto con el equipo de soporte técnico de VMware.
280006	Alta	Sí	Failed to mark agent as available.	Se produjo un error interno al marcar la máquina virtual del agente ESX como disponible. Acción: resuelva la alarma con la API `resolve`. Si la alarma no se puede resolver, recopile los registros de las máquinas virtuales del servicio siguiendo el procedimiento que aparece en la KB http://kb.vmware.com/kb/2144624 y póngase en contacto con el equipo soporte técnico de VMware.

Replicación: eventos del sistema de sincronización universal

En la tabla se explican los mensajes de eventos del sistema para la replicación: sincronización universal de gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
310001	Crítica	No	Full sync failed for object type {#} on NSX Manager {#}.	Se produjo un error al realizar una sincronización completa de los objetos universales en un NSX Manager secundario. Acción: recopile los registros de soporte técnico de NSX Manager y póngase en contacto con el equipo de soporte técnico de VMware.
310003	Crítica	No	Universal sync operation failed for the entity {#} on NSX Manager {#}.	Se produjo un error al sincronizar un objeto universal con el NSX Manager secundario en un entorno Cross-vCenter. Acción: recopile los registros de soporte técnico de NSX Manager y póngase en contacto con el equipo de soporte técnico de VMware.

Eventos del sistema de NSX Management

En la tabla se explican los mensajes de eventos del sistema para NSX Management con gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
320001	Crítica	No	The NSX Manager IP has been assigned to another machine with the MAC Address.	La dirección IP de la administración de NSX Manager se asignó a una máquina virtual en la misma red. En las versiones anteriores a 6.2.3, no se detecta ni se evita la existencia de una dirección IP de NSX Manager duplicada. Esto puede causar la interrupción de la ruta de datos. En la versión 6.2.3 y las versiones posteriores, este evento se produce cuando se detecta una dirección duplicada. Acción: resuelva el problema de dirección duplicada.

Eventos del sistema de VXLAN

En la tabla se explican los mensajes de eventos del sistema referentes a VXLAN y que tienen una gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
814	Crítica	No	Logical Switch {#} is no longer properly configured since some of the backing distributed virtual port groups were modified and/or removed.	Uno o varios grupos de puertos DVS que respaldan un conmutador lógico de NSX se modificaron o se eliminaron, o bien se produjo un error al cambiar el modo del plano de control del conmutador lógico. Acción: si el evento se activó al eliminar o modificar un grupo de puertos, aparecerá un error en la página Conmutadores lógicos (Logical Switches) en vSphere Web Client. Haga clic en el error para crear los grupos de puertos DVS que faltan. Si el evento se activó debido a que se produjo un error al cambiar el modo del plano de control, vuelva a realizar la actualización. Consulte el apartado sobre cómo actualizar las zonas de transporte y los conmutadores lógicos en la *Guía de actualización de NSX*.
1900	Crítica	No	VXLAN initialization failed on the host.	Se produjo un error en la inicialización de VXLAN, ya que no se pudieron configurar los vmknics para el número necesario de VTEP. NSX prepara el DVS que seleccionó el usuario para VXLAN y crea un grupo de puertos DV para que lo use VTEP vmknics. El método de equilibrio de carga y formación de equipos, la MTU y el ID de VLAN se seleccionan durante la configuración de VXLAN. Los métodos de equilibrio de carga y formación de equipos deben coincidir con la configuración del DVS seleccionado para la VXLAN. Acción: revise `vmkernel.log`. Asimismo, consulte la sección "Preparación de la infraestructura" en la *Guía para solucionar problemas de NSX*.
1901	Crítica	No	VXLAN port initialization failed on the host.	Se produjo un error al configurar la VXLAN en el puerto DV asociado y el puerto se desconectó. NSX prepara el DVS que seleccionó el usuario para VXLAN y crea un grupo de puertos DV para que lo use cada conmutador lógico configurado. Acción: revise `vmkernel.log`. Asimismo, consulte la sección "Preparación de la infraestructura" en la *Guía para solucionar problemas de NSX*.
1902	Crítica	No	La instancia VXLAN no existe en el host.	Un puerto DV recibió la configuración de VXLAN cuando el DVS del host ESXi todavía no estaba habilitado para VXLAN. Acción: revise `vmkernel.log`. Asimismo, consulte la sección "Preparación de la infraestructura" en la *Guía para solucionar problemas de NSX*.
1903	Crítica	No	Logical Switch {#} can't work properly since the backing IP interface couldn't join specific multicast group.	Se produjo un error en la interfaz de VTEP al unir el grupo de multidifusión especificado. El tráfico a algunos hosts se puede ver afectado hasta que se resuelva el problema. NSX usa un mecanismo de reintentos periódicos (cada cinco segundos) para unir el grupo de multidifusión. Acción: revise `vmkernel.log`. Asimismo, consulte la sección "Preparación de la infraestructura" en la *Guía para solucionar problemas de NSX*.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
1905	Crítica	No	Transport Zone may not be used since the backing IP interface can't acquire correct IP Address.	Se produjo un error al asignar una IP válida a VTEP vmknic. Se descartará todo el tráfico de VXLAN a través de vmknic. Acción: confirme que DHCP esté disponible en las VLAN de transporte de VXLAN si se utiliza DHCP para la asignación de direcciones IP para VMKNics. Consulte el artículo sobre el error en la preparación del host NSX: Direcciones IP insuficientes en el grupo de IP (Insufficient IP addresses in IP pool) (http://kb.vmware.com/kb/2137025).
1906	Crítica	No	VXLAN overlay class is missing on DVS.	Los VIB de NSX no se instalaron cuando el DVS se configuró para VXLAN. Se producirá un error en todas las interfaces de VXLAN al conectarse a DVS. Acción: consulte el artículo sobre los problemas de conectividad de red después de actualizar un entorno NSX/VCNS (http://kb.vmware.com/kb/2107951).
1.920	Crítica	No	VXLAN Controller {#} has been removed due to the connection can't be built, please check controller IP configuration and deploy again.	Se produjo un error en la implementación del controlador. Acción: consulte que se pueda acceder a la dirección IP asignada. Asimismo, consulte la sección "NSX Controller" en la *Guía para solucionar problemas de NSX*.
1930	Crítica	No	The controller {#} cannot establish the connection to the node {#}(active={#}). Current connection status = {#}.	Dos nodos controladores están desconectados, lo que afecta a la comunicación entre controladores. Acción: consulte la sección "NSX Controller" en la *Guía para solucionar problemas de NSX*.
1935	Crítica	No	Host {#} information could not be sent to controllers as all controllers are inactive. Controller synchronization may be needed once controllers become active.	Se produjo un error al enviar la información del certificado del host al clúster de NSX Controller. El canal de comunicación entre el host y el clúster del controlador puede comportarse de forma no esperada. Acción: confirme que el estado del clúster de NSX Controller sea normal antes de preparar un host ESXi. Use la API `controller sync` para solucionar este problema.
1937	Crítica	No	VXLAN vmknic {#} [PortGroup = {#}] is missing or deleted from host {#}.	El vmknic de VXLAN no se encuentra o se eliminó del host. Esto afectará al tráfico desde y hacia el host. Acción: solucione este problema haciendo clic en el vínculo **Resolver (Resolve)** en la pestaña **Instalación (Installation) > Preparación de red lógica (Logical Network Preparation) > Transporte de VXLAN (VXLAN Transport)**.
1939	Crítica	No	VXLAN vmknic {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues.	NSX Manager detectó que falta un vmknic de VXLAN en Virtual Center. Esto puede deberse a problemas de comunicación de vCenter Server con el host. Además, cuando vCenter Server o un host se reinician, NSX Manager no puede detectar el vmknic de VXLAN durante un breve periodo de tiempo y se origina este evento. Cuando se finalice el reinicio de vCenter Server y del host, NSX Manager comprobará los vmknics de VXLAN y borrará el evento si todo está correcto. Acción: solucione este problema si no es transitorio haciendo clic en el vínculo **Resolver (Resolve)** de la pestaña **Instalación (Installation) > Preparación de red lógica (Logical Network Preparation) > Transporte de VXLAN (VXLAN Transport)**.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
1941	Crítica	No	Host Connection Status Changed: Event Code: {#}, Host: {#} (ID: {#}), NSX Manager - Firewall Agent: {#}, NSX Manager - Control Plane Agent: {#}, Control Plane Agent - Controllers: {#}.	NSX Manager detectó un estado de inactividad en una de las siguientes conexiones: de NSX Manager al agente del firewall del host, de NSX Manager al agente del plano de control del host o del agente del plano de control del host a NSX Controller. Acción: si la conexión de NSX Manager tal agente del firewall del host está inactiva, compruebe el registro de NSX Manager y del agente del firewall (*/var/log/vsfwd.log*) o envíe la llamada de POST `https://NSX-Manager-IP-Address/api/2.0/nwfabric/configure?action=synchronize` REST API para volver a sincronizar la conexión. Si la conexión de NSX Manager al agente del plano de control está inactiva, compruebe el registro del agente del plano de control y de NSX Manager (*/var/log/netcpa.log*). Si la conexión del agente del plano de control al NSX Controller está inactiva, diríjase a **Redes y seguridad (Networking & Security) > Instalación (Installation)** y compruebe el estado de la conexión del host.
1942	Crítica	No	The backing portgroup [moid = {#}] of LogicalSwitch {#} is marked as missing.	NSX Manager detectó que en Virtual Center falta un grupo de puertos DV de respaldo para un conmutador lógico de NSX. Acción: haga clic en el vínculo **Resolver (Resolve)** en la pestaña **Instalación (Installation) > Preparación de red lógica (Logical Network Preparation) > Transporte de VXLAN (VXLAN Transport)**, o bien utilice la REST API (POST `https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate`) para volver a crear el grupo de puertos.
1945	Crítica	No	The device {#} on controller {#} has the disk latency alert on.	NSX Manager detectó una latencia de disco elevada para NSX Controller. Acción: consulte la sección sobre NSX Controller en la *Guía para solucionar problemas de NSX*.
1947	Crítica	No	Controller Virtual Machine is powered off on vCenter.	NSX Manager detectó que una máquina virtual de NSX Controller se desconectó desde Virtual Center. El estado del clúster del controlador puede estar desconectado, lo que ejerce un impacto en todas las operaciones que necesitan un clúster en funcionamiento. Acción: haga clic en el botón **Resolver (Resolve)** del controlador en la pestaña **Instalación (Installation) > Administración (Management)**, o bien realice la llamada a la API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` para encender la máquina virtual del controlador.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
1948	Crítica	No	Controller Virtual Machine is deleted from vCenter.	NSX Manager detectó que una máquina virtual de NSX Controller se eliminó de Virtual Center. El estado del clúster del controlador puede estar desconectado, lo que ejerce un impacto en todas las operaciones que necesitan un clúster en funcionamiento. Acción: haga clic en el botón **Resolver (Resolve)** del controlador en la pestaña **Instalación (Installation) > Administración (Management)**, o bien realice la llamada a la API POST `https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate` para eliminar el estado del controlador en la base de datos de NSX Manager.
1952	Crítica	No	The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies.	NSX Manager detectó que la directiva de creación de equipos del grupo de puertos VXLAN es diferente a la directiva de creación de equipos del DVS asociado. Esto puede provocar un comportamiento impredecible. Acción: vuelva a configurar el grupo de puertos VXLAN o DVS, de forma que tengan la misma directiva de creación de equipos.

Eventos del sistema del firewall de identidad

En la tabla se explican los mensajes de eventos del sistema del firewall de identidad (IDFW) que tienen una gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
395000	Crítica	No	SecurityLog on Domain Controller Eventlog Server is Full.	El registro de seguridad del servidor de registros de eventos de Active Directory está completo. El IDFW dejará de funcionar si está configurado para usar la extracción de registros. Acción: póngase en contacto con el administrador del servidor de Active Directory y aumente el tamaño del registro de seguridad, bórrelo o archívelo.

Eventos del sistema de EAM

En la tabla se explican los mensajes de eventos del sistema de ESX Agent Manager (EAM) que tienen una gravedad alta, crítica o importante.

Código de evento	Gravedad del evento	Alarma activada	Mensaje del evento	Descripción
270000	Alta	Sí	EAM alarm received.	ESX Agent Manager (EAM) detectó un problema en la instalación o la actualización de NSX con los VIB de NSX o las máquinas virtuales del servicio. Acción: para resolver la alarma, haga clic en el vínculo **Resolver (Resolve)** en la pestaña **Instalación (Installation) > Preparación del host (Host preparation)** o use la API `resolve`.

Índice