



Notas de la versión de VMware NSX for vSphere 6.3.4

VMware NSX for vSphere 6.3.4 | Publicado el jueves, 12 de octubre de 2017 | Compilación 7087695

Consulte el [Historial de revisión](#) de este documento.

Contenido de las notas de la versión

Las notas de la versión contienen los siguientes temas:

- [Novedades de NSX 6.3.4](#)
- [Instalación, versiones y requisitos del sistema](#)
- [Funciones obsoletas y suspendidas](#)
- [Notas sobre la actualización](#)
- [Cumplimiento de FIPS](#)
- [Historial de revisión](#)
- [Problemas resueltos](#)
- [Problemas conocidos](#)

Novedades de NSX 6.3.4

Información importante sobre NSX 6.3.4: NSX for vSphere 6.3.4 se reempaquetó para corregir los problemas mencionados en los artículos [2151719](#) y [000051144](#) de la base de conocimientos de VMware. La compilación publicada originalmente, 6845891, se sustituyó por la 7087695. Para obtener más información, consulte los artículos de la base de conocimientos de VMware. Para obtener más información sobre la actualización, consulte la sección [Notas sobre la actualización](#).

NSX for vSphere 6.3.4 soluciona varios errores específicos de los clientes. Consulte la sección [Problemas resueltos](#) para obtener más información.

Consulte las notas de la versión de versiones anteriores:

- NSX [6.3.3](#)
- NSX [6.3.2](#)
- NSX [6.3.1](#)
- NSX [6.3.0](#)

Instalación, versiones y requisitos del sistema

Nota:

- En la siguiente tabla, se muestran las versiones recomendadas del software de VMware. Estas recomendaciones son generales y no deben sustituir ni anular las recomendaciones específicas del entorno.
- Esta información está actualizada según la fecha de publicación de este documento.

- Consulte la [matriz de interoperabilidad de productos VMware](#) para conocer las versiones mínimas admitidas de NSX y de otros productos de VMware. VMware determina las versiones mínimas admitidas basándose en pruebas internas.
 - La versión mínima admitida y requerida de vSphere para la interoperabilidad de NSX varía entre NSX 6.3.2 y NSX 6.3.3. Consulte la sección [Matriz de interoperabilidad de productos de VMware](#) para obtener más información.

Producto o componente	Versión recomendada
NSX for vSphere	<p>VMware recomienda la versión más reciente de NSX 6.3 para nuevas implementaciones y cuando se actualiza desde la versión 6.1.x.</p> <p>Al actualizar las implementaciones existentes, revise las notas de la versión de NSX o póngase en contacto con su representante del soporte técnico de VMware para obtener más información sobre problemas específicos antes de planificar una actualización.</p>
vSphere	<ul style="list-style-type: none"> • vSphere 5.5U3 y versiones posteriores. • vSphere 6.0U3 y versiones posteriores. vSphere 6.0U3 resuelve el problema de VTEP duplicados que aparecen en los hosts ESXi después de reiniciar vCenter Server. Consulte el artículo 2144605 de la base de conocimientos de VMware para obtener más información. • vSphere 6.5U1 y versiones posteriores. vSphere 6.5U1 soluciona el problema de EAM con tipo OutOfMemory. Consulte el artículo 2135378 de la base de conocimientos de VMware para obtener más información.
Guest Introspection para Windows	<p>Se admiten todas las versiones de VMware Tools. Algunas funciones basadas en Guest Introspection requieren versiones de VMware Tools más recientes:</p> <ul style="list-style-type: none"> • Use VMware Tools 10.0.9 y 10.0.12 para habilitar el componente de controlador de introspección de red opcional de Thin Agent que se incluye con VMware Tools. • Actualice a VMware Tools 10.0.8 y a versiones posteriores para resolver el problema relacionado con el bajo rendimiento de las máquinas virtuales tras actualizar VMware Tools en NSX/vCloud Networking and Security (consulte el artículo 2144236 de la base de conocimientos de VMware). • Use VMware Tools 10.1.0 y versiones posteriores para garantizar su compatibilidad con Windows 10. • Utilice VMware Tools 10.1.10 y versiones posteriores para garantizar su compatibilidad con Windows Server 2016.

Esta versión de NSX admite las siguientes versiones de Linux:

Guest Introspection
para Linux

- RHEL 7 GA (64 bits)
- SLES 12 GA (64 bits)
- Ubuntu 14.04 LTS (64 bits)

Nota: Actualmente, VMware no admite NSX for vSphere 6.3.x con vRealize Networking Insight 3.2.

Requisitos del sistema e instalación

Para ver la lista completa de requisitos previos para la instalación de NSX, consulte la sección sobre [requisitos del sistema para NSX](#) en la *Guía de instalación de NSX*.

Para obtener instrucciones de instalación, acceda a la [Guía de instalación de NSX](#) o la [Guía de instalación de Cross-vCenter NSX](#).

Funciones obsoletas y suspendidas

Advertencias sobre la finalización del ciclo de vida y del soporte técnico

Consulte la [matriz del ciclo de vida de productos de VMware](#) para obtener información sobre NSX y otros productos de VMware que deben actualizarse próximamente.

- **NSX for vSphere 6.1.x** llegó a las etapas de fin de disponibilidad (End of Availability, EOA) y de fin de soporte técnico general (End of General Support, EOGS) el 15 de enero de 2017. (Consulte también el [artículo 2144769 de la base de conocimientos de VMware](#)).
- **Se eliminó NSX Data Security:** En NSX 6.3.0, la función NSX Data Security se eliminó del producto.
- **La función Supervisión de actividad (Activity Monitoring, SAM) de NSX está obsoleta:** A partir de NSX 6.3.0, no se admite la función de Supervisión de actividad (Activity Monitoring) de NSX. En su lugar, utilice la función Supervisión de endpoints (Endpoint Monitoring). Para obtener más información, consulte [Supervisión de endpoints \(Endpoint Monitoring\)](#) en la *Guía de administración de NSX*.
- **Se eliminó la función Terminal de acceso web (Web Access Terminal):** La función Terminal de acceso web (Web Access Terminal, WAT) se ha eliminado de NSX 6.3.0. No puede configurar el acceso web de SSL VPN-Plus y habilitar el acceso de URL pública a través de NSX Edge. VMware recomienda utilizar el cliente con acceso completo con implementaciones de VPN SSL para mejorar la seguridad. Si está usando la funcionalidad WAT en una versión más reciente, debe deshabilitarla antes de actualizar a 6.3.0.
- **Se eliminó IS-IS de NSX Edge:** A partir de NSX 6.3.0, no puede configurar el protocolo IS-IS desde la pestaña Enrutamiento (Routing).
- **vCNS Edge ya no es compatible.** Debe actualizar a una instancia de NSX Edge antes de actualizar a NSX 6.3.x.

Eliminaciones de la API y cambios del comportamiento

Eliminar la configuración del firewall o una sección predeterminada:

- La solicitud para eliminar la sección del firewall ahora se rechaza si se especifica la sección **predeterminada**: `DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId`

- Se introdujo un nuevo método para obtener la configuración predeterminada. Use la salida de este método para reemplazar la configuración completa o cualquiera de las secciones predeterminadas:
 - Obtenga la configuración predeterminada con `GET /api/4.0/firewall/globalroot-0/defaultconfig`
 - Actualice la configuración completa con `PUT /api/4.0/firewall/globalroot-0/config`
 - Actualice una sección única con `PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}`

Se eliminó el parámetro `defaultOriginate` de los siguientes métodos únicamente para los dispositivos NSX Edge del enrutador lógico (distribuido):

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

No se puede establecer el valor verdadero (`true`) en `defaultOriginate` en un dispositivo perimetral de enrutador (distribuido) lógico de NSX 6.3.0 o posterior.

Todos los métodos IS-IS se eliminaron del enrutamiento de NSX Edge.

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

Cambios de comportamiento y eliminaciones de la CLI

No utilice comandos no admitidos en nodos de NSX Controller

Existen comandos sin documentar para configurar NTP y DNS en los nodos de NSX Controller. Estos comandos no son compatibles y no deben utilizarse en nodos de NSX Controller. Debe utilizar solo los comandos que aparecen documentados en la guía de la CLI de NSX.

Notas sobre la actualización

- [Notas generales sobre la actualización](#)
- [Notas sobre la actualización de los componentes de NSX](#)
- [Notas sobre la actualización de FIPS](#)

Nota: Para obtener una lista de problemas conocidos que afectan a la instalación y las actualizaciones, consulte la sección [Problemas conocidos de instalación y actualización](#).

Notas generales sobre la actualización

- **Actualización de NSX 6.3.4 compilación 6845891 a NSX 6.3.4 compilación 7087695:** Solo es necesario actualizar NSX Manager y el clúster de NSX Controller. No es necesario actualizar los hosts, los dispositivos NSX Edge ni Guest Introspection.
- **Actualización completa de NSX:** Para actualizar NSX, debe realizar una actualización completa de NSX, incluido el clúster del host (que actualiza los VIB del host). Para obtener instrucciones, acceda a la [Guía de actualización de NSX](#), donde se encuentra la sección sobre [cómo actualizar los clústeres del host](#).
- **Requisitos del sistema:** Si desea obtener información sobre los requisitos del sistema para la instalación y actualización de NSX, consulte la sección [Requisitos del sistema para NSX](#) de la documentación de NSX.
- **Ruta de acceso de actualización desde NSX 6.x:** La [matriz de interoperabilidad de productos VMware](#) proporciona los detalles sobre las rutas de acceso de actualización desde VMware NSX. Encontrará información sobre la actualización de Cross-vCenter NSX en la [Guía de actualización de](#)

NSX.

- **Las versiones anteriores no son compatibles:**
 - Realice siempre una copia de seguridad de NSX Manager antes de realizar una actualización.
 - Una vez que NSX se actualice correctamente, no podrá volver a utilizar una versión anterior.
- Para validar que su actualización a NSX 6.3.x se realizó correctamente, consulte el [artículo de la base de conocimientos 2134525](#).
- No existe compatibilidad para las actualizaciones de vCloud Networking and Security con NSX 6.3.x. En primer lugar, debe actualizar a una versión compatible con la versión 6.2.x.
- **Interoperabilidad:** Consulte la sección [Matriz de interoperabilidad de productos de VMware](#) para obtener información sobre todos los productos de VMware relevantes antes de actualizar.
 - **Actualizar a vSphere 6.5a o a una versión posterior:** Al actualizar de vSphere 5.5 o 6.0 a vSphere 6.5a o a una versión posterior, debe actualizar primero a NSX 6.3.x. Consulte [cómo actualizar vSphere en un entorno de NSX](#) en la *Guía de actualización de NSX*.
Nota: NSX 6.2.x no es compatible con vSphere 6.5.
 - **Actualizar a NSX 6.3.3 o una versión posterior:** La versión mínima admitida de vSphere para la interoperabilidad de NSX varía entre NSX 6.3.2 y NSX 6.3.3. Consulte la sección [Matriz de interoperabilidad de productos de VMware](#) para obtener más información.
- **Compatibilidad con servicios de partner:** Si su sitio web utiliza servicios de partners de VMware para Guest Introspection o para Network Introspection, consulte la [Guía de compatibilidad de VMware](#) antes de realizar la actualización para comprobar que el servicio del proveedor sea compatible con esta versión de NSX.
- **Complemento de Redes y seguridad:** Después de actualizar NSX Manager, debe cerrar sesión y volver a iniciarla en vSphere Web Client. Si el complemento de NSX no se muestra correctamente, borre el historial y la memoria caché del explorador. Si el complemento de Redes y seguridad no aparece en vSphere Web Client, restablezca el servidor de vSphere Web Client como se explica en la [Guía de actualización de NSX](#).
- **Entornos sin estado:** En las actualizaciones de NSX en un entorno de host sin estado, los VIB nuevos se agregan previamente al perfil de imagen del host durante el proceso de actualización de NSX. Como resultado, el proceso de actualización de NSX en hosts sin estado sigue esta secuencia: Antes de NSX 6.2.0, había una sola URL en NSX Manager a partir de la cual podían encontrarse los VIB para una versión determinada del host ESX. Esto significa que el administrador solo necesitaba conocer una sola URL, independientemente de la versión de NSX. En NSX 6.2.0 y posteriores, los VIB de NSX nuevos están disponibles en distintas URL. Para encontrar los VIB correctos, debe realizar los pasos siguientes:
 1. Busque la URL de VIB nueva en `https://<NSXManager>/bin/vdn/nwfabric.properties`.
 2. Obtenga los VIB de la versión de host ESX requerida desde la URL correspondiente.
 3. Agréguelos al perfil de imagen del host.

Notas sobre la actualización de los componentes de NSX

Actualización de NSX Manager

- Si utiliza SFTP para realizar copias de seguridad de NSX, cambie a `hmac-sha2-256` después de actualizar a 6.3.x, porque no se admite `hmac-sha1`. Consulte el [artículo 2149282 de la base de conocimientos de VMware](#) para obtener una lista de los algoritmos de seguridad que se admiten en 6.3.x.
- Si desea actualizar de NSX 6.3.3 a NSX 6.3.4, primero debe seguir las instrucciones de solución alternativa del [artículo 2151719 de la base de conocimientos de VMware](#).

Actualización de Controller

- En NSX 6.3.3, el tamaño de disco del dispositivo NSX Controller cambia de 20 GB a 28 GB.
- El clúster de NSX Controller debe contar con tres nodos del controlador para actualizar a NSX 6.3.3. Si tiene menos de tres controladores, debe agregarlos antes de iniciar la actualización. Para obtener instrucciones, consulte la sección [Implementar clúster de NSX Controller](#).
- En la versión 6.3.3 de NSX, el sistema operativo subyacente de NSX Controller cambia. Esto significa que, cuando se actualiza de NSX 6.3.2 o de una versión anterior a NSX 6.3.3 o una versión posterior, en vez de una actualización local de software, los controladores existentes se eliminan uno a uno y se implementan nuevos controladores basados en Photon OS mediante las mismas direcciones IP. Consulte [Actualizar el clúster de NSX Controller](#)

Actualización del clúster del host

- En NSX 6.3.3, cambian los nombres de VIB de NSX. Los VIB esx-vsip y esx-vxlan se sustituyen por esx-nsxv si tiene NSX 6.3.3 o una versión posterior.
- **Desinstalación y actualización sin reinicio en los hosts:** A partir de vSphere 6.0, una vez que actualizó a NSX 6.3.x, no será necesario reiniciar después de realizar cambios en el VIB de NSX. En su lugar, los hosts deben entrar en modo de mantenimiento para completar el cambio de VIB.

No es necesario ningún reinicio del host durante las siguientes tareas:

- Las actualizaciones de NSX 6.3.0 a NSX 6.3.x en ESXi 6.0 o una versión posterior.
- La instalación del VIB de NSX 6.3.x que se requiere después de actualizar de ESXi 6.0 a 6.5.0a o versiones posteriores.

Nota: La actualización de ESXi aún requiere un reinicio del host.

- La desinstalación del VIB de NSX 6.3.x en ESXi 6.0 o versiones posteriores.

Se necesita un reinicio del host durante las siguientes tareas:

- Las actualizaciones de NSX 6.2.x o versiones anteriores a NSX 6.3.x (cualquier versión de ESXi).
- Las actualizaciones de NSX 6.3.0 a NSX 6.3.x en ESXi 5.5.
- La instalación del VIB de NSX 6.3.x que se necesita después de actualizar ESXi 5.5 a 6.0 o versiones posteriores.
- La desinstalación del VIB de NSX 6.3.x en ESXi 5.5.
- **Es posible que el host se bloquee en el estado de instalación:** Durante actualizaciones grandes de NSX, es posible que un host se bloquee en el estado de instalación durante un periodo de tiempo prolongado. Esto puede ocurrir debido a problemas originados al desinstalar los VIB anteriores de NSX. En este caso, el subproceso EAM asociado a este host aparecerá como bloqueado en la lista de tareas del cliente VI.

Solución alternativa: Haga lo siguiente:

- Inicie sesión en vCenter mediante el cliente VI.
- Haga clic con el botón derecho en la tarea EAM bloqueada y cáncela.
- En vSphere Web Client, emita una acción Resolver (Resolve) en el clúster. Es posible que el host bloqueado aparezca ahora como En curso (InProgress).
- Inicie sesión en el host y reinicie para forzar la finalización de la actualización en dicho host.

Actualización de NSX Edge

- En NSX 6.3.0 cambiaron los tamaños del disco del dispositivo de NSX Edge:
 - **Compacto, grande, cuádruple:** 1 disco de 584 MB + 1 disco de 512 MB
 - **Extra grande:** 1 disco de 584 MB + 1 disco de 2 GB + 1 disco de 256 MB

- Los clústeres del host deben estar preparados para NSX antes de actualizar los dispositivos de NSX Edge: A partir de la versión 6.3.0, no se admite la comunicación en el plano de administración entre NSX Manager y Edge a través del canal VIX. Solo se admite el canal del bus de mensajería. Cuando actualiza de NSX 6.2.x o una versión anterior a NSX 6.3.0 o una versión posterior, debe verificar que los clústeres del host donde se implementan los dispositivos NSX Edge estén preparados para NSX y que el estado de la infraestructura de mensajería sea de color VERDE. Si los clústeres del host no están preparados para NSX, se producirá un error en la actualización del dispositivo de NSX Edge. Consulte [Actualizar NSX Edge](#) en la *Guía de actualización de NSX* para obtener más información.

- **Actualizar la puerta de enlace de servicios Edge (ESG):**

A partir de la versión 6.2.5 de NSX, la reserva de los recursos se realiza al mismo tiempo que la actualización de NSX Edge. Cuando vSphere HA está habilitado en un clúster con recursos insuficientes, se puede producir un error en la operación de actualización, ya que se infringe la restricción de vSphere HA.

Para evitar estos errores de actualización, realice los siguientes pasos antes de actualizar una ESG:

NSX Manager usará las siguientes reservas de recursos si no configuró explícitamente los valores en el momento de instalación o actualización.

NSX Edge Factor de forma	Reserva de CPU	Reserva de memoria
COMPACTA (COMPACT)	1000 MHz	512 MB
GRANDE (LARGE)	2000 MHz	1024 MB
CUÁDRUPLE (QUADLARGE)	4000 MHz	2048 MB
EXTRA GRANDE (X-LARGE)	6000 MHz	8192 MB

1. Asegúrese siempre de que su instalación sigue las prácticas recomendadas para vSphere HA. Consulte el [artículo 1002080 de la base de conocimientos](#).

2. Use la API de configuración de ajuste de NSX:

PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>
para asegurarse de que los valores de `edgeVCpuReservationPercentage` y `edgeMemoryReservationPercentage` se encuentran dentro de los recursos disponibles para el factor de forma (consulte la tabla anterior para ver los valores predeterminados).

- **Deshabilite la opción Iniciar máquina virtual (Virtual Machine Startup) de vSphere cuando vSphere HA está habilitado y los Edges están implementados.** Tras actualizar NSX Edge 6.2.4 a la versión 6.2.5 u otras posteriores, debe desactivar la opción para iniciar la máquina virtual de vSphere en cada NSX Edge que se encuentre en un clúster en el que esté habilitado vSphere HA y en el que se hayan implementado Edges. Para ello, abra vSphere Web Client, busque el host ESXi donde se encuentra la máquina virtual de NSX Edge, haga clic en Administrar (Manage) > Configuración (Settings) y, en Máquinas virtuales (Virtual Machines), seleccione Inicio y apagado automático de la máquina virtual (VM Startup/Shutdown), haga clic en Editar (Edit) y asegúrese de que las máquinas virtuales estén en modo Manual (es decir, asegúrese de que no se añadiera a la lista de inicio/apagado automático).

- **Antes de actualizar a NSX 6.2.5 o una versión posterior, asegúrese de que todas las listas de cifrados del equilibrador de carga estén separadas por dos puntos.** Si su lista de cifrados utiliza otro separador, como, por ejemplo, comas, realice una llamada PUT a

https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles y sustituya cada lista `<ciphers>` de `<clientSsl>` y `<serverSsl>` por una lista separada por dos puntos. Por ejemplo, el segmento relevante del cuerpo de la solicitud puede tener la siguiente apariencia. Repita este procedimiento para todos los perfiles de la aplicación:

```

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

```

- **Establezca la versión correcta del cifrado para los clientes del equilibrador de carga en versiones de vROPs anteriores a 6.2.0:** los miembros del grupo vROPs de versiones anteriores a la 6.2.0 usan la versión 1.0 de TLS y, por lo tanto, debe establecer un valor de extensión de supervisión configurando explícitamente "ssl-version=10" en la configuración del equilibrador de carga de NSX. Consulte [Crear un monitor de servicio en la Guía de administración de NSX](#) para obtener instrucciones.

```

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

```

Notas sobre la actualización de FIPS

Cuando actualice de una versión de NSX anterior a NSX 6.3.0 a esta versión o una versión posterior, no debe habilitar el modo FIPS antes de que se complete la actualización. Si habilita el modo FIPS antes de que se haya completado la actualización, la comunicación entre los componentes actualizados y no actualizados se interrumpirá. Consulte la [descripción del modo FIPS y la actualización de NSX](#) en la *Guía de actualización de NSX* para obtener más información.

- **Cifrados admitidos en OS X Yosemite y OS X El Capitan:** Si usa el cliente de VPN de SSL en OS X 10.11 (El Capitan), podrá conectarse usando los cifrados AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA38, AES256-SHA y AES128-SHA. Por su parte, aquellos que usen OS X 10.10 (Yosemite) podrán conectarse usando únicamente los cifrados AES256-SHA y AES128-SHA.
- No habilite FIPS antes de que se complete la actualización a NSX 6.3.x. Consulte la [descripción del modo FIPS y la actualización de NSX](#) en la *Guía de actualización de NSX* para obtener más información.
- Antes de habilitar FIPS, compruebe que todas las soluciones para partners tengan el certificado del

modo FIPS. Consulte la [Guía de compatibilidad de VMware](#) y la documentación relevante del partner.

Cumplimiento de FIPS

- **NSS y OpenSwan:** IPsec VPN de NSX Edge utiliza el módulo de cifrado de Mozilla NSS. Debido a problemas de seguridad críticos, esta versión de NSX utiliza una versión más reciente de NSS que no cuenta con la validación de FIPS 140-2. Aunque VMware afirma que el módulo funciona correctamente, ya no está validado formalmente.
- **NSS y entrada de contraseña:** El hash de contraseñas de NSX Edge utiliza el módulo de cifrado de Mozilla NSS. Debido a problemas de seguridad críticos, esta versión de NSX utiliza una versión más reciente de NSS que no cuenta con la validación de FIPS 140-2. Aunque VMware afirma que el módulo funciona correctamente, ya no está validado formalmente.
- **Controller y VPN de agrupación en clústeres:** NSX Controller utiliza IPsec VPN para conectarse a los clústeres de Controller. IPsec VPN utiliza el módulo de cifrado del kernel de Linux para VMware (entorno Photon 1), que está en proceso de ser validado mediante CMVP.

Historial de revisión del documento

12 de octubre de 2017: Primera edición.

27 de octubre de 2017: Segunda edición. Se agregó el problema conocido 1965859.

9 de noviembre de 2017: Tercera edición: Se agregó información de la nueva compilación de la versión 6.3.4. Se agregó el problema resuelto 1989763. Se agregaron los siguientes problemas conocidos: 1783528, 1843197.

13 de mayo de 2019: Cuarta edición. Se actualizó la sección Actualización del clúster del host.

Problemas resueltos

Los problemas resueltos se agrupan del siguiente modo:

- [Problemas de servicios Edge y de redes lógicas resueltos en NSX 6.3.4](#)
- [Problemas de NSX Controller resueltos en NSX 6.3.4](#)

Problemas de servicios Edge y de redes lógicas resueltos en NSX 6.3.4

- **Problema solucionado 1970527:** ARP no se puede resolver en las máquinas virtuales cuando la tabla ARP del enrutador lógico distribuido supera el límite de 5K
Solucionado en 6.3.4.
- **Problema solucionado 1961105:** La conexión VTEP del hardware deja de funcionar después de reiniciar el controlador
Se produce una excepción BufferOverflow cuando algunas configuraciones VTEP del hardware se envían de NSX Manager a NSX Controller. Este problema de desbordamiento no permite que NSX Controller obtenga la configuración completa de la puerta de enlace del hardware.
Solucionado en 6.3.4.

Problemas de NSX Controller resueltos en NSX 6.3.4

- **Problema solucionado 1955855:** Se puede producir un error en la API del controlador debido a una limpieza de archivos de referencia del servidor de la API
Después de limpiar los archivos necesarios, se pueden producir errores en los flujos de trabajo, como Traceflow y la CLI central. Si los eventos externos interrumpen las conexiones TCP persistentes entre NSX Manager y el controlador, NSX Manager perderá la capacidad de establecer conexiones API con los controladores y estos aparecerán como desconectados en la IU. Esto no afecta a la ruta de acceso a los datos. *Solucionado en 6.3.4.*
- **Problema 1989763:** NSX Controller no se puede implementar porque caducó la contraseña de

la cuenta del usuario

Las cuentas de los usuarios de NSX Controller caducan a los 90 días. Esto hace que las contraseñas de las implementaciones de NSX Controller caduquen inmediatamente si se implementan 90 días después de la compilación. Este problema no afecta a la ruta de datos.

Solución alternativa: Consulte el [artículo 000051144 de la base de conocimientos de VMware](#).

Solucionado en NSX 6.3.3 compilación 7087283 y NSX 6.3.4 compilación 7087695.

Problemas conocidos

Los problemas conocidos se dividen del siguiente modo.

- [Problemas conocidos generales](#)
- [Problemas conocidos de instalación y actualización](#)
- [Problemas conocidos de NSX Controller](#)
- [Problemas conocidos de NSX Edge y redes lógicas](#)
- [Problemas conocidos de los servicios de seguridad](#)
- [Problemas conocidos de servicios de supervisión](#)
- [Problemas conocidos de interoperabilidad de soluciones](#)

Problemas conocidos generales

- **Problema 1874863:** No se puede autenticar con una contraseña modificada después de habilitar o deshabilitar el servicio VPN SSL con el servidor de autenticación local
Cuando el servicio VPN SSL está deshabilitado y se vuelve a habilitar con la autenticación local, los usuarios no podrán iniciar sesión con las contraseñas que se modificaron.

Consulte el [artículo 2151236 de la base de conocimientos de VMware](#) para obtener más información.

- **Problema 1702339:** Los escáneres de vulnerabilidad podrían notificar sobre la vulnerabilidad CVE-2016-4049 bgp_dump_routes de Quagga

Los escáneres de vulnerabilidad podrían notificar sobre la vulnerabilidad CVE-2016-4049 bgp_dump_routes de Quagga en NSX for vSphere. NSX for vSphere usa Quagga, pero la funcionalidad BGP (incluida la vulnerabilidad) no está habilitada. Esta alerta de vulnerabilidad se puede ignorar de forma segura.

Solución alternativa: No es necesaria ninguna, ya que el producto no es vulnerable.

- **Problema 1740625, 1749975:** Problemas de UI con Mac OS en Firefox y Safari
Si usa Firefox o Safari en Mac OS, el botón de navegación Atrás (Back) no funcionará en NSX Edge en la página Redes y seguridad (Network and Security) de vSphere 6.5 Web Client y, en ocasiones, se inmoviliza la UI en Firefox.

Solución alternativa: Use Google Chrome en Mac OS o haga clic en el botón Inicio y, a continuación, actúe como sea necesario.

- **Problema 1700980:** En la aplicación de revisión de seguridad CVE-2016-2775, un nombre de consulta demasiado largo puede causar un error de segmentación en lwresd
NSX 6.2.4 cuenta con BIND 9.10.4 instalado en el producto, pero no usa la opción lwres en *named.conf*y, por lo tanto, el producto no es vulnerable.

Solución alternativa: No es necesaria ninguna, ya que el producto no es vulnerable.

- **Problema 1568180:** Lista de funciones incorrecta para NSX cuando se usa vCenter Server Appliance (vCSA) 5.5.

Para ver las funciones de una licencia en vSphere Web Client, seleccione la licencia y haga clic en **Acciones (Actions) > Ver funciones (View Features)**. Si actualiza a NSX 6.2.3, su licencia se actualizará a una licencia empresarial, que habilita todas las funciones. Sin embargo, si NSX Manager se registró con vCenter Server Appliance (vCSA) 5.5, al seleccionar **Ver funciones (View Features)** se mostrará la lista de funciones de la licencia utilizada antes de la actualización, no la nueva licencia empresarial.

Solución alternativa: Todas las licencias empresariales tienen las mismas funciones, aunque no se muestren correctamente en vSphere Web Client. Consulte la [página de concesión de licencia de NSX](#) para obtener más información.

Problemas conocidos de instalación y actualización

Antes de la actualización, lea la sección [Notas sobre la actualización](#), más arriba en este documento.

- **Problema 1932907:** Error al actualizar la SVM de Guest Introspection

Al intentar actualizar la SVM de Guest Introspection, el estado de instalación de la SVM de GI cambia a "Error" ("Failed"). Esto se puede aplicar a las SVM de GI de uno o varios hosts del clúster.

Solución alternativa:

1. Eliminar la SVM de GI desde VC.
2. Haga clic en **Resolver (Resolve)** en el panel de implementación de servicio de SVM de GI. Se volverá a implementar la SVM de GI.

- **Problema 1848058:** Es posible que se produzca un error al actualizar los VIB del host ESXi a NSX 6.3.2

En ciertos casos, durante una actualización de los VIB del host ESXi a NSX 6.3.2, el directorio de VIB anterior se elimina de NSX Manager, lo que provoca un error en la actualización. Al hacer clic en el botón **Resolver (Resolve)**, el problema no se soluciona.

Solución alternativa: Para solucionar este problema, utilice la API de actualización:

```
PUT https://<nsx-mgr-ip>/api/2.0/nwfabric/configure
```

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.vxlan</featureId>
  <resourceConfig>
    <resourceId>domain-cXX</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

donde <nsx-mgr-ip> es la dirección IP de NSX Manager y domain-cXX es el ID de dominio del clúster.

- **Problema 1747217:** La preparación de resultados de hosts ESXi en muxconfig.xml.bad y Guest Introspection no funciona correctamente

Si la "ruta de acceso de vmx" no está en una de las máquinas virtuales en muxconfig.xml, cuando MUX intenta analizar el archivo de configuración y no encuentra la propiedad "xml path", cambia el nombre del archivo de configuración a "muxconfig.xml.bad", envía el error "Error - configuración de análisis MUX" a la USVM y cierra el canal de configuración.

Solución alternativa: Quite las máquinas virtuales huérfanas del inventario de vCenter.

- **Problema 1859572:** Durante la desinstalación de la versión 6.3.x de VIB de NSX en hosts ESXi administrados por la versión 6.0.0 de vCenter, el host continúa en modo de mantenimiento
Si va a desinstalar la versión 6.3.x de VIB de NSX en un clúster, el flujo de trabajo implica colocar los hosts en modo de mantenimiento, desinstalar los VIB y, a continuación, quitar los hosts del modo de mantenimiento por el servicio EAM. Sin embargo, si dichos hosts están administrados por la versión 6.0.0 de vCenter Server, esto dará lugar a que el host se bloquee en el modo de mantenimiento después de desinstalar los VIB. El servicio EAM responsable de desinstalar los VIB

pone al host en modo de mantenimiento, pero se produce un error al sacar los hosts de dicho modo.

Solución alternativa: Sacar manualmente el host del modo de mantenimiento. Este problema no se producirá si el host está administrado por la versión 6.5a y posteriores de vCenter Server.

- **Problema 1435504:** Comprobación de estado HTTP/HTTPS aparece en estado INACTIVO tras actualizar de 6.0.x o 6.1.x a 6.3.x con la razón de error "El código de retorno de 127 está fuera de los límites: es posible que el complemento falte"

En las versiones 6.0.x y 6.1.x de NSX, las direcciones URL configuradas sin comillas dobles (") generaron un fallo de comprobación de estado con el siguiente error: "El código de retorno de 127 está fuera de los límites: es posible que el complemento falte". La solución a este problema fue agregar las comillas dobles (") a la URL de entrada (esto no era necesario para enviar, recibir o esperar campos). Sin embargo, este problema se solucionó en la versión 6.2.0 y, como resultado, si va a actualizar de 6.0.x o 6.1.x a 6.3.x, las comillas dobles adicionales hacen que los miembros del grupo se muestren como INACTIVOS en la comprobación de estado.

Solución alternativa: Elimine las comillas dobles (") en el campo de URL de todas las configuraciones relevantes de comprobación de estado después de actualizar.

- **Problema 1734245:** Data Security provoca que se produzcan errores en las actualizaciones a la versión 6.3.0

Se producirán errores en las actualizaciones a la versión 6.3.0 si Data Security se configura como parte de una directiva de servicio. Asegúrese de eliminar Data Security de las directivas de servicio antes de actualizar la versión.

- **Problema 1801685:** No se pueden ver los filtros en ESXi después de actualizar de la versión 6.2.x a la 6.3.0 debido a un error al conectarse al host

Tras actualizar NSX de la versión 6.2.x a la 6.3.0 y los VIB de clúster a 6.3.0 bits, aunque el estado de la instalación se muestre como correcto y esté habilitado el firewall, el "estado del canal de comunicación" mostrará la conectividad de NSX Manager para el agente firewall y la conectividad de NSX Manager para el agente de plano de control como inactivo. Esto generará errores en la publicación de reglas del firewall y la directiva de seguridad, y provocará que la configuración de VXLAN no se envíe a los hosts.

Solución alternativa: Ejecute la llamada API de sincronización del bus de mensajes para el clúster que utilice la API POST: `https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize`.

Cuerpo de la API:

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

- **Problema 1797307:** NSX Edge puede ejecutarse como cerebro dividido tras una actualización o reimplementación.

En la instancia de NSX Edge en espera, el comando de la CLI `service highavailability` muestra el estado de alta disponibilidad como "En espera" (Standby) y el estado del motor de configuración como "Activo" (Active).

Solución alternativa: Reinicie la instancia de NSX Edge en espera.

- **Problema 1789989:** Durante la actualización de un clúster de hosts, puede producirse la pérdida de paquetes en el plano de datos.

Durante la actualización de VIB, se elimina el archivo de contraseñas de VSFWD (vShield Firewall Daemon), que se guarda en el VIB, de modo que VSFWD no puede utilizar la antigua contraseña para conectarse a NSX Manager y tiene que esperar hasta que se actualice la nueva contraseña.

Este proceso tarda algo de tiempo en completarse tras el reinicio del host. Sin embargo, en un clúster de DRS totalmente automatizado, las VM se mueven inmediatamente una vez que el host preparado se muestra activo. Puesto que en ese momento el proceso de VSFWD no está listo, existe la posibilidad de que se produzca una pérdida de paquetes en el plano de datos durante un corto período de tiempo.

Solución alternativa: En lugar de realizar una conmutación por recuperación desde el momento en que el host se vuelve a mostrar activo, demore la conmutación por recuperación al host recién preparado de estas VM.

- **Problema 1797929: Canal de bus de mensajes inactivo tras la actualización del clúster de hosts**
Tras una actualización del clúster de hosts, vCenter 6.0 (y versiones anteriores) no genera el evento "reconectar" (reconnect) y, como resultado, NSX Manager no establece la infraestructura de mensajería en el host. Este problema se solucionó en vCenter 6.5.

Solución alternativa: Vuelva a sincronizar la infraestructura de mensajería de la siguiente manera:

POST `https://<ip>:/api/2.0/nwfabric/configure?action=synchronize`

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

- **Problema 1768144: Las reservas de recursos de dispositivos NSX Edge anteriores que superen los nuevos límites pueden provocar errores durante la actualización o la nueva implementación**
En NSX 6.2.4 y versiones anteriores, podía especificar una gran reserva de recursos para un dispositivo NSX Edge. NSX no aplicaba un valor máximo. Después de actualizar NSX Manager a la versión 6.2.5 o posterior, si Edge tiene recursos reservados (sobre todo memoria) que superan el nuevo valor máximo impuesto para el factor de forma seleccionado, se producen errores durante la actualización o nueva implementación (que activa una actualización) de Edge. Por ejemplo, supongamos que el usuario especificó una reserva de memoria de 1000 MB en un dispositivo Edge GRANDE con una versión anterior a la 6.2.5 y, después de actualizarlo a la versión 6.2.5, cambia el tamaño a COMPACTO. La reserva de memoria especificada por el usuario superará el nuevo valor máximo establecido (en este caso, 512 para un Edge COMPACTO) y se producirá un error en la operación.

Consulte cómo [actualizar la puerta de enlace del servicio Edge \(ESG\)](#) para obtener más información sobre la asignación de recursos a partir de NSX 6.2.5.

Solución alternativa: Use la REST API del dispositivo PUT

`https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/` para volver a configurar la reserva de memoria y que se encuentre dentro de los valores especificados para el factor de forma sin más cambios en el dispositivo. Podrá modificar el tamaño del dispositivo una vez que se complete esta operación.

- **Problema 1600281: En el estado de instalación de USVM para Guest Introspection aparece Error (Failed) en la pestaña Implementaciones de servicio (Service Deployments)**
Si el almacén de datos de copias de seguridad para la Universal SVM de Guest Introspection se desconecta o aparece inaccesible, es necesario reiniciar la USVM o volverla a implementar para su recuperación.

Solución alternativa: Reinicie o vuelva a implementar la USVM para su recuperación.

- **Problema 1660373: vCenter aplica la licencia de NSX caducada**
En la versión vSphere 5.5 actualización 3 o vSphere 6.0.x, se incluye vSphere Distributed Switch en la licencia de NSX. Sin embargo, vCenter no permite que se agreguen hosts ESX a vSphere Distributed Switch si caducó la licencia de NSX.

Solución alternativa: La licencia de NSX debe estar activa para agregar un host a vSphere Distributed Switch.

- **Problema 1569010/1645525:** Al actualizar de la versión 6.1.x a NSX for vSphere 6.2.3 en un sistema conectado a vCenter 5.5, el campo Producto (Product) de la ventana "Asignar clave de licencia" (Assign License Key) muestra la licencia de NSX con el valor genérico de "NSX for vSphere" y no con uno más específico como "NSX for vSphere - Enterprise".

Solución alternativa: Ninguna.

- **Problema 1636916:** En un entorno de vCloud Air, al actualizar la versión de NSX Edge de vCNS 5.5.x a NSX 6.x, las reglas de Edge Firewall con un valor de protocolo de origen de "cualquiera" (any) se cambian a "tcp:cualquiera, udp:cualquiera" (tcp:any, udp:any) Como resultado, se bloquea el tráfico ICMP y se puede apreciar la colocación de paquetes.

Solución alternativa: Antes de actualizar su versión de NSX Edge, cree reglas de Edge Firewall y sustituya el valor "cualquiera" (any) con valores específicos del puerto de origen.

- **Problema 1474238:** Después de la actualización de vCenter, es posible que vCenter pierda conectividad con NSX
Si se utiliza SSO integrado de vCenter y se actualiza vCenter 5.5 a vCenter 6.0, es posible que vCenter pierda conectividad con NSX. Esto sucede si vCenter 5.5 se registró con NSX con el nombre de usuario raíz. En NSX 6.2, el registro de vCenter con raíz es obsoleto.
Nota: Si se utiliza un SSO externo, no es necesario hacer cambios. Puede mantener el mismo nombre de usuario, por ejemplo, admin@miempresa.midominio, y la conectividad de vCenter no se perderá.

Solución alternativa: Registre vCenter con NSX con el nombre de usuario administrator@vsphere.local en lugar del de raíz.

- **Problema 1375794:** Cerrar sistema operativo invitado para máquinas virtuales de agente (SVA) antes de apagar
Cuando se coloca un host en modo de mantenimiento, todos los dispositivos de servicio se apagan, en lugar de cerrarse de manera estable. Esto puede provocar errores en aplicaciones de terceros.

Solución alternativa: Ninguna.

- **Problema 1112628:** No se puede encender el dispositivo de servicio que se implementó con la vista Implementaciones de servicios (Service Deployments)

Solución alternativa: Antes de continuar, compruebe lo siguiente:

- Se completó la implementación de la máquina virtual.
- Ninguna tarea, como clonación, reconfiguración, etc., está en curso en la máquina virtual que se muestra en el panel de tareas de vCenter.
- En el panel de eventos vCenter de la máquina virtual, se muestran los eventos siguientes una vez iniciada la implementación:

Se aprovisionó la máquina virtual de agente <nombre de máquina virtual>
(Agent VM <vm name> has been provisioned).

Marque el agente como disponible para continuar con el flujo de trabajo del agente (Mark agent as available to proceed agent workflow).

En tal caso, elimine la máquina virtual de servicio. En la interfaz de usuario de implementación de servicios, el estado de la implementación es Con errores (Failed). Cuando hace clic en el icono rojo, se muestra una alarma de una máquina virtual de agente no disponible para el host. Cuando resuelve la alarma, se vuelve a implementar la máquina virtual y se enciende.

- Si no están preparados todos los clústeres del entorno, el mensaje de actualización de Distributed Firewall no aparece en la pestaña Preparación del host (Host Preparation) de la página Instalación (Installation)

Cuando se preparan los clústeres para la virtualización de red, se habilita Distributed Firewall en esos clústeres. Si no están preparados todos los clústeres del entorno, el mensaje de actualización de Distributed Firewall no aparece en la pestaña Preparación del host (Host Preparation).

Solución alternativa: Utilice la llamada REST siguiente para actualizar Distributed Firewall:

PUT <https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state>

- **Problema 1215460:** Si se modifica un grupo de servicios después de una actualización para agregar o quitar servicios, estos cambios no se ven reflejados en la tabla del firewall
Los grupos de servicios creados por el usuario se expanden en la tabla Firewall de Edge (Edge Firewall) durante la actualización, es decir, la columna Servicio (Service) de la tabla del firewall muestra todos los servicios incluidos en el grupo de servicios. Si se modifica el grupo de servicios después de una actualización para agregar o quitar servicios, estos cambios no se ven reflejados en la tabla del firewall.

Solución alternativa: Cree un grupo de servicios nuevo con un nombre distinto y, a continuación, utilice este grupo de servicios en la regla del firewall.

- **Problema 1413125:** No se puede volver a configurar SSO después de la actualización
Cuando el servidor de SSO configurado en NSX Manager es el nativo en vCenter Server, no se pueden volver a configurar las opciones de SSO en NSX Manager una vez que vCenter Server se actualizó a la versión 6.0 y NSX Manager a la versión 6.x.

Solución alternativa: Ninguna.

- **Problema 1263858:** La VPN SSL no envía una notificación de actualización al cliente remoto
La puerta de enlace de la VPN SSL no envía una notificación de actualización a los usuarios. El administrador debe comunicar manualmente a los usuarios remotos que la puerta de enlace de la VPN SSL (servidor) está actualizada y que deben actualizar los clientes.

Solución alternativa: Los usuarios deben desinstalar la versión anterior del cliente e instalar la última versión manualmente.

- **Problema 1462319:** El VIB esx-dvfilter-switch-security ya no está presente en el resultado del comando "esxcli software vib list | grep esx"
A partir de NSX 6.2, los módulos esx-dvfilter-switch-security se incluyen en el VIB esx-vxlan. Los únicos VIB de NSX instalados para la versión 6.2 son esx-vsip y esx-vxlan. Durante una actualización de NSX a 6.2, el VIB antiguo esx-dvfilter-switch-security se quita de los hosts ESXi. Desde NSX 6.2.3, se proporciona un tercer VIB, el esx-vdpi, junto con los VIB de NSX esx-vsip y esx-vxlan. Si la instalación se realiza correctamente, se mostrarán los 3 VIB.

Solución alternativa: Ninguna.

- **Problema 1481083:** Después de la actualización, es posible que los enrutadores lógicos con formación de equipos por conmutación por error explícita configurada no puedan reenviar correctamente los paquetes
Cuando los hosts ejecutan ESXi 5.5, la directiva de formación de equipos de NSX 6.2 por conmutación por error explícita no es compatible con varios vínculos superiores activos en los enrutadores lógicos distribuidos.

Solución alternativa: Altere la directiva de formación de equipos por conmutación por error explícita de modo que haya solo un vínculo superior activo y que los demás vínculos superiores se encuentren en modo en espera.

- **Problema 1411275:** vSphere Web Client no muestra la pestaña Redes y seguridad (Networking and Security) después de la copia de seguridad y restauración en NSX for vSphere 6.2
Cuando realiza una operación de copia de seguridad y restauración después de la actualización a NSX for vSphere 6.2, vSphere Web Client no muestra la pestaña Redes y seguridad (Networking and Security).

Solución alternativa: Cuando se restaura una copia de seguridad de NSX Manager, se cierra la sesión del Administrador de dispositivos (Appliance Manager). Espere unos minutos antes de iniciar sesión en vSphere Web Client.

- **No se enciende la máquina virtual de servicios implementada desde la pestaña Implementaciones de servicios (Service Deployments) en la página Instalación (Installation)**

Solución alternativa:

1. Quite manualmente la máquina virtual de servicio del grupo de recursos *Agentes de ESX* (ESX Agents) en el clúster.
2. Haga clic en **Redes y seguridad** (Networking and Security) y, a continuación, en **Instalación** (Installation).
3. Haga clic en la pestaña **Implementaciones de servicios** (Service Deployments).
4. Seleccione el servicio adecuado y haga clic en el icono **Resolver** (Resolve).
Se vuelve a implementar la máquina virtual de servicio.

- **Problema 1764460:** Después de completar la preparación del host, todos los miembros del clúster están listos, pero aparece de forma errónea que el estado del clúster es "No válido" (Invalid)

Una vez que complete la preparación del host, todos los miembros de clúster muestran el estado correcto "Listo" (Ready), pero el estado del clúster aparece como "No válido" (Invalid). Se indica que debe reiniciar el host aunque ya lo hizo.

Solución alternativa: Haga clic en el icono de advertencia rojo y seleccione **Resolver** (Resolve).

Problemas conocidos de NSX Manager

- **Problema 1892999:** No se puede modificar los criterios de selección única, aunque no existan máquinas virtuales conectadas a la etiqueta de seguridad universal
Si se elimina una máquina virtual conectada a una etiqueta de seguridad universal, un objeto interno que representa la máquina virtual seguirá conectado a esta. Esto ocasiona que el cambio en los criterios de selección universal genere un error que indica que hay etiquetas de seguridad universal que aún están conectadas a las máquinas virtuales.

Solución alternativa: Elimine todas las etiquetas de seguridad universal y, a continuación, cambie los criterios de selección universal.

- **Problema 1926309:** El complemento de NSX Manager no se carga y muestra el mensaje "Excepción de autenticación" (Authentication Exception)
A veces, el complemento de NSX Manager no puede cargar ninguna página y, finalmente, muestra un error de tiempo de espera.

Solución alternativa: Reinicie el servicio de gestión de NSX o reinicie el dispositivo NSX Manager.

- **Problema 1904842:** NSX Manager no se está registrando con vCenter ni con Platform Service Controller
NSX Manager no aparece en la interfaz de usuario y se produce un error en todas las llamadas de REST a NSX Manager.

Solución alternativa: Reinicie el servicio de gestión de NSX o reinicie el dispositivo NSX Manager.

- **Problema 1801325:** Registros y eventos del sistema "Críticos" (Critical) generados en el NSX

Manager con un elevado uso de disco o de CPU

Es posible que aparezcan algunos de los siguientes problemas si tiene un elevado uso de espacio de disco, una renovación de datos del trabajo elevada o una cola de trabajos con gran tamaño en NSX Manager:

- Eventos del sistema "Críticos" (Critical) en vSphere Web Client
- Uso elevado de disco en NSX Manager para la partición `/common`
- Uso elevado de CPU durante periodos prolongados o intervalos regulares.
- Impacto negativo en el rendimiento de NSX Manager

Solución alternativa: Póngase en contacto con el servicio de atención al cliente de VMware.

Consulte el [artículo 2147907 de la base de conocimientos de VMware](#) para obtener más información.

- **Problema 1781080: Se produce un error en la configuración de búsqueda de DNS cuando se agrega más de un dominio y se utilizan comas para separarlos**

Al agregar más de un sufijo de búsqueda de dominio a NSX Manager, se producirá un error en todas las búsquedas de DNS que no estén usando el nombre completo. Esto se debe a un problema de formato interno de `/etc/resolv.conf`.

Solución alternativa: Utilice un sufijo de búsqueda de DNS único.

- **Problema 1806368: Reutilizar controladores de un NSX Manager principal en el que se produjo un error y que vuelve a ser principal después de una conmutación por error provoca que la configuración DLR no se envíe a todos los hosts**

En una instalación de Cross-vCenter NSX, cuando se produce un error en el NSX Manager principal, uno secundario pasa a ser principal y se implementa un nuevo clúster del controlador para su uso con el NSX Manager secundario, que ahora es el principal. Cuando el NSX Manager principal vuelve a estar activo, se degrada el NSX Manager secundario y el primario se restaura. En este caso, si vuelve a utilizar los controladores existentes que se implementaron en este NSX Manager principal antes de la conmutación por error, la configuración DLR no se transmite a todos los hosts. Este problema no ocurre si, en su lugar, crea un nuevo clúster del controlador.

Solución alternativa: Implemente un nuevo clúster del controlador para el NSX Manager principal restaurado.

- **Problema 1831131: Se produce un error en la conexión de NSX Manager con SSO al realizar la autenticación con el usuario LocalOS**

Se produce un error en la conexión de NSX Manager con SSO al realizar la autenticación con el usuario LocalOS y aparece el mensaje: "No se pudo establecer comunicación con NSX Manager. Póngase en contacto con el administrador" (Could not establish communication with NSX Manager. Please contact administrator).

Solución alternativa: Agregue la función de administrador de organización para `nsxmanager@localos`, además de `nsxmanager@domain`.

- **Problema 1800820: Se produce un error al actualizar la interfaz UDLR en el NSX Manager secundario si la anterior se eliminó del sistema**

En un escenario donde el servicio de sincronización universal (replicador) deja de funcionar en el NSX Manager principal, debe eliminar las interfaces UDLR (enrutador lógico distribuido universal) y ULS (conmutador lógico universal) del NSX Manager principal, crearlas de nuevo y, a continuación, replicarlas en el NSX Manager secundario. En este caso, la interfaz UDLR no se actualiza en el NSX Manager secundario porque una nueva ULS se crea en ese NSX Manager durante la replicación y la UDLR no se conecta con la nueva ULS.

Solución alternativa: Asegúrese de que se esté ejecutando el replicador y elimine la interfaz UDLR (LIF) del NSX Manager principal que tiene una ULS recién creada como copia de seguridad y vuelva a crear la interfaz UDLR (LIF) con la misma ULS como copia de seguridad.

- **Problema 1772911: NSX Manager trabaja muy lento y el uso de espacio en disco y los tamaños de las tablas de tareas y trabajos aumentan hasta alcanzar cerca del 100% de uso de CPU.**

Experimentará lo siguiente:

- La CPU de NSX Manager presenta un uso cercano al 100% o tiene picos que alcanzan regularmente el 100% de uso y añadir recursos adicionales al dispositivo de NSX Manager no soluciona nada.
- Ejecutar el comando `show process monitor` en la interfaz de líneas de comandos (CLI) de NSX Manager muestra el proceso de Java que consume los ciclos de CPU más altos.
- Ejecutar el comando `show filesystems` en la CLI de NSX Manager muestra que el directorio `/common` utiliza un porcentaje muy alto, como, por ejemplo, superior al 90%.
- Algunos de los cambios de configuración agotan su tiempo de espera (a veces tardan más de 50 minutos) y no son eficaces.

Consulte el [artículo 2147907 de la base de conocimientos de VMware](#) para obtener más información.

Solución alternativa: Póngase en contacto con el servicio de atención al cliente para obtener una solución a este problema.

- **Problema 1785142:** Se produce una demora al mostrar "Problemas de sincronización" (Synchronization Issues) en el NSX Manager principal cuando se bloquea la comunicación entre el NSX Manager principal y el secundario.
Cuando se bloquea la comunicación entre el NSX Manager principal y el secundario, los "Problemas de sincronización" (Synchronization Issues) no aparecen de inmediato en el NSX Manager principal.

Solución alternativa: Espere unos 20 minutos a que se vuelva a establecer la comunicación.

- **Problema 1786066:** En una instalación cross-vCenter de NSX, desconectar un NSX Manager secundario podría impedir que dicho NSX Manager se reconecte como secundario.
En una instalación cross-vCenter de NSX, si desconecta un NSX Manager secundario, puede que no sea capaz de volver a añadir más adelante dicho NSX Manager como NSX Manager secundario. Los intentos de reconectar el NSX Manager como secundario harán que el NSX Manager se muestre como "Secundario" (Secondary) en la pestaña Administración (Management) de vSphere Web Client, pero no se establecerá la conexión con el principal.

Solución alternativa:

1. Desconecte el NSX Manager secundario del NSX Manager primario.
2. Agregue de nuevo el NSX Manager secundario al NSX Manager primario.

- **Problema 1713669:** NSX Manager falla debido a que el disco está lleno cuando el tamaño de `ai_useripmap` de la tabla de base de datos se hace demasiado grande.
Este problema hace que el disco de dispositivo NSX Manager se llene, lo que da lugar al error de NSX Manager. El proceso postgres no puede iniciarse tras un reinicio. La partición `/common` está llena. Esto se produce con mayor frecuencia en los sitios que colocan una carga pesada en el Servidor de registro de eventos (ELS) y en sitios con una gran cantidad de tráfico de Introspección de invitados (Guest Introspection, GI). Los sitios que utilizan Identity Firewall (IDFW) se ven afectados frecuentemente. Consulte el [artículo 2148341 de la base de conocimientos de VMware](#) para obtener más información.

Solución alternativa: Póngase en contacto con el servicio de atención al cliente de VMware para obtener ayuda para solucionar este problema.

- **Problema 1783528:** El uso que hace NSX Manager de los recursos de la CPU aumenta el viernes por la noche/el sábado por la mañana
NSX realiza una sincronización completa con LDAP todos los viernes por la noche. No existe ninguna opción para configurar unidades organizativas o contenedores de Active Directory específicos, por lo que NSX sincroniza todos los objetos relacionados con el dominio proporcionado.

Solución alternativa: Aumentar las vCPU de NSX Manager de 4 a 6

- **Problema 1715354: Demora en la disponibilidad de REST API**

NSX Manager API tarda en activarse y en ejecutarse después de que se reinicie NSX Manager cuando el modo FIPS está activado. Es posible que parezca que la API está bloqueada, pero esto ocurre porque el controlador tarda en volver a establecer la conexión con NSX Manager. Se aconseja que espere a que el servidor de NSX API esté activo y en funcionamiento, y que se asegure de que todos los controladores estén en estado conectado antes de realizar ninguna operación.

- **Problema 1441874: Se produce un error al actualizar un único NSX Manager en un entorno de vCenter Linked Mode**

En un entorno con varios VMware vCenter Server con múltiples NSX Managers, al seleccionar uno o varios NSX Manager desde vSphere Web Client > Redes y seguridad > Instalación > Preparación del host (vSphere Web Client > Networking and Security > Installation > Host Preparation), verá este error:

"No se pudo establecer comunicación con NSX Manager. Póngase en contacto con el administrador" (Could not establish communication with NSX Manager. Please contact administrator).

Solución alternativa: Consulte el [artículo 2127061 de la base de conocimientos de VMware](#) para obtener más información.

- **Problema 1696750: Para asignar una dirección IPv6 a NSX Manager a través de una API de PUT se deberá reiniciar el sistema**

Para cambiar la configuración de red en NSX Manager a través de `https://{NSX Manager IP address}/api/1.0/appliance-management/system/network`, se deberá reiniciar el sistema. Hasta que el sistema se reinicie, se mostrará la configuración existente.

Solución alternativa: Ninguna.

- **Problema 1529178: Si se carga un certificado de servidor que no incluye un nombre común, se mostrará un mensaje de "error interno del servidor"**

Si carga un certificado de servidor que no tenga un nombre común, aparecerá un mensaje "error interno del servidor" ("internal server error").

Solución alternativa: Utilice un certificado de servidor que tenga tanto un SubAltName como un nombre común o, al menos, un nombre común.

- **Problema 1655388: La interfaz de usuario de la versión NSX Manager 6.2.3 se muestra en inglés en lugar de hacerlo en el idioma local cuando se usa el explorador IE11/Edge en sistemas operativos Windows 10 para los idiomas JA, CN y DE**

Al iniciar NSX Manager 6.2.3 con el explorador IE11/Edge en sistemas operativos Windows 10 para los idiomas JA, CN y DE, la interfaz se muestra en inglés.

Solución alternativa:

1. Inicie el Editor del Registro de Microsoft (regedit.exe) y diríjase a Equipo > HKEY_CURRENT_USER > SOFTWARE > Microsoft > Internet Explorer > International.
2. Modifique el valor del archivo *AcceptLanguage* para aceptar el idioma local. Por ejemplo, si desea cambiar el idioma a DE, cambie el valor y asegúrese de que DE aparezca en el primer lugar.
3. Reinicie el explorador e inicie sesión de nuevo en NSX Manager. De esta forma se muestra el idioma correcto.

- **Problema 1435996: Los archivos de registro exportados como CSV desde NSX Manager tienen la marca de tiempo de época en lugar de fecha y hora**

Los archivos exportados en formato .csv desde NSX Manager mediante vSphere Web Client incluyen una marca de tiempo de época en milisegundos, en lugar de mostrar la hora que correspondería a la zona horaria.

Solución alternativa: Ninguna.

- Problema 1644297:** La operación de agregar o eliminar cualquier sección DFW de NSX principal crea dos configuraciones de DFW guardadas en NSX secundario
 En la configuración de Cross-vCenter, cuando se agrega una sección de DFW adicional local o universal al NSX Manager principal, se guardan dos configuraciones de DFW en el NSX Manager secundario. Aunque no afecta a ninguna función, este problema hará que se alcance más rápidamente el límite de configuraciones guardadas y que, posiblemente, se sobrescriban las configuraciones críticas.
Solución alternativa: Ninguna.
- Problema 1477138:** El servicio de gestión de NSX no está disponible si el nombre de host tiene más de 64 caracteres
 Para crear certificados a través de la biblioteca OpenSSL, el nombre de host debe tener 64 caracteres o menos.
- Problema 1437664:** La lista de NSX Manager aparecerá lentamente en Web Client
 En los entornos vSphere 6.0 con varios NSX Manager, vSphere Web Client puede tardar hasta dos minutos en mostrar la lista de los NSX Manager cuando el usuario conectado se está validando con una configuración de grupo de AD grande. Es posible que aparezca un error de tiempo de espera del servicio de datos al intentar mostrar la lista de NSX Manager. No hay solución. Debe esperar a que la lista se cargue o volver a iniciar la sesión para ver la lista de NSX Manager.
- Problema 1534606:** No se puede cargar la página de preparación del host
 Al ejecutar vCenter en modo de conexión, cada vCenter debe estar conectado a un NSX Manager de la misma versión de NSX. Si las versiones de NSX son distintas, vSphere Web Client solo podrá comunicarse con el NSX Manager que esté ejecutando la versión posterior de NSX. Aparecerá un error similar al siguiente: "No se ha podido establecer la comunicación con NSX Manager. Póngase en contacto con el administrador (Could not establish communication with NSX Manager. Please contact administrator)" en la pestaña Preparación del host (Host Preparation).
Solución alternativa: Deberá actualizar todos los NSX Manager a la misma versión del software de NSX.
- Problema 1386874:** No se muestra la pestaña Redes y seguridad (Networking and security) en vSphere Web Client
 Una vez que vSphere se actualizó a la versión 6.0, no se puede ver la pestaña Redes y seguridad (Networking and Security) cuando se inicia sesión en vSphere Web Client con el nombre de usuario raíz.
Solución alternativa: Inicie sesión como administrator@vsphere.local o como cualquier otro usuario de vCenter que existía en vCenter Server antes de la actualización y cuyo rol se definió en NSX Manager.
- Problema 1027066:** Es posible que vMotion de NSX Manager muestre el mensaje de error "El adaptador de red 1 de la tarjeta Ethernet virtual no es compatible" (Virtual ethernet card Network adapter 1 is not supported)
 Se puede ignorar este error. Las redes funcionan correctamente después de vMotion.
- Problema 1460766:** La interfaz de usuario de NSX Manager no cierra automáticamente la sesión después de cambiar la contraseña con la interfaz de línea de comandos de NSX
 Si se está conectado a NSX Manager y se acaba de cambiar la contraseña con la CLI, es posible continuar conectado a la interfaz de usuario de NSX Manager con la contraseña antigua. Por lo general, el cliente NSX Manager debería cerrar la sesión automáticamente si se agota el tiempo de espera de la sesión por inactividad.
Solución alternativa: Cierre la sesión de la interfaz de usuario de NSX Manager y vuelva a iniciar sesión con la contraseña nueva.

- **Problema 1467382: No se puede editar un nombre de host de red**

Una vez que inicia sesión en el dispositivo virtual NSX Manager y se desplaza hasta Administración de dispositivos (Appliance Management), hace clic en Administrar configuración de dispositivos (Manage Appliance Settings) y en Red (Network) en la sección Configuración (Settings) para editar el nombre de host de red, es posible que aparezca un error de lista de nombres de dominio no válida. Esto sucede cuando los nombres de dominio especificados en el campo Buscar dominios (Search Domains) se separan con caracteres de espacios en blanco en lugar de comas. NSX Manager solo acepta nombres de dominio separados por coma.

Solución alternativa:

1. Inicie sesión en el dispositivo virtual NSX Manager.
2. En Administración de dispositivos (Appliance Management), haga clic en Administrar configuración de dispositivos (Manage Appliance Settings).
3. En el panel Configuración (Settings), haga clic en Red (Network).
4. Haga clic en Editar (Edit) junto a Servidores DNS (DNS Servers).
5. En el campo Buscar dominios (Search Domains), reemplace todos los caracteres de espacios en blanco por comas.
6. Haga clic en Aceptar (OK) para guardar los cambios.

- **Problema 1436953: Se genera un evento falso del sistema incluso después de restaurar correctamente NSX Manager desde una copia de seguridad**

Después de restaurar correctamente NSX Manager desde una copia de seguridad, aparecen los eventos del sistema siguientes en vSphere Web Client cuando se desplaza hasta Redes y seguridad (Networking & Security): NSX Manager: Monitor (Supervisar): Eventos del sistema (System Events).

- Restore of NSX Manager from backup failed (with Severity=Critical).
- Restore of NSX Manager successfully completed (with Severity=Informational).

Solución alternativa: Si el mensaje del evento del sistema final muestra que se completó correctamente, puede omitir los mensajes de eventos generados por el sistema.

- **Problema 1843197: El adaptador de red de NSX Manager muestra una advertencia que indica que este tipo de adaptador de red no es compatible con {0} otras versiones de Linux de 64 bits**
Tras instalar y configurar correctamente NSX Manager, desplácese a vCenter > Editar configuración (Edit settings) del NSX Manager implementado. En Adaptador de red (Network Adapter), se muestra una advertencia que indica que este tipo de adaptador de red no es compatible con {0} otras versiones de Linux de 64 bits ("This type of network adapter is not supported by {0} Other Linux (64-bit)")

Problemas conocidos de NSX Controller

- **Problema 1856465: Si un host ESXi está desactivado en uno de los sitios de un entorno de Cross-vCenter NSX, el modo CDO no se habilita en ese sitio**

Si un host ESXi está desactivado en un sitio, no se podrá habilitar ni deshabilitar correctamente el modo CDO en dicho sitio.

Si el host está desactivado en uno de los sitios secundarios, la operación del modo CDO se realizará correctamente en el sitio principal. Sin embargo, se producirá un error en la operación del modo CDO en el sitio secundario. Esto puede ocasionar un comportamiento incoherente.

Solución alternativa: Este problema afecta a NSX 6.3.0 y versiones posteriores.

- Asegúrese de que todos los hosts ESXi están activos antes de realizar las operaciones CDO.
- Para recuperarse de un estado incoherente, quite el host del inventario de vCenter y vuelva a

agregarlo.

- **Problema 1965859:** La memoria de NSX Controller aumenta con la configuración VTEP del hardware, lo que causa un uso elevado de la CPU
Se observa un aumento de la memoria de procesamiento de NSX Controller cuando se ejecutan configuraciones VTEP del hardware durante varios días. El aumento de memoria causa un uso elevado de la CPU que dura algún tiempo (minutos) mientras NSX Controller recupera la memoria. Durante este tiempo, la ruta de datos se ve afectada.

Solución alternativa: Póngase en contacto con el servicio de atención al cliente de VMware.

Problemas conocidos de NSX Edge y redes lógicas

- **Problema 1904612:** El túnel VPN de la capa 2 se muestra como "activo" (up) en el servidor de L2VPN cuando el cliente se desconecta
El servidor de NSX Edge seguirá mostrando que el túnel VPN está activo si crea una VPN de L2 entre dos NSX Edge y, a continuación, apaga el cliente de NSX Edge.

Solución alternativa: Ninguna.

- **Problema 1242207:** El cambio del ID del enrutador durante el tiempo de ejecución no se refleja en la topología OSPF
Si se intenta cambiar el ID del enrutador sin deshabilitar OSPF, no vuelve a generarse ningún anuncio sobre el estado del vínculo (LSA) con este ID de enrutador, lo que provoca la pérdida de rutas externas de OSPF.

Deshabilite OSPF, cambie el ID del enrutador y, a continuación, vuelva a habilitar OSPF.

- **Problema 1894277:** La PSK de configuración del sitio de IPSec no se conserva cuando se cambia la subred local o del mismo nivel
Como la PSK enmascarada se guarda en la base de datos, el túnel entre los pares no aparecerá debido a que la contraseña no coincide.

Solución alternativa: Vuelva a configurar la configuración de IPSec con una contraseña válida.

- **Problema 1492497:** No se puede filtrar el tráfico DHCP de NSX Edge
No puede aplicar ningún filtro de firewall al tráfico DHCP de un NSX Edge, porque el servidor DHCP de un NSX Edge utiliza sockets sin procesar que omiten la pila TCP/IP.

Solución alternativa: Ninguna.

- **Problema 1781438:** En los dispositivos NSX Edge de DLR o ESG, el servicio de enrutamiento no envía ningún mensaje de error si recibe más de una vez el atributo de ruta BGP MULTI_EXIT_DISC.
El enrutador de Edge o el enrutador lógico distribuido no envían ningún mensaje de error si reciben el atributo de ruta BGP MULTI_EXIT_DISC más de una vez. Según la sección 5 de RFC 4271, el mismo atributo (atributo del mismo tipo) no puede aparecer más de una vez en el campo Atributos de ruta (Path Attributes) de un mensaje ACTUALIZAR (UPDATE) en particular.

Solución alternativa: Ninguna.

- **Problema 1786515:** Un usuario con privilegios "Administrador de seguridad" (Security Administrator) no puede editar la configuración del equilibrador de carga utilizando la IU de vSphere Web Client
Un usuario con privilegios "Administrador de seguridad" (Security Administrator) para un NSX Edge específico no puede editar la Configuración global del equilibrador de carga (Global Load Balancer Configuration) de ese Edge mediante la IU de vSphere Web Client. Aparece el siguiente mensaje de error: "El usuario no tiene autorización para acceder al objeto Global ni a la función si.service. Compruebe el ámbito de acceso del objeto y los permisos para las funciones de este usuario" ("User is not authorized to access object Global and feature si.service, please check object access scope and feature permissions for the user").

Solución alternativa: Ninguna.

- **Problema 1849042/1849043: Se bloquea la cuenta del administrador después de configurar la caducidad de la contraseña en el dispositivo NSX Edge**
Si se configura la caducidad de la contraseña del usuario administrador en el dispositivo NSX Edge, cuando esta caduca, existe un periodo de 7 días durante el cual se le solicitará al usuario que cambie la contraseña cuando inicie sesión en el dispositivo. El error que se produce al cambiar la contraseña puede provocar que se bloquee la cuenta. Además, si la contraseña se cambia cuando se inicia sesión en la solicitud de CLI, es posible que la nueva contraseña no cumpla la directiva de contraseña segura que aplican la IU y REST.

Solución alternativa: Para evitar este problema, use siempre la IU o REST API para cambiar la contraseña del administrador antes de que la contraseña existente caduque. Si se bloquea la cuenta, también puede usar la IU o REST API para configurar una nueva contraseña y la cuenta se volverá a desbloquear.

- **Problema 1711013: Se tarda aproximadamente 15 minutos en sincronizar la FIB entre el NSX Edge activo y en espera tras reiniciar la máquina virtual en espera.**
Cuando un NSX Edge en espera se desconecta, no se cierra la sesión TCP entre el modo en espera y el activo. El Edge activo detectará que la espera está inactiva tras el error Keepalive (15 minutos). Tras 15 minutos, se establece una nueva conexión de socket con el Edge en espera y la FIB se sincroniza entre el Edge activo y el que está en espera.

Solución alternativa: Ninguna.

- **Problema 1733282: NSX Edge ya no es compatible con las rutas estáticas del dispositivo**
NSX Edge no admite la configuración de rutas estáticas con la dirección de salto siguiente NULL.

Solución alternativa: Ninguna.

- **Problema 1860583: Evite usar un servidor de sysloggers remoto como FQDN si el DNS no está accesible.**
En una instancia de NSX Edge, si se configuran los servidores de sysloggers remotos mediante FQDN y el DNS no está accesible, es posible que la funcionalidad de enrutamiento se vea afectada. El problema podría no producirse de forma coherente.

Solución alternativa: Se recomienda utilizar direcciones IP en lugar de FQDN.

- **Problema 1850773: Configuración no válida de los informes NAT de NSX Edge cuando se utilizan varios puertos en la configuración del equilibrador de carga**
Este problema ocurre cada vez que configure un servidor virtual del equilibrador de carga con más de un puerto. Debido a esto, NAT no se podrá administrar mientras exista este estado de configuración para las instancias de NSX Edge afectadas.

Solución alternativa: Consulte el [artículo 2149942 de la base de conocimientos de VMware](#) para obtener más información y una solución alternativa.

- **Problema 1764258: Tráfico bloqueado hasta 8 minutos después de que se produzca un error de HA o una sincronización forzada en NSX Edge configurada con una subinterfaz**
Si se activa un error de HA o inicia una sincronización forzada en una subinterfaz, el tráfico se bloqueará hasta 8 minutos.

Solución alternativa: No utilice subinterfaces para HA.

- **Problema 1767135: Se producen errores al intentar acceder a los perfiles de aplicaciones y certificados que se encuentran en el equilibrador de carga**
Los usuarios con privilegios de Administrador de seguridad (Security Admin) y alcance de Edge no pueden acceder a los perfiles de aplicaciones y certificados que se encuentran en el equilibrador de carga. vSphere Web Client muestra mensajes de error.

Solución alternativa: Ninguna.

- **Problema 1792548:** NSX Controller puede quedarse atascado en el mensaje: "Esperando unirse al clúster" (Waiting to join cluster)

NSX Controller puede quedarse atascado en el mensaje: "Esperando unirse al clúster" ("Waiting to join cluster") (comando de la CLI: `show control-cluster status`). Esto se produce porque se configuró la misma dirección IP para las interfaces `eth0` y `breth0` del controlador al mismo tiempo que este aparece. Para comprobarlo, utilice en el controlador el siguiente comando de la CLI: `show network interface`

Solución alternativa: Póngase en contacto con el servicio de atención al cliente de VMware.

- **Problema 1747978:** Las adyacencias OSPF se eliminan con la autenticación MD5 después de la conmutación por error de NSX Edge HA

En un entorno NSX for vSphere 6.2.4 donde NSX Edge está configurado para HA con el reinicio OSPF configurado y se usa MD5 para la autenticación, se produce un error al iniciar OSPF. Las adyacencias se forman solo después de que caduque el temporizador de inactividad en los nodos de los vecinos OSPF.

Solución alternativa: Ninguna

- **Problema 1804116:** El enrutador lógico entra en un estado Incorrecto (Bad) en un host que ha perdido la comunicación con NSX Manager.

Si un enrutador lógico se alimenta o reimplementa en un host que ha perdido la comunicación con NSX Manager (debido a un problema de comunicación del host o a un error en la actualización/instalación de NSX VIB), el enrutador lógico entrará en un estado Incorrecto (Bad) y fallará la operación de recuperación automática continua mediante la sincronización forzada.

Solución alternativa: Tras resolver el problema de comunicación del host y NSX Manager, reinicie NSX Edge de forma manual y espere a que aparezcan todas las interfaces. Esta solución alternativa solo es necesaria para enrutadores lógicos y no para la puerta de enlace de servicios de NSX Edge (ESG), porque el proceso de recuperación automática mediante sincronización forzada reinicia NSX Edge.

- **Problema 1783065:** No se puede configurar el equilibrador de carga para el puerto UDP junto con TCP mediante direcciones IPv4 e IPv6 conjuntamente.

UDP solo admite `ipv4-ipv4`, `ipv6-ipv6` (frontend-backend). Hay un error en NSX Manager que hace que incluso la dirección local de vínculo IPv6 se lea e inserte como dirección IP del objeto de agrupamiento y no se le permite seleccionar el protocolo de IP para utilizarlo en la configuración de LB.

A continuación se presenta una configuración de LB de muestra que demuestra este problema: En la configuración del equilibrador de carga, el grupo "vCloud Connector" se configura con un objeto de agrupamiento (vm-2681) como miembro de grupo. Este objeto contiene tanto direcciones IPv4 como IPv6, que no admite el motor LB L4.

```
{
    "algorithm" : {
        ...
    },
    "members" : [
        {
            ... ,
            ...
        }
    ],
    "applicationRules" : [],
    "name" : "vCloud_Connector",
```

```

        "transparent" : {
            "enable" : false
        }
    }

    {
        "value" : [
            "fe80::250:56ff:feb0:d6c9",
            "10.204.252.220"
        ],
        "id" : "vm-2681"
    }
}

```

Solución alternativa:

- Opción 1: Introduzca la dirección IP del miembro del grupo en lugar de objetos de agrupamiento en el miembro del grupo.
- Opción 2: No utilice IPv6 en las VM.

- **Problema 1777792:** La conexión de IPsec falla si se establece un endpoint par como "CUALQUIERA" (ANY).

Cuando la configuración de IPsec de NSX Edge establece un endpoint par remoto como CUALQUIERA (ANY), Edge actúa como un "servidor" IPsec y espera que los pares remotos inicien las conexiones. No obstante, cuando un iniciador envía una solicitud de autenticación utilizando PSK+XAUTH, Edge muestra este mensaje de error: "mensaje de modo principal inicial recibido en XXX.XXX.XX.XX:500, pero no se ha establecido ninguna conexión autorizada mediante policy=PSK+XAUTH" (initial Main Mode message received on XXX.XXX.XX.XX:500 but no connection has been authorized with policy=PSK+XAUTH) e IPsec no se puede establecer.

Solución alternativa: Utilice la dirección IP de endpoint par específica o el FQDN en la configuración IPsec VPN en lugar de CUALQUIERA (ANY).

- **Problema 1741158:** Si crea un nuevo NSX Edge sin configurar y le aplica configuración, puede producirse una activación prematura del servicio de Edge.
Si usa NSX API para crear un nuevo NSX Edge sin configurar, después realiza una llamada API para deshabilitar uno de los servicios de Edge (por ejemplo, asigna el valor false a dhcp-enabled) y, finalmente, aplica cambios de configuración al servicio de Edge deshabilitado, este se activará inmediatamente.

Solución alternativa: Después de hacer cambios en la configuración de un servicio de Edge que quiere mantener en estado deshabilitado, realice de forma inmediata una llamada PUT para asignarle el valor "false" a la marca habilitada de ese servicio.

- **Problema 1758500:** La ruta estática con varios saltos siguientes no se instala en las tablas de enrutamiento y reenvío de NSX Edge si al menos uno de los saltos siguientes configurados es la dirección IP de la vNIC de Edge.
Con ECMP y varias direcciones de salto siguiente, NSX permite que la dirección IP de la vNIC de Edge se configure como salto siguiente si al menos una de las direcciones IP de salto siguiente es válida. Esto se acepta sin errores ni advertencias, pero la ruta de la red se elimina de la tabla de reenvío/enrutamiento de Edge.

Solución alternativa: No configure la dirección IP de la vNIC de Edge como salto siguiente en rutas estáticas si utiliza ECMP.

- **Problema 1716464:** El equilibrador de carga NSX no enrutará las máquinas virtuales etiquetadas recientemente con una etiqueta de seguridad (Security).

Si se implementan dos máquinas virtuales con una etiqueta dada y, a continuación, se configura un LB para enrutar a esa etiqueta, el LB se enrutará correctamente a esas dos máquinas virtuales. Sin embargo, si se implementa una tercera máquina virtual con esa etiqueta, el LB solo enrutará las dos primeras.

Solución alternativa: Haga clic en Guardar (Save) en el Grupo LB (LB Pool). Esto hará que se vuelvan a examinar las máquinas virtuales y se empiece a enrutar a las nuevas máquinas virtuales etiquetadas.

- **Problema 1753621:** Cuando Edge con AS local y privada envía enrutamientos a pares EGBP, todas las rutas privadas AS se eliminan de las actualizaciones de enrutamiento BGP enviadas. NSX tiene actualmente una limitación que evita que comparta la ruta AS completa con vecinos eGBP cuando la ruta AS solo contiene rutas AS privadas. Mientras que este es el comportamiento esperado en la mayoría de los casos, existen casos en los que el administrador pueda querer compartir rutas AS privadas con un vecino eGBP.

Solución alternativa: No existe ninguna solución disponible para que Edge anuncie todas las rutas AS en la actualización de BGP.

- **Problema 1461421:** El resultado del comando "show ip bgp neighbor" para NSX Edge retiene el recuento del historial de las conexiones establecidas previamente
El comando "show ip bgp neighbor" muestra el número de veces que la máquina de estado BGP cambió al estado establecido para un par ya existente. Cambiar la contraseña utilizada con la autenticación MD5 hace que la conexión de dicho par se elimine y se vuelva a crear, acción que a su vez limpiará los contadores. Este problema no sucede con Edge DLR.

Solución alternativa: Para limpiar los contadores, ejecute el comando "clear ip bgp neighbor".

- **Problema 1656713:** Faltan directivas de seguridad (SP) IPsec en NSX Edge tras conmutación por error de HA y el tráfico no fluye a través del túnel
La conmutación En espera (Standby)>Activa (Active) no hará posible que el tráfico fluya en los túneles de IPsec.

Solución alternativa: Deshabilite o habilite IPsec tras la conmutación de NSX Edge.

- **Problema 1354824:** Cuando una máquina virtual de Edge está dañada o no se puede establecer la comunicación con ella por causas tales como un fallo en la alimentación, se activan los eventos del sistema al fallar la comprobación del estado de NSX Manager
En la pestaña Eventos del sistema (System Events) se muestran los eventos con el estado "Error de comunicación con Edge" (Edge Unreachability). Puede que la lista de dispositivos NSX Edge siga mostrando Implementado (Deployed) en el Estado (Status).

Solución alternativa: Utilice la siguiente API para obtener información detallada sobre el estado de NSX Edge:

```
GET https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status?detailedStatus=true
```

- **Problema 1647657:** Los comandos para Mostrar (Show) en un host ESXi con visualización del enrutador lógico distribuido (Distributed Logical Router, DLR) no muestran más de 2.000 rutas por instancia DLR

Los comandos para Mostrar (Show) en un host ESXi con visualización DLR habilitada no muestran más de 2.000 rutas por instancia DLR, aunque haya en ejecución un número superior a este. Se trata solo de un problema de visualización, por lo que las rutas de datos funcionarán según lo esperado en todas las rutas.

Solución alternativa: Ninguna.

- **Problema 1634215:** El resultado de los comandos CLI de OSPF no indica si el enrutamiento está

deshabilitado

Cuando el protocolo OSPF está deshabilitado, el resultado de los comandos CLI de enrutamiento no muestra ningún mensaje que indique que *"El protocolo OSPF está deshabilitado" (OSPF is disabled)*. El resultado está vacío:

Solución alternativa: El comando `show ip ospf` muestra el estado correcto.

- **Problema 1647739:** Implementar de nuevo una máquina virtual de Edge después de una operación de vMotion hace que la máquina virtual de DLR o Edge se vuelva a colocar en el clúster original.

Solución alternativa: Para ubicar la máquina virtual de Edge en un clúster o grupo de recursos diferente, use la interfaz de usuario de NSX Manager para configurar la ubicación que desee.

- **Problema 1463856:** Cuando NSX Edge Firewall esté habilitado, se bloquearán las conexiones TCP existentes

Las conexiones TCP están bloqueadas por el firewall de Edge con estado, ya que no se puede ver el protocolo inicial de enlace de tres vías.

Solución alternativa: Para controlar los flujos existentes, siga estas instrucciones. Use la API REST de NSX para habilitar la marca "tcpPickOngoingConnections" en la configuración global del firewall. Esto cambia el firewall de un modo estricto a un modo más permisivo. El siguiente paso es habilitar el firewall. Una vez seleccionadas las conexiones existentes (esto puede producirse unos minutos después de habilitar el firewall), vuelva a establecer la marca "tcpPickOngoingConnections" en falso (false) para que el firewall funcione en modo estricto. (Esta configuración es persistente.)

```
PUT /api/4.0/edges/{edgeId}/firewall/config/global
```

```
<globalConfig>
```

```
<tcpPickOngoingConnections>true</tcpPickOngoingConnections>
```

```
</globalConfig>
```

- **Problema 1374523:** Es necesario reiniciar ESXi o ejecutar `[services.sh restart]` tras la instalación del VIB de VXLAN para que los comandos de VXLAN estén disponibles al utilizar `esxcli`. Tras la instalación de VXLAN VIB, debe reiniciar ESXi o bien ejecutar el comando `[services.sh restart]` para que los comandos de VXLAN estén disponibles al utilizar `esxcli`.

Solución alternativa: En vez de utilizar `esxcli`, utilice `localcli`.

- **Problema 1525003:** La restauración de una copia de seguridad de NSX Manager con una contraseña incorrecta falla silenciosamente, ya que no se puede acceder a carpetas raíz esenciales

Solución alternativa: Ninguna.

- **Problema 1637639:** Al utilizar el cliente PHAT de la VPN SSL de Windows 8, la IP virtual no se asigna desde el grupo de IP

En Windows 8, la dirección IP virtual no se asigna, como cabría esperar, desde el grupo de IP cuando se asigna una nueva dirección IP mediante la puerta de enlace de servicios Edge o cuando el grupo de IP cambia para usar un intervalo de IP diferente.

Solución alternativa: Este problema solo ocurre en Windows 8. Use un sistema operativo Windows diferente para no experimentar este problema.

- **Problema 1628220:** Las observaciones de NetX o DFW no se muestran en el receptor. Es posible que Traceflow no muestre las observaciones de NetX y DFW en el lado del receptor si se cambió el puerto del conmutador asociado con la vNIC de destino. Este no será fijo para las versiones de vSphere 5.5. En las versiones vSphere 6.0 y posteriores no se produce este problema.
Solución alternativa: No deshabilite la vNIC. Reinicie la máquina virtual.

- **Problema 1483426:** El estado del servicio de VPN L2 e IPsec se muestra como inactivo aunque el servicio no esté habilitado

En la ficha Configuración (Settings) de la interfaz de usuario, el estado del servicio L2 aparecerá inactivo mientras que en API, el estado de servicio aparecerá activo. El servicio IPsec y VPN L2 se

muestran siempre inactivos en la ficha Configuración (Settings) si no se actualiza la página de la interfaz de usuario.

Solución alternativa: Actualizar la página.

- **Problema 1446327:** Es posible que el tiempo de espera finalice en algunas aplicaciones basadas en TCP si se conectan a través de NSX Edge

El tiempo de espera de inactividad predeterminado de la conexión TCP es 3600 segundos. NSX Edge elimina la inactividad de las conexiones que supere al tiempo de espera de inactividad y desecha dichas conexiones.

Solución alternativa:

1. Si la aplicación tiene un tiempo de inactividad relativamente largo, active los keepalive de TCP en los hosts configurando `keep_alive_interval` en menos de 3600 segundos.
2. Aumente el tiempo de espera de inactividad de Edge TCP a más de 2 horas a través de la siguiente API REST de NSX. Puede aumentarlo a 9000 segundos: URL de la API de NSX:
`/api/4.0/edges/{edgeId}/systemcontrol/config PUT Method <systemControl>
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</property> </systemControl>`

- **Problema 1089238:** No se puede configurar OSPF en más de un vínculo superior de DLR Edge
Actualmente no es posible configurar OSPF en más de uno de los ocho vínculos superiores de DLR Edge. Esta limitación es un resultado del uso compartido de una única dirección de reenvío por instancia DLR.

Solución alternativa: Esta es una limitación actual del sistema y no hay solución alternativa.

- **Problema 1499978:** Los mensajes de syslog de Edge no llegan al servidor syslog remoto
Inmediatamente después de la implementación, el servidor syslog de Edge no puede resolver los nombres de host de ningún servidor syslog remoto configurado.

Solución alternativa: Configure los servidores de Syslog remotos con sus direcciones IP o utilice la interfaz de usuario para forzar la sincronización de Edge.

- **Problema 1489829:** Los ajustes de configuración del cliente DNS del enrutador lógico no se aplicaron por completo luego de la actualización de la API Edge REST

Solución alternativa: Cuando utilice una API REST para configurar el reenviador de DNS (resolución), realice los pasos siguientes:

1. Especifique la configuración de los servidores XML del cliente DNS de tal forma que coincida con la configuración del reenviador de DNS.
2. Habilite el reenviador de DNS y asegúrese de que la configuración del reenviador sea la misma que la configuración de los servidores del cliente DNS especificada en la configuración de XML.

- **Problema 1243112:** Mensaje de error y validación ausentes en salto siguiente no válido en la ruta estática, con ECMP habilitado

Cuando se intenta agregar una ruta estática, con ECMP habilitado, si la tabla de enrutamiento no contiene una ruta predeterminada y hay un salto siguiente al que no se puede acceder en la configuración de la ruta estática, no se muestra ningún mensaje de error y la ruta estática no se instala.

Solución alternativa: Ninguna.

- **Problema 1281425:** Si una máquina virtual NSX Edge con una subinterfaz respaldada por un conmutador lógico se elimina a través de la interfaz de usuario de vCenter Web Client, es posible que la ruta de datos no funcione para una máquina virtual nueva que se conecta al mismo puerto

Cuando se elimina la máquina virtual Edge a través de la interfaz de usuario de vCenter Web Client (y no desde NSX Manager), el tronco de VXLAN configurado en dvPort por canal opaco no se restablece. Esto se debe a que NSX Manager administra la configuración del tronco.

Solución alternativa: Elimine manualmente la configuración del tronco de VXLAN con los pasos siguientes:

1. Desplácese hasta el Explorador de objetos administrados de vCenter (vCenter Managed Object Browser); para ello, escriba lo siguiente en la ventana del explorador:
`https://<vc-ip>/mob?vmob1=1`
2. Haga clic en **Contenido (Content)**.
3. Recupere el valor `dvsUuid` con los pasos siguientes.
 - a. Haga clic en el vínculo `rootFolder` (por ejemplo, `group-d1(Datacenters)`).
 - b. Haga clic en el vínculo del nombre del centro de datos (por ejemplo, `datacenter-1`).
 - c. Haga clic en el vínculo `networkFolder` (por ejemplo, `group-n6`).
 - d. Haga clic en el vínculo del nombre de DVS (por ejemplo, `dvs-1`).
 - e. Copie el valor de `uuid`.
4. Haga clic en **DVSManager** y, a continuación, en **updateOpaqueDataEx**.
5. En **selectionSet**, agregue el XML siguiente.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>value</dvsUuid>
  <portKey>value</portKey> <!--port number of the DVPD where trunk vnic got
connected-->
</selectionSet>
```

6. En **opaqueDataSpec**, agregue el XML siguiente.

```
<opaqueDataSpec>
  <operation>remove</operation>
  <opaqueData>
    <key>com.vmware.net.vxlan.trunkcfg</key>
    <opaqueData></opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

7. Establezca **isRuntime** en falso.
8. Haga clic en **Invocar método (Invoke Method)**.
9. Repita los pasos 5 a 8 para cada puerto troncal configurado en la máquina virtual Edge eliminada.

- **Problema 1637939: No se admiten certificados MD5 al implementar puertas de enlace de hardware**

Al implementar conmutadores de puerta de enlace de hardware como VTEP para realizar un puente de VLAN L2 a VXLAN lógico, los conmutadores físicos admiten al menos certificados SHA1 SSL para la conexión OVSDb entre el controlador NSX y el conmutador OVSDb.

Solución alternativa: Ninguna.

- **Problema 1637943: No se admiten los modos de replicación Híbrido (Hybrid) o Multidifusión (Multicast) para los VNI que tienen enlaces de puerta de enlace de hardware**

Los conmutadores de puerta de enlace de hardware, cuando se usan como VTEP para realizar un puente de VXLAN a VLAN L2, admiten solo el modo de replicación Unidifusión (Unicast).

Solución alternativa: Utilice solo el modo de replicación Unidifusión (Unicast).

Problemas conocidos de los servicios de seguridad

- **Problema 1918023: USVM de Guest Introspection consume el 100 % de la memoria**

USVM de Guest Introspection consume el 100 % de la memoria, lo que puede hacer que las máquinas virtuales invitadas pierdan la conectividad a las USVM de Guest Introspection.

Solución alternativa: Consulte el [artículo 2151235 de la base de conocimientos de VMware](#) para obtener más información y soluciones alternativas.

- **Problema 1897878:** Los eventos y las tareas de ESXi muestran el mensaje de error "Comunicación perdida con el módulo ESX" (Lost Communication with ESX module)
Si el módulo Guest Introspection del host ESXi (EPsec Mux) pierde la comunicación con el módulo ESX, el error "Comunicación perdida con el módulo ESX" (Lost Communication with ESX module) aparece en los hosts ESXi.

Solución alternativa: Consulte el [artículo 2151235 de la base de conocimientos de VMware](#) para obtener más información y soluciones alternativas.

- **Problema 1944599:** Las IP traducidas no se agregan a los filtros vNIC, lo que provoca que Distributed Firewall pierda tráfico

Cuando se implementan nuevas máquinas virtuales, los filtros de vNIC no se actualizan con el conjunto adecuado de IP, lo que provoca que Distributed Firewall bloquee el tráfico.

Solución alternativa:

1. Fuerce la sincronización de las reglas del firewall distribuido en los clústeres afectados con nuevas máquinas virtuales implementadas. Consulte "Forzar sincronización de las reglas de Firewall".
2. Haga clic en Editar (Edit) en el grupo de seguridad al que le faltan IP de máquinas virtuales y envíelo sin cambios.

- **Problema 1854661:** En una configuración cross-VC, las reglas del filtro del firewall no muestran el valor del índice si cambia entre diferentes NSX Manager

Después de aplicar un criterio de filtrado por reglas a un NSX Manager y de cambiar a otro diferente, el índice de reglas muestra el valor "0" para todas las reglas del filtro, en lugar de mostrar la posición real de la regla.

Solución alternativa: Borre el filtro para ver la posición de la regla.

- **Problema 1846402:** Si hay varias direcciones IP en la misma vNIC, se generan retrasos en la operación de publicación de firewall

El problema se produce cuando una vNIC tiene varias direcciones IP y está habilitada la intromisión de ARP. Cada paquete que esté fuera de la vNIC puede dar lugar a un mensaje de ARP de host a administrador con la dirección IP recién detectada. Esto es debido a que el host solo puede enviar una dirección IP de intromisión de ARP al administrador. Cuando la vNIC cambia de una dirección IP a otra, el host detecta la dirección IP como nueva y envía el mensaje de intromisión de ARP al administrador. Por lo general, esto hace que se renueven los mensajes del contenedor en NSX Manager, lo que genera retrasos en la configuración del firewall en el host.

Solución alternativa: Deshabilitar la intromisión de ARP cuando las vNIC tienen varias direcciones IP. Utilice la intromisión de DHCP o VMTools en su lugar.

- **Problema 1474650:** Para los usuarios de NetX, los hosts ESXi 5.5.x y 6.x reciben una pantalla de diagnóstico de color púrpura con el mensaje **ALERT: NMI: 709: NMI IPI received**
Cuando se transmite o se recibe un gran número de paquetes a través de una máquina virtual de servicio, DVFilter sigue dominando la CPU, lo que provoca una pérdida de latidos y aparece una pantalla de diagnóstico de color púrpura. Consulte el [artículo 2149704 de la base de conocimientos de VMware](#) para obtener más información.

Solución alternativa: Actualice el host ESXi a cualquiera de las siguientes versiones de ESXi que son un requisito mínimo para usar NetX:

- Revisión 10 de la versión 5.5
- ESXi 6.0U3
- ESXi 6.5

- **Problema 1799543:** Tras actualizar de NSX 6.2.x a NSX 6.3.0, vSphere Web Client muestra de forma errónea y le permite seleccionar grupos de seguridad universales NSX 6.2.x y grupos de seguridad universales no activos-en espera al crear el primer grupo de seguridad universal

activo-en espera.

Cuando crea el primer grupo de seguridad universal activo-en espera, la UI de vSphere Web Client le muestra y le permite agregar un grupo de seguridad universal que se creó en NSX 6.2.x. La operación no podrá realizarse y se mostrará el mensaje de error "El miembro solicitado no es un miembro válido" (The requested member is not a valid member).

Solución alternativa: Cree al menos un grupo de seguridad universal activo-en espera y no se producirá este problema al crear el siguiente grupo de seguridad universal activo-en espera.

- **Problema 1787680: Error al eliminar la sección del firewall universal cuando NSX Manager está en modo de tránsito**

Cuando intenta eliminar una sección del firewall universal de la UI de un NSX Manager en modo de tránsito y publica, se produce un error en la publicación como resultado de que no puede establecer el NSX Manager en modo independiente.

Solución alternativa: Use la REST API de eliminación de sección única para eliminar la sección del firewall universal.

- **Problema 1741844: Detectar direcciones de vNIC con varias direcciones IP mediante la intromisión ARP provoca el consumo total de la CPU.**

Este problema aparece cuando el vNIC de una máquina virtual se configura con varias direcciones IP y la intromisión ARP se habilita para la detección de IP. El módulo de detección de IP envía actualizaciones de vNIC-IP a NSX Manager continuamente para cambiar la asignación de vNIC-IP en todas las máquinas virtuales configuradas con varias direcciones IP.

Solución alternativa: No hay solución. La función de intromisión de ARP admite actualmente solo una dirección IP por vNIC. Para obtener más información, consulte la sección [Detección de IP para máquinas virtuales](#) en la *Guía de administración de NSX*.

- **Problema 1689159: La función Agregar regla (Add Rule) de Flow Monitoring no funciona correctamente en los flujos de ICMP.**

Al agregar una regla de Flow Monitoring, el campo Servicios (Services) se quedará vacío si no le asigna ICMP explícitamente. Como resultado, es posible que tenga que agregar una regla con el tipo de servicio "CUALQUIERA" (ANY).

Solución alternativa: Actualice este campo para que refleje el tráfico de ICMP.

- **Problema 1632235: Durante la instalación de Guest Introspection, la lista desplegable de redes solo muestra "Especificadas en host" (Specified on Host)**

Cuando se instala Guest Introspection con la licencia de solo antivirus de NSX y la licencia de vSphere Essential o estándar, la lista desplegable de redes mostrará solo la lista de los grupos de puertos DV existentes. Esta licencia no es compatible con la creación de DVS.

Solución alternativa: Antes de instalar Guest Introspection en un host de vSphere con una de estas licencias, especifique primero la red en la ventana "Configuración de máquina virtual agente" (Agent VM Settings).

- **Problema 1652155: No se pueden crear ni migrar reglas de firewall mediante las API de REST bajo ciertas condiciones y aparece un error HTTP 404**

No es compatible agregar ni migrar reglas de firewall mediante las API de REST en las siguientes condiciones:

- Creando reglas de firewall como una operación masiva cuando se configure el valor autosavedraft=true.
- Agregando reglas de firewall en diferentes secciones simultáneamente.

Solución alternativa: Configure como "falso" (false) el parámetro autoSaveDraft en la llamada de API cuando se creen o se migren reglas de firewall de forma masiva.

- **Problema 1509687: La longitud de la URL admite hasta 16.000 caracteres cuando se asigna una etiqueta de seguridad única a muchas máquinas virtuales de forma simultánea en una**

llamada de API

Una etiqueta de seguridad única no se puede asignar a un gran número de máquinas virtuales de forma simultánea con una única API si la longitud de la URL supera los 16.000 caracteres.

Solución alternativa: Para optimizar el rendimiento, etiqüete hasta un máximo de 500 máquinas virtuales en una única llamada.

- **Problema 1662020:** La operación de publicación puede fallar, lo que resulta en un mensaje "Error en la última publicación en el host *número de host*" (Last publish failed on host host number) en las secciones General y Servicios de seguridad de partners (Partner Security Services) de la interfaz de usuario de DFW

Después de cambiar cualquier regla, la interfaz de usuario muestra el mensaje "Error en la última publicación en el host *número de host*" (Last publish failed on host host number). Es posible que los hosts enumerados en la interfaz de usuario no dispongan de la versión correcta de las reglas de firewall, lo que resulta en una falta de seguridad o interrupciones en el funcionamiento de la red.

Este problema se produce normalmente en las situaciones siguientes:

- Después de actualizar de una versión anterior a la versión más reciente de NSX-v.
- Al sacar un host de un clúster y volver a introducirlo en él.
- Al mover un host de un clúster a otro.

Solución alternativa: Para realizar la recuperación, debe forzar la sincronización de los clústeres afectados (solo firewall).

- **Problema 1481522:** No se admite la migración de los borradores de reglas de firewall de la versión 6.1.x a la versión 6.2.3, ya que no son compatibles entre estas versiones

Solución alternativa: Ninguna.

- **Problema 1628679:** Con el firewall basado en la identidad, la máquina virtual de los usuarios eliminados continúa formando parte del grupo de seguridad

Cuando se elimina un usuario de un grupo del servidor de AD, la máquina virtual a la que el usuario está conectado continúa formando parte del grupo de seguridad (SG). De esta forma se conservan las directivas de firewall en la vNIC de la máquina virtual en el hipervisor, con lo que se otorga al usuario acceso completo a los servicios.

Solución alternativa: Ninguna. Por diseño, este es el comportamiento previsto.

- **Problema 1496273:** La interfaz de usuario permite la creación de reglas de firewall de NSX de entrada/salida que no se pueden aplicar a las instancias de Edge

El cliente web, incorrectamente, permite la creación de una regla de firewall de NSX aplicada a una o más instancias de NSX Edge cuando la regla tiene tráfico que se traslada en dirección "de entrada" o "de salida", y cuando PacketType es IPV4 o IPV6. La interfaz de usuario no debería permitir la creación de tales reglas, dado que NSX no puede aplicarlas a las instancias de NSX Edge.

Solución alternativa: Ninguna.

- **Problema 1557924:** Se permite consumir el conmutador lógico universal en el campo AppliedTo de una regla de DFW local

Cuando un conmutador lógico universal se utiliza como miembro de un grupo de seguridad, la regla de DFW puede utilizar este grupo en el campo AppliedTo. Esto aplica indirectamente la regla en el conmutador lógico universal, lo que no se debería permitir porque puede provocar un comportamiento desconocido de estas reglas.

Solución alternativa: Ninguna.

- **Problema 1559971:** La lista de exclusión del firewall de Cross-vCenter NSX no se publica si el firewall está deshabilitado en un clúster

En Cross-vCenter NSX, la lista de exclusión del firewall no se publica en ningún clúster si el firewall está deshabilitado en uno de los clústeres.

Solución alternativa: fuerce la sincronización que afectó a los dispositivos NSX Edge.

- **Problema 1407920:** Error al volver a publicar la regla de firewall tras utilizar ELIMINAR API (DELETE API)

Si elimina la configuración entera del firewall a través del método DELETE API y a continuación intenta volver a publicar todas las reglas de un borrador de reglas de firewall previamente guardado, la regla publicada no funcionará.

- **Problema 1494718:** No se pueden crear reglas universales nuevas y las reglas universales existentes no se pueden editar desde la interfaz de usuario de Flow Monitoring

Solución alternativa: No se pueden agregar ni editar reglas universales desde la interfaz de usuario de Flow Monitoring. Se deshabilitará automáticamente EditRule.

- **Problema 1442379:** Configuración del firewall de Service Composer no sincronizada

En NSX Service Composer, si cualquier directiva de firewall no es válida (por ejemplo, si se eliminó un grupo de seguridad que se utilizaba en una regla de firewall en ese momento), eliminar o modificar otra directiva de firewall hace que Service Composer pierda la sincronización y se muestra el mensaje de error `Configuración de firewall no sincronizada`.

Solución alternativa: Elimine cualquier regla de firewall no válida y, a continuación, sincronice la configuración del firewall. Seleccione Service Composer: Directivas de seguridad (Security Policies) y en cada directiva de seguridad que tenga reglas de firewall asociadas, haga clic en Acciones (Actions) y seleccione Sincronizar config. de firewall (Synchronize Firewall Config). Para evitar este problema, solucione o elimine siempre las configuraciones de firewall no válidas antes de realizar más cambios de configuración en el firewall.

- **Problema 1066277:** El nombre de la directiva de seguridad no permite más de 229 caracteres

El campo Nombre de directiva de seguridad (Security Policy Name) en la pestaña Directiva de seguridad (Security Policy) de Service Composer puede aceptar hasta 229 caracteres. Esto se debe a que los nombres de las directivas están anteceditos por un prefijo.

Solución alternativa: Ninguna.

- **Problema 1443344:** Algunas versiones de VM-Series de Networks de terceros no funcionan con la configuración predeterminada de NSX Manager

Algunos componentes de NSX 6.1.4 o versiones posteriores deshabilitan SSLv3 de forma predeterminada. Antes de realizar la actualización, es necesario comprobar que todas las soluciones de terceros integradas en la implementación de NSX *no* dependan de la comunicación de SSLv3. Por ejemplo, algunas versiones de la solución VM-Series de Palo Alto Networks requieren compatibilidad con SSLv3, por lo que es necesario comprobar los requisitos de la versión con los proveedores.

- **Problema 1660718:** El estado de las directivas de Service Composer aparece "En curso" (In Progress) en la interfaz de usuario y "Pendiente" (Pending) en el resultado de la API

Solución alternativa: Ninguna.

- **Problema 1620491:** El estado de sincronización a nivel de directivas en Service Composer no muestra el estado de publicación de las reglas de una directiva

Cuando se crea o se modifica una directiva, Service Composer muestra un estado correcto que solo indica el estado de persistencia. No refleja si las reglas se publicaron correctamente en el host.

Solución alternativa: Utilice la interfaz de usuario del firewall para ver el estado de la publicación.

- **Problema 1317814:** Service Composer pierde la sincronización cuando se realizan cambios en la directiva mientras una de las instancias de Service Manager está inactiva

Si se realizan cambios de directivas mientras una o varias instancias de Service Manager estén inactivas, dichos cambios no se realizarán y la sincronización de Service Composer se detendrá.

Solución alternativa: Asegúrese de que Service Manager responda y, a continuación, emita una sincronización forzada desde Service Composer.

- **Problema 1070905:** No se puede quitar y volver a agregar un host a un clúster protegido por Guest Introspection y soluciones de seguridad de terceros

Si se desconecta y quita un host de vCenter Server con el fin de quitarlo de un clúster protegido por Guest Introspection y soluciones de seguridad de terceros, es posible que surjan problemas si se intenta volver a agregar el mismo host al clúster.

Solución alternativa: Para quitar un host de un clúster protegido, primero coloque el host en modo de mantenimiento. Después, mueva el host a un clúster sin protección o fuera de todos los clústeres y, a continuación, desconecte y quite el host.

- **Problema 1648578:** NSX obliga a agregar un clúster, una red o un almacenamiento cuando se crea una nueva instancia del servicio basada en un host NetX

Cuando cree una nueva instancia del servicio desde vSphere Web Client para los servicios basados en el host NetX como el firewall, IDS e IPS, se le obliga a agregar un clúster, una red o un almacenamiento aunque no sean necesarios.

Solución alternativa: Al crear una nueva instancia del servicio, puede agregar cualquier información del clúster, de la red o del almacenamiento para rellenar los campos. Esto le permitirá crear la instancia del servicio y podrá continuar con el procedimiento.

- **Problema 1772504:** Service Composer no admite los grupos de seguridad con el conjunto MAC
Service Composer admite el uso de los grupos de seguridad en las Configuraciones de directivas (Policy configurations). Si un grupo de seguridad contiene un conjunto MAC, Service Composer lo aceptará sin problemas, pero se producirá un error al aplicar reglas a ese conjunto MAC específico. Esto es porque Service Composer funciona en Layer3 y no admite construcciones de Layer2. Tenga en cuenta que, si un grupo de seguridad tiene un conjunto IP y un conjunto MAC, el valor de la IP seguirá siendo efectivo pero el conjunto MAC se ignorará. No existe ningún problema al hacer referencia a un grupo de seguridad que contenga un conjunto MAC. El usuario debe saber que el conjunto MAC se ignorará.

Solución alternativa: Si la intención del usuario es crear reglas del firewall con un conjunto MAC, debe usar una configuración DFW Layer2/Ethernet en lugar de Service Composer.

- **Problema 1718726:** No se puede forzar la sincronización de Service Composer después de que un usuario haya eliminado manualmente la sección Directiva de Service Composer con una DFW REST API

En un entorno de Cross-vCenter NSX, se producirá un error cuando un usuario intenta forzar la sincronización de la configuración de NSX Service Composer si solo había una sección Directiva y dicha sección (la sección de directiva administrada por Service Composer) se eliminó previamente a través de una llamada REST API.

Solución alternativa: No elimine la sección de directiva administrada por Service Composer a través de una llamada REST API (tenga en cuenta que la interfaz de usuario ya evita la eliminación de esta sección).

Problemas conocidos de servicios de supervisión

- **Problema 1466790:** No se pueden elegir las máquinas virtuales en la red con puente mediante la herramienta NSX Traceflow

Con la herramienta NSX Traceflow, no se pueden seleccionar las máquinas virtuales que no están asociadas a un conmutador lógico. Esto significa que las máquinas virtuales en una red con puente L2 no se pueden elegir por nombre de máquina virtual como dirección de origen o destino para una inspección de Traceflow.

Solución alternativa: En el caso de las máquinas virtuales asociadas a redes con puente L2, utilice la dirección IP o la dirección MAC de la interfaz que desea especificar como destino en una inspección de Traceflow. No puede elegir máquinas virtuales asociadas a redes con puente L2 como origen. Consulte el [artículo de la base de conocimientos 2129191](#) para obtener más información.

Problemas conocidos de interoperabilidad de soluciones

- **Problema 1568861:** La implementación de NSX Edge falla durante cualquier implementación de Edge que se realice desde una celda de vCloud Director que no controle el agente de escucha

de vCenter

La implementación de NSX Edge falla durante cualquier implementación de Edge que se realice desde una celda de vCloud Director que no controle el agente de escucha de vCenter. Además, se produce un error desde vCloud Director en las acciones de NSX Edge, entre las que se incluye una nueva implementación.

Solución alternativa: Implemente un NSX Edge desde la celda de vCloud Director que controla el agente de escucha de vCenter.