

# Notas de la versión de VMware NSX for vSphere 6.3.0

VMware NSX for vSphere 6.3.0 | Publicado el 2 de febrero de 2017 | Compilación 5007049

## Contenido de las notas de la versión

Las notas de la versión contienen los siguientes temas:

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

## Novedades

Las nuevas funciones de NSX 6.3.0 se pueden dividir en las siguientes categorías:

- [Plataforma y funciones de cumplimiento](#)
- [Mejoras en las operaciones](#)
- [Mejoras en servicios y enrutamiento](#)
- [Mejoras en la seguridad](#)
- [CMP e integración de partners](#)
- [Instalación y actualización](#)
- [Copia de seguridad y restauración](#)

### Plataforma y funciones de cumplimiento

- Con respecto a la plataforma:
  - **Mejoras del DFW activo-en espera de Cross-vCenter NSX:** NSX 6.3.0 tiene las siguientes mejoras:
    - Ahora se admiten varias secciones de DFW universal. Las reglas locales y universales pueden utilizar los Grupos de seguridad universales en los campos **Origen** (Source), **Destino** (Destination) y **Aplicado a** (AppliedTo).
    - Grupos de seguridad universales: La pertenencia a un Grupo de seguridad universal (Universal Security Group) se puede definir de forma dinámica o estática. La pertenencia estática se consigue al agregar de forma manual una etiqueta de seguridad universal a cada máquina virtual. La pertenencia dinámica se consigue al agregar las máquinas virtuales como miembros basándose en un criterio dinámico (nombre de máquina virtual).

- **Etiquetas de seguridad universales:** Ahora puede definir las etiquetas de seguridad universal en el NSX Manager principal y marcar los NSX Manager secundarios para la sincronización universal. Las etiquetas de seguridad universal se pueden asignar a máquinas virtuales de forma estática, basadas en una selección de ID único, o bien de forma dinámica, en respuesta a los criterios, como los exámenes antivirus o de vulnerabilidad.
- **Criterios de selección de ID único:** En las versiones anteriores de NSX, las etiquetas de seguridad eran locales para un NSX Manager y se asignaban a las máquinas virtuales usando el ID del objeto administrado de la máquina virtual. En un entorno activo y en espera, puede que el ID del objeto administrado de una determinada máquina virtual no sea el mismo que el de los centros de datos activos y en espera. NSX 6.3.x le permite configurar los criterios de selección de ID único en el NSX Manager primario que se usa para identificar las máquinas virtuales cuando se conectan a etiquetas de seguridad universal: UUID de la instancia de la máquina virtual, BIOS UUID de la máquina virtual, el nombre de la máquina virtual o una combinación de estas opciones. Consulte la [selección de ID único](#) en la *Guía de administración de NSX* para obtener más información.
- **Recuperación automática del agente de plano de control (netcpa):** Un mecanismo de recuperación automática mejorado para el proceso netcpa garantiza que la comunicación de la ruta de datos sea continua. El proceso automático de supervisión netcpa también se reinicia automáticamente en caso de problemas y proporciona alertas a través del servidor syslog. Un resumen de beneficios:
  - supervisión automática del proceso netcpa
  - reiniciar automáticamente el proceso en caso de problemas, por ejemplo, si el sistema deja de responder
  - generación automática de archivos de núcleo para depurar
  - alerta a través de syslog del evento de reinicio automático
- **Compatibilidad con vSphere 6.5:** NSX 6.3.0 introduce compatibilidad con vSphere 6.5a y versiones posteriores. NSX 6.3.0 preserva la compatibilidad con vSphere 5.5 y 6.0.
- **Previsualización técnica: Modo Operación con controlador desconectado (Controller Disconnected Operation, CDO):** El modo Operación con controlador desconectado (Controller Disconnected Operation, CDO) se introdujo como una función de previsualización técnica. Este modo asegura que, cuando los hosts pierdan la conectividad al controlador, esto no afecte a la conectividad del plano de datos. Consulte la sección sobre el [modo Operación con controlador desconectado](#) (Controller Disconnected Operation, CDO) en la *Guía de administración de NSX*. Consulte también el problema 1803220.

• **Funciones de cumplimiento:**

- **FIPS:** NSX 6.3.0 tiene un modo FIPS que usa únicamente los conjuntos de cifrado que cumplen los estándares de FIPS. NSX Manager y NSX Edge tienen un modo FIPS que se puede habilitar a través de vSphere Web Client o de la REST API de NSX. Consulte las [diferencias de funcionalidad entre el modo FIPS y el modo no FIPS](#) en la *Guía de administración de NSX* para obtener una lista de funcionalidades a las que afectan el modo FIPS.

**Nota:** Los partners de desarrollo de VMware están en proceso de obtener una certificación para usar las nuevas soluciones para partners compatibles con FIPS en NSX. Las conexiones salientes de NSX 6.3.0 son TLS 1.1 o superiores y solo usan los conjuntos de cifrado aprobados por FIPS. Esto supone que los dispositivos del partner que reciban devoluciones de llamadas deben configurar el agente de escucha a varios conjuntos de cifrado de seguridad. A continuación se incluyen los cifrados de modo FIPS y de modo predeterminado:

■ **Cifrado de modo predeterminado: (Modo FIPS desactivado)**

```
[TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
```

■ **Cifrado de modo FIPS:** [TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256,  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA,  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA]

Los modos predeterminado y FIPS son compatibles con los protocolos TLS 1.1 y 1.2. Consulte la [Guía de compatibilidad de VMware](#) para verificar si las soluciones del partner tienen el certificado del modo FIPS.

- **Criterios comunes:** Para el cumplimiento de los criterios comunes, NSX se ha sometido a pruebas de conformidad con el nivel de garantía EAL2+. Para ejecutar una instalación de NSX conforme a los criterios comunes, es necesario configurar NSX tal como se explica en el documento [Configurar NSX para criterios comunes](#), que forma parte de la *Guía de administración de NSX*.
- **ICSA:** Este es un certificado aceptado en todo el sector que prueba y certifica productos, entre los que se incluyen los productos de antivirus, de firewall, de IPsec VPN, de cifrado, de VPN SSL, de IPS de red, de anti spyware y de firewall del equipo. Tanto Distributed Firewall como Edge Firewall están certificados según los criterios de ICSA Corporate Firewall.
- **Cambio en el formato de registro de paquetes de DFW debido al requisito de la certificación ICSA:** NSX 6.3.0 introduce un cambio en los registros de paquetes de DFW. En la versión 6.3.0 y versiones posteriores, incluimos el código y tipo ICMP a fin de cumplir con los requisitos de la certificación ICSA.

Este es el aspecto que tenía el registro antes de la versión 6.3.0, sin tipo ni código ICMP:

```
2016-09-29T20:52:21.983Z 6673 INET6 match PASS domain-c27/1001 IN 96 ICMP
```

```
fe80:0:0:0:21d:b502:f984:c601->ff02:0:0:0:0:0:0:1
```

En la versión 6.3.0 y versiones posteriores, tiene el aspecto del siguiente tipo y código ICMP. En este ejemplo, 8 es el código y 0 es el tipo:

```
2016-09-29T20:54:16.051Z 42991 INET match PASS domain-c27/1001 IN 84 ICMP 8
0 10.113.226.5->10.28.79.55
```

## Mejoras en las operaciones

- **Panel de control para solucionar los problemas:** El panel de control de NSX se actualizó en NSX 6.3.0 para incluir más funciones como el estado de la implementación del servicio, el estado de las copias de seguridad de NSX Manager y las notificaciones de los dispositivos Edge.
- **Etiquetado de seguridad:** Esto permite asignar y limpiar varias etiquetas para una máquina virtual a través de las llamadas de API.
- **Mejoras de syslog:** Una nueva actualización de syslog está disponible específicamente para el equilibrador de carga.
- **Paquete de contenido de Log Insight:** Esto se actualizó para que el equilibrador de carga proporcione un panel de control centralizado, una supervisión de un extremo a otro y una planificación de capacidad mejorada desde la interfaz de usuario (UI).
- **Control de acceso basado en la función:** Esta función restringe la administración del usuario únicamente a los administradores de empresa; en consecuencia, el administrador de NSX ya no tendrá permiso para crear nuevos usuarios ni para asignar funciones a nuevos usuarios. Desde el punto de vista de la seguridad, esto ayuda a crear una clara demarcación de estas dos funciones de administración.
- **Estado Purga (Drain) para los miembros del grupo de equilibradores de carga** Ahora puede hacer que los miembros del grupo entren en estado *Purga* (Drain), lo que provoca que el servidor se apague correctamente para su mantenimiento. Al establecer un miembro del grupo en el estado de purga, se elimina el servidor backend del equilibrador de carga, pero se sigue permitiendo que el servidor acepte nuevas conexiones persistentes.

## Mejoras en servicios y enrutamiento

- **Compatibilidad ASN de 4 bits para BGP:** La compatibilidad de la configuración BGP con ASN de 4 bits está disponible junto con la compatibilidad con versiones anteriores para los pares BGP ASN de 2 bits que existían anteriormente.
- **Mejoras NAT para las coincidencias de la 5-tupla:** Para ofrecer una flexibilidad y una configuración más pormenorizadas para las reglas NAT, está disponible una compatibilidad de la coincidencia de 5-tupla para NSX 6.3.0:
  - Los criterios de la coincidencia se basan en cinco parámetros: protocolo, IP de origen, puerto de origen, IP de destino y puerto de destino.
  - Los cambios en la interfaz de usuario (UI) se proporcionaron para ayudarle a especificar las configuraciones SNAT/DNAT fácilmente. Cuando cambia las configuraciones DNAT/SNAT en versiones anteriores de Edge, la UI continúa mostrando el estilo anterior de los paneles.
  - La NSX REST API agrega campos para los nuevos parámetros:

```
<natRules>
  <natRule>
    {...}
  <!-- new fields applicable for DNAT -->
    <dnatMatchSourceAddress>any</dnatMatchSourceAddress>
    <dnatMatchSourcePort>any</dnatMatchSourcePort>
  </natRule>
```

```

    <natRule>
    {...}
    <!-- new fields applicable for SNAT -->
    <snatMatchDestinationAddress>any</snatMatchDestinationAddress>
    <snatMatchDestinationPort>any</snatMatchDestinationPort>
    </natRule>
</natRules>

```

- **Rendimiento mejorado de la VPN de Capa 2** Se mejoró el rendimiento de la VPN de Capa 2. Esto permite a un único dispositivo Edge admitir hasta 1,5 Gb/s de rendimiento, lo que supone una mejora si se compara con los 750 Mb/s permitidos anteriormente.
- **Configuración de OSPF mejorada:** Mientras se configura OSPF en una puerta de enlace de servicios Edge (ESG), NSSA puede traducir LSA de tipo 7 a LSA de tipo 5.

## Mejoras en la seguridad

Existen varias mejoras en Distributed Firewall:

- **Temporizadores DFW:** NSX 6.3.0 introduce temporizadores de sesión que definen el tiempo que se mantendrá una sesión en el firewall estando inactiva. Cuando se agota el tiempo de espera de sesión del protocolo, se cierra la sesión. En el firewall, puede definir los tiempos de espera para las sesiones de TCP, de UDP y de ICMP, y las aplica a un grupo de máquinas virtuales o de vNIC definidos por el usuario. Consulte los [temporizadores de sesiones](#) en la *Guía de administración de NSX*.
- **Nuevas funciones de microsegmentación:** Para poder utilizar la microsegmentación en las herramientas de planificación y de visibilidad, se introdujeron dos nuevas funciones:
  - Administrador de reglas de aplicaciones (Application Rule Manager) simplifica el proceso de creación de grupos de seguridad y envía a la lista blanca las reglas de firewall para las aplicaciones existentes.
  - Endpoint Monitoring permite que el propietario de una aplicación realice un perfil de la aplicación e identifique los procesos para establecer conexiones de red.
- **Compatibilidad de Linux con Guest Introspection:** NSX 6.3.0 habilita Guest Introspection para las máquinas virtuales de Linux. En las máquinas virtuales invitadas basadas en Linux, la función NSX Guest Introspection aprovecha las capacidades `fanotify` y `inotify` proporcionadas por el kernel de Linux. Consulte [cómo instalar Guest Introspection para Linux](#) en la *Guía de administración de NSX* para obtener más información. Consulte las [versiones](#) para obtener una lista de las versiones de Linux que admite NSX.
- **Estado de la publicación para Service Composer:** El estado de la publicación de Service Composer ya está disponible para comprobar si una directiva está sincronizada. Esto proporciona una mayor visibilidad de las traducciones de las directivas de seguridad en reglas de DFW del host.

## Cloud Management Platform (CMP) e integración de los partners

- Una mejor interoperabilidad entre vCloud Director 8.20 y NSX 6.3.0 ayuda a los proveedores del servicio a ofrecer servicios de seguridad y de red avanzados a sus arrendatarios. vCloud Director 8.20 con NSX 6.3.0 muestra las funcionalidades de NSX nativas que admiten varios arrendatarios y su autoservicio.
- NSX 6.3.0 se puede utilizar con la nueva versión 1.1 del complemento vRO, que es compatible con vRA e introduce la capacidad de admitir otras aplicaciones que no sean vRA.
- NSX NetX 6.3.0 proporciona mejoras de rendimiento y de escala relacionadas con la inserción de servicios.

## Instalación y actualización

- Los módulos del kernel de NSX ahora son independientes de la versión de ESXi: A partir de NSX 6.3.0, los módulos del kernel de NSX usan únicamente la VMKAPI disponible públicamente para que se garanticen las interfaces a través de las diferentes versiones. Esta mejora ayuda a reducir la probabilidad de que se produzcan errores en las actualizaciones del host debido a que las versiones del módulo del kernel no son correctas. En versiones anteriores, cada actualización de ESXi en un entorno de NSX requiere al menos dos reinicios para asegurar que la funcionalidad de NSX siga operativa (esto se debe a que es necesario publicar nuevos módulos de kernel para cada versión de ESXi nueva).
- NSX 6.3.0 también comprueba que NSX esté preparado antes de finalizar el modo de mantenimiento del host. Esto garantiza que DRS solo envíe las cargas de trabajo al host donde NSX esté preparado. De esta forma, se evita la pérdida de red para algunas máquinas virtuales de carga de trabajo.
- Los parámetros de OVF ahora están separados por coma: Los siguientes parámetros de OVF pasaron de estar separados por espacio a estar separados por coma:
  - Lista del servidor de DNS (vsm\_dns1\_0)
  - Lista de búsqueda de dominios (vsm\_domain\_0)
  - Lista del servidor NTP (vsm\_ntp\_0)

## Copia de seguridad y restauración

A partir de NSX 6.3.0, se admiten los siguientes cifrados para la copia de seguridad de SFTP:

- **Cifrado:** aes128-cbc, aes128-ctr, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr
- **Autenticación de mensaje (mac):** hmac-sha2-256
- **Intercambio de claves:** diffie-hellman-group-exchange-sha256

**Nota:** No hay compatibilidad para `hmac-sha1`; se admite solo `hmac-sha2-256`. Si utiliza SFTP para la copia de seguridad, cambie a `hmac-sha2-256` después de actualizar a la versión 6.3.0. Consulte el [artículo 2149282 de la base de conocimientos de VMware](#) para obtener más información.

## 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.

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"> <li>• vSphere 5.5U3 y versiones posteriores.</li> <li>• 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 <a href="#">artículo 2144605 de la base de conocimientos de VMware</a> para obtener más información.</li> <li>• vSphere 6.5U1 y versiones posteriores. vSphere 6.5U1 soluciona el problema de EAM con tipo OutOfMemory. Consulte el <a href="#">artículo 2135378 de la base de conocimientos de VMware</a> para obtener más información.</li> </ul>
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"> <li>• 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.</li> <li>• 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 <a href="#">artículo 2144236 de la base de conocimientos de VMware</a>).</li> <li>• Use VMware Tools 10.1.0 y versiones posteriores para garantizar su compatibilidad con Windows 10.</li> </ul>
Guest Introspection para Linux	<p>Esta versión de NSX admite las siguientes versiones de Linux:</p> <ul style="list-style-type: none"> <li>• RHEL 7 GA (64 bits)</li> <li>• SLES 12 GA (64 bits)</li> <li>• Ubuntu 14.04 LTS (64 bits)</li> </ul>
vRealize Orchestrator	<p>Versión 1.1.0 de NSX-vRO o una versión posterior.</p>

**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:** NSX for vSphere 6.1.x llegó a su fin de disponibilidad (End of Availability, EOA) y al 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](#)).
- **Nuevo** Se eliminó NSX Data Security: En NSX 6.3.0, la función NSX Data Security se eliminó del producto.
- **Nuevo** 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*.
- **Nuevo** 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.
- **Nuevo** 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).
- **Nuevo** vCNS Edge ya no se admite. 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 de 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

## Notas sobre la actualización

- [Notas sobre la actualización relacionadas con NSX y vSphere](#)
- [Notas sobre la actualización relacionadas con los componentes de NSX](#)
- [Notas actualizadas de FIPS](#)

**Nota:** Si utiliza SFTP para hacer copias de seguridad de NSX, consulte [Copia de seguridad y restauración](#) para obtener una lista de los algoritmos de seguridad compatibles a partir de la versión 6.3.x.

**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 sobre la actualización relacionadas con NSX y vSphere

- 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.

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
- **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 a NSX 6.3.0. En primer lugar, debe actualizar a una versión compatible con la versión 6.2.x.
- **Actualizar a vSphere 6.5a:** Al actualizar desde vSphere 5.5 o 6.0 a vSphere 6.5a, debe actualizar primero a NSX 6.3.0. 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.

- **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.
- Si tiene una puerta de enlace del hardware (VTEP de hardware) instalada en su entorno, la actualización a NSX 6.3.0 se bloqueará. Debe ponerse en contacto con el soporte técnico de VMware para realizar la actualización. Consulte el [artículo 2148511 de la base de conocimientos de VMware](#) para obtener más información.
- **Restablecer vSphere Web Client:** Después de actualizar NSX Manager, debe restablecer el servidor vSphere Web Client como se explica en la [documentación de actualización de NSX](#). Hasta entonces, es posible que no aparezca la pestaña **Redes y seguridad** (Networking and Security) en vSphere Web Client. Es posible que también tenga que limpiar la caché o el historial del navegador.
- **Entornos sin estado:** Las actualizaciones de NSX en un entorno de host sin estado utilizan URL de VIB nuevas: 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:
  1. Se descargan manualmente los VIB de NSX más recientes de NSX Manager desde una URL fija.
  2. Se agregan los VIB al perfil de imagen del host.

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:

- Busque la URL de VIB nueva en `https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties`.
- Obtenga los VIB de la versión de host ESX requerida desde la URL correspondiente.
- Agréguelos al perfil de imagen del host.

## Notas sobre la actualización relacionadas con los componentes de NSX

- **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:

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 que aparece a continuación para ver los valores predeterminados).

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

- 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.

Realice el siguiente procedimiento para verificar que el estado de la infraestructura de mensajería del host en la que se va a implementar NSX Edge sea de color VERDE:

- Utilice el método API `GET /api/2.0/nwfabric/status?resource={resourceId}`, donde `resourceId` es el identificador del objeto administrado por vCenter de un clúster o host (p. ej., `host-21` o `dominio-c33`). Consulte el apartado sobre cómo encontrar los identificadores de los objetos de vCenter en la *Guía de NSX API* para obtener instrucciones sobre cómo encontrar los identificadores de los recursos de hosts y clústeres.
- Busque el estado que corresponde a `featureId` de `com.vmware.vshield.vsm.messagingInfra` en el cuerpo de la respuesta:

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

- **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).
- **Diseño de disco de NSX Controller** Las actualizaciones desde 6.2.2 y versiones anteriores no recibirán el nuevo diseño de disco que se introdujo en 6.2.3, lo que proporciona particiones de discos independientes para obtener datos y registros para mejorar la estabilidad del controlador.

- 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"
}
```

- 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 subprocesso 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 cáncélela.
- 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.

## Notas actualizadas 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-SHA384, 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 6.3.0. 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.

## Problemas conocidos

Los problemas conocidos se agrupan de la siguiente manera:

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

### Problemas conocidos generales

**Nuevo** 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*, por lo tanto, el producto no es vulnerable.

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

**Problema 1558285:** Al eliminar un clúster con Guest Introspection desde vCenter, la acción acaba en una excepción de puntero nulo

Se deben eliminar servicios como Guest Introspection antes de eliminar un clúster de vCenter.

*Solución alternativa:* Elimine la agencia EAM para la implementación del servicio sin clúster asociado.

**Problema 1629030:** La captura de paquetes de la CLI central (depurar la captura de paquetes y mostrar captura de paquetes) necesita vSphere 5.5U3 o versiones posteriores

Estos comandos no son compatibles con versiones anteriores a vSphere 5.5.

*Solución alternativa:* VMware aconseja a todos los clientes de NSX que ejecuten vSphere 5.5U3 o una versión posterior.

**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.

**Nuevo 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.

**Nuevo 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>
```

**Nuevo Problema 1808478:** Se produce un error en el servicio vsfwd si no se puede asignar la memoria de vmvisor después de actualizar de NSX 6.2.x a NSX 6.3.0

Se produce un error en el servicio vsfwd si no se puede asignar la memoria de vmvisor después de actualizar de NSX 6.2.x a NSX 6.3.0. Consulte el [artículo 2148974 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.

**Nuevo Problema 1818257:** La información VTEP no se envía a los controladores cuando la función LACP mejorado (Enhanced LACP) se utiliza con VXLAN después de actualizar el host de NSX 6.2.x a NSX 6.3.0 con ESXi 6.0

Al actualizar de NSX 6.2.x a NSX 6.3.0 con ESXi 6.0, después de la actualización del host, la información de VTEP no se envía a los controladores si se utiliza LACP mejorado (Enhanced LACP). Consulte el [artículo 2149210 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.

**Nuevo Problema 1791371:** Al actualizar los hosts ESXi a vSphere 6.5a, si Guest Introspection y los VIB de VXLAN se actualizaron en paralelo, se activa una alarma

Los VIB de VXLAN y de Guest Introspection son diferentes para vSphere 6.5a y, cuando se actualizan en paralelo, la actualización de los VIB de VXLAN activa una alarma que solicita que se reinicie el host.

*Solución alternativa:* Instale en primer lugar los VIB de VXLAN y, a continuación, los de Guest Introspection cuando actualice a vSphere 6.5a.

**Nuevo Problema 1805983:** Cuando actualice a NSX 6.2.5, 6.2.6 o 6.3.0, los servidores virtuales no funcionan si no contienen un grupo de servidores.

Los servidores virtuales sin grupos de servidores solo pueden proporcionar redireccionamiento HTTP/HTTPS. No tienen otra funcionalidad.

*Solución alternativa:* Cree un grupo ficticio sin miembros y asígnelo al servidor virtual.

**Nuevo 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.

**Nuevo 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 conectar con 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.

**Nuevo 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>
```

**Nuevo Problema 1802688: Actualizar de NSX 6.2.x a 6.3.0 no refleja el estado habilitado de DFW actualizado.**

Tras actualizar NSX de la versión 6.2.x a 6.3.0 y los VIB de clúster a bits 6.3.0, al agregar un nuevo host al clúster actualizado, los estados del firewall del host en cuestión y del clúster siguen girando como ocupados y no se actualizan aunque se hayan instalado los nuevos VIB en el nuevo host.

*Solución alternativa:* Haga lo siguiente:

1. Ejecute la llamada API de sincronización del bus de mensajes para el host que utilice la API `POST https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize`. De este modo, el estado del firewall del clúster y del host cambiará a "Deshabilitado" ("Disabled").

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

2. Ahora habilite el firewall para dicho clúster desde la página Instalación de la UI (UI Installation) > Preparación del host (Hostprep). Esto debería activar el modo DFW habilitado (DFW enabled) en todos los hosts de dicho clúster.

**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 1660355:** Las máquinas virtuales que se migran de la versión 6.1.5 a la versión 6.2.3 y posteriores no ofrecerán compatibilidad con ALG de TFTP  
Aunque el host esté habilitado, las máquinas virtuales que se migran de la versión 6.1.5 a la versión 6.2.3 y posteriores no ofrecerán compatibilidad con ALG de TFTP.

*Solución alternativa:* Agregue y elimine la máquina virtual de la lista de exclusión o reiníciela, de modo que el nuevo filtro de la versión 6.2.3 y posteriores se cree para ofrecer compatibilidad con ALG de TFTP.

**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 1332563:** 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 1473537:** 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 1266433:** 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 1474066:** Parece que la llamada API REST de NSX para habilitar o deshabilitar la detección de IP no surte efecto

Si no se completó la preparación del clúster del host, la llamada API REST de NSX para habilitar o deshabilitar la detección de IP (<https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features>) no surte efecto.

**Solución alternativa:** Antes de emitir esta llamada API, asegúrese de que se haya completado la preparación del clúster del host.

### Problema 1459032: Error en la configuración de la puerta de enlace de VXLAN

Cuando se configura una VXLAN con un grupo de direcciones IP estáticas (en **Redes y seguridad** [Networking & Security] > **Instalación** [Installation] > **Preparación del host** [Host Preparation] > **Configurar VXLAN** [Configure VXLAN]) y la configuración no puede establecer una IP de puerta de enlace de grupo de direcciones IP en VTEP (debido a que la puerta de enlace no está correctamente configurada o no es posible comunicarse con ella), el estado de configuración de la VXLAN entra en estado de error (ROJO) en el clúster del host.

El mensaje de error es La puerta de enlace de la VXLAN no puede establecerse en el host y el estado de error es `VXLAN_GATEWAY_SETUP_FAILURE`. En la llamada API REST, GET `https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>`, el estado de la VXLAN es el siguiente:

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

**Solución alternativa:** Existen dos opciones para solucionar el error.

- Opción 1: Quite la configuración de la VXLAN del clúster del host, solucione la configuración de la puerta de enlace subyacente en el grupo de direcciones IP (asegúrese de que la puerta de enlace esté configurada correctamente y de que se pueda establecer una comunicación con ella) y, a continuación, vuelva a configurar la VXLAN del clúster del host.
- Opción 2: Realice los pasos siguientes.
  1. Solucione la configuración de la puerta de enlace subyacente en el grupo de direcciones IP; para ello, asegúrese de que la puerta de enlace esté configurada correctamente y de que se pueda establecer una comunicación con ella.
  2. Coloque el host (o los hosts) en modo de mantenimiento para asegurar que no haya tráfico de máquina virtual activo en el host.
  3. Elimine los VTEP de la VXLAN del host.
  4. Finalice el modo de mantenimiento del host. Al finalizar el modo de mantenimiento del host, se activa el proceso de creación de VTEP de la VXLAN en NSX Manager. NSX Manager intenta recrear los VTEP necesarios en el host.

### 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-vgpi`, 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 1485862:** La desinstalación de NSX de un clúster de hosts a veces genera una condición de error

Cuando se utiliza la acción Desinstalar (Uninstall) en la pestaña Instalación (Installation): Preparación del host (Host Preparation) es posible que ocurra un error y aparezca el mensaje

`eam.issue.OrphanedAgency` en los registros de EAM de los hosts. Después de utilizar la acción Resolver (Resolve) y de reiniciar los hosts, el estado de error continúa a pesar de que se desinstalaron correctamente los VIB de NSX.

*Solución alternativa:* Elimine la agencia huérfana de vSphere ESX Agent Manager (Administración [Administration]: Extensiones de vCenter Server [vCenter Server Extensions]: vSphere ESX Agent Manager).

**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:* Siga los pasos a continuación.

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

**Nuevo 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 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.

**Nuevo Problema 1770436:** Alertas generadas incluso si no hay una dirección IP duplicada

A veces, el comando `arping` informa de que la dirección IP de NSX Manager está duplicada en la red, aunque no sea así. Esto genera un evento de falso positivo.

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

**Nuevo 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.

**Nuevo Problema 1785142:** Demora al mostrar los "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.

**Nuevo 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:* Haga lo siguiente:

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

**Nuevo 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 1787542:** Excepciones en el registro de los NSX Manager secundarios después de la restauración de DB del NSX Manager primario

Después de restaurar DB, las secciones del DFW universal primarias y reinstaladas no aparecen en los NSX Manager secundarios.

*Solución alternativa:* Ninguna. Reinicie el NSX Manager secundario para solucionar esta cuestión.

**Nuevo 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 Managers 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:*

Realice los pasos siguientes:

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 1534877:** 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 1537258:** 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 Managers 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 1477041:** La página de resumen del dispositivo virtual NSX Manager no muestra ningún nombre DNS

Cuando se inicia sesión en el dispositivo virtual NSX Manager, la página Resumen (Summary) tiene un campo para el nombre DNS. Este campo permanece en blanco a pesar de que se definió un nombre DNS para el dispositivo NSX Manager.

*Solución alternativa:* Puede ver el nombre de host y los dominios de búsqueda de NSX Manager en la página Administrar (Manage): Red (Network).

**Problema 1492880:** 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 1468613:** 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:* Realice los pasos siguientes:

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 1489768:** Cambio en el comportamiento de la llamada API REST de NSX para agregar un espacio de nombre en un centro de datos

En NSX 6.2, la llamada de REST API POST `https://<nsxmgr-`

`ip>/api/2.0/namespace/datacenter/` devuelve una URL con una ruta absoluta, por ejemplo

`http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2.`

En las versiones anteriores de NSX, esta llamada API devolvía una URL con una ruta de acceso relativa, por ejemplo: `/api/2.0/namespace/datacenter/datacenter-1628/2.`

*Solución alternativa:* Ninguna.

## Problemas conocidos de redes lógicas y problemas conocidos de NSX Edge

**Nuevo Problema 1825416:** Se produce un error de las vApps contenidas en vCloud Director 8.20 tras actualizar a NSX for vSphere 6.3.x

Tras actualizar a NSX 6.3.x y NSX Edge Gateways a 6.3.x en vCloud Director 8.20, se produce un error de las vApps contenidas y las máquinas virtuales de la red contenida no se pueden comunicar con su puerta de enlace. Consulte el [artículo 2150010 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.

**Nuevo Problema 1781438:** En el dispositivo 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.

**Nuevo 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.

**Nuevo Problema 1791264:** Al hacer doble clic en una zona de transporte, no se puede habilitar o deshabilitar el modo CDO.

Si intenta habilitar o deshabilitar el modo CDO desde la página Resumen (Summary) a la que se accede después de hacer doble clic en una zona de transporte desde vSphere Web Client, la acción no surte efecto.

*Solución alternativa:* Haga lo siguiente:

1. Vuelva a la página de resumen de la zona de transporte: Instalación (Installation) > Preparación de redes lógicas (Logical Network Preparation) > Zonas de transporte (Transport Zones) y seleccione la zona de transporte deseada.
2. Seleccione Habilitar modo CDO/Deshabilitar modo CDO (Enable CDO mode/Disable CDO mode) en el menú desplegable Acciones (Actions).
3. Se aplicará la acción seleccionada.

**Nuevo Problema 1773500:** Una ruta no válida (0.0.0.0/32) provoca que NSX se bloquee

Si inserta la ruta 0.0.0.0/32 en el DLR de NSX, esta no se admite y se rechaza. Sin embargo, esto causa un bloqueo (PSOD) cuando la LIF asociada se elimina y se vuelve a agregar con una dirección IP en la misma subred.

*Solución alternativa:* 0.0.0.0/32 no es una ruta válida. No la configure ni utilice ningún mapa de rutas para rechazarla.

**Nuevo**Problema 1769941: Tabla del puente L2VPN "dañada" por la dirección PMAC del DLR con una respuesta de ARP duplicada

El puerto troncal vxlan del servidor L2VPN en el host no coloca la respuesta de ARP que procede de la máquina virtual del cliente con una dirección MAC de destino como pMAC, lo que provoca que la tabla MAC del puente se dañe y se bloquee el tráfico.

*Solución alternativa:* Para solucionar este problema, agregue un filtro de tráfico para el puerto dvport troncal de VXLAN con el fin de colocar la respuesta de ARP destinada a la dirección pMAC.

Para agregar un calificador de tráfico:

1. Vaya a dvport, donde está conectado NSX Edge.
2. Desplácese hasta Editar configuración (Edit settings) > Filtrado y marcado de tráfico (Traffic Filtering and Marking).
3. Agregue un calificador de MAC con el destino configurado para pMAC.

**Nuevo**Problema 1782321: Algunas instancias de NSX Edge se enfrentan a situaciones de cerebro dividido, incluso si se muestra correctamente el estado de alta disponibilidad

Debido a una condición de carrera en el mecanismo de HA, es posible que algunas instancias de NSX Edge actualizadas a NSX 6.2.5 y versiones posteriores se enfrenten a un escenario de cerebro dividido, incluso si se muestra correctamente el estado de alta disponibilidad. Esto también podría ocurrir después de una nueva implementación de Edge.

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

**Nuevo**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.

**Nuevo**Problema 1771760: NSX Edge bloquea los paquetes de respuesta SNMP que contienen Counter64 del tipo OID cuando se habilite NAT.

SNMP ALG en NSX Edge no puede procesar los tipos Counter64 del paquete de respuesta SNMP y este se bloqueará. Como resultado, el cliente no obtiene ninguna respuesta para la solicitud.

*Solución alternativa:* Si se detecta este problema, póngase en contacto con el servicio de atención al cliente de VMware.

**Nuevo**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.

**Nuevo**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.

**Nuevo 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*

**Nuevo Problema 1803220:** Pérdida de conectividad de VXLAN con hosts con la función CDO habilitada cuando la conexión entre el controlador y el host se queda inactiva.

La función Operación con controlador desconectado (Controller Disconnected Operation, CDO) garantiza la conectividad de la VXLAN cuando todo el clúster de controladores está inactivo o inaccesible. Sin embargo, en los casos en los que el clúster de controladoras esté Activo (Up) y un host pierda la conectividad con él, podría descartarse el tráfico del plano de datos destinado a dicho host desde otros hosts que estén conectados a la controladora. Cuando se produce esta condición, el host se eliminó de la lista VTEP por VNI y se descartan los ARP enviados por hosts remotos. Para el tráfico que se origina en el host que ha perdido la conectividad con el controlador, la función CDO garantiza que será capaz de llegar al destino adecuado.

**Nuevo 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.

**Nuevo 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.

**Nuevo Problema 1773127:** En configuraciones con un número significativo de hosts y conmutadores lógicos, no se puede cargar correctamente la pantalla que muestra los hosts relacionados con un determinado conmutador lógico.

Cuando selecciona Conmutador lógico (Logical Switch) > Objetos relacionados (Related Objects) > Hosts en su configuración con un número de hosts significativo, vSphere Web Client no puede cargar tras esperar un par de minutos y se muestra el siguiente error: Se agotó el tiempo de espera del servicio de datos porque una tarea backend tardó más de 120 segundos en ejecutarse. Esto se produce porque la llamada de la API remota a NSX Manager tarda mucho en regresar.

**Solución alternativa:** Existen dos maneras de evitar este problema:

- La primera opción: Puede evitar este problema aumentando el tiempo de espera de la API, tal como se describe en el [artículo 2040626 de la base de conocimientos de VMware](#). Puede que tenga que reiniciar vSphere Web Client tras aumentar este tiempo de espera. El resultado más probable de aumentar el tiempo de espera es que no se produzca el error, pero tendrá que esperar entre 2 y 4 minutos a que se vuelva a cargar la página.
- La segunda opción: Si solo quiere ver correctamente los hosts relacionados, puede ir a Inicio (Home) > Redes (Networking) > Grupo de puertos (Port group) > Objetos relacionados (Related Objects) > Hosts para ver la lista de hosts asociados al conmutador lógico.

**Nuevo Problema 177792:** 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).

**Nuevo Problema 1770114:** El mensaje de error en el nivel del clúster no desaparece tras preparar el host correctamente.

Si asigna un grupo de direcciones IP a un clúster que no tiene suficientes direcciones IP y, a continuación, intenta agregar un host a este clúster, obtiene el error "Direcciones IP insuficientes" (Insufficient IP addresses). Incluso después de cambiar este grupo para agregar direcciones IP adicionales y de que pueda agregar correctamente hosts a este clúster, el mensaje de error se sigue mostrando a nivel de clúster.

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

**Problema 1789088:** NSX Edge atascado en el símbolo del sistema de grub.

NSX Edge puede fallar al arrancar y se puede quedar atascado en el símbolo del sistema de grub.

### *Solución alternativa:*

- En primer lugar, investigue:
  1. Compruebe el entorno existente con el comando `set`.
  2. Utilice los comandos `ls` y `cat` para localizar y volcar el archivo `/boot/grub/grub.cfg`.

```
grub> ls /boot
grub> ls /boot/grub
grub> cat /boot/grub/grub.cfg
```
  3. Capture los registros de host en este momento (lo más cerca posible al momento en que se produce el problema). Puede que haya algunos registros de NFS que indiquen un problema de almacenamiento NFS.
- A continuación, inicie manualmente NSX Edge. Intente lo siguiente en el orden indicado a continuación (pruebe la siguiente opción solo en caso de que con la opción anterior no se inicie Edge correctamente):
  1. Reinicie la VM de Edge seleccionando la opción Reiniciar (Power Reset) en vSphere Web Client.
  2. O especifique de nuevo el archivo de configuración grub, que debería cargar inmediatamente el menú que reinicia Edge.  
Invoque el siguiente comando en el símbolo del sistema de grub:

```
grub> configfile /boot/grub/grub.cfg
```

3. O utilice los siguientes comandos en el símbolo del sistema de grub:

```
grub> insmod ext2
grub> set root=(hd0,1)
grub> linux /boot/vmlinuz loglevel=3 root=/dev/sda1
grub> boot
```

**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 EBGP, 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 eBGP 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 eBGP.

*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 1676085:** No se puede habilitar HA de Edge si se produce un error en la reserva de recursos

A partir de NSX for vSphere 6.2.3, se producirá un error al habilitar la alta disponibilidad en una instancia de Edge existente cuando no se puedan reservar recursos suficientes para el dispositivo de la máquina virtual de Edge secundario. La configuración se restaurará a la última configuración conocida y efectiva. En las versiones anteriores, si se habilita HA antes de la implementación de Edge y se produce un error en la reserva de recursos, se crea la máquina virtual de Edge igualmente.

*Solución alternativa:* Este cambio de comportamiento es correcto.

**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 API <https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status> con *detailedStatus=true*.

**Problema 1556924:** Error Bloquearía (Would Block) por la pérdida de conectividad de L3 con VXLAN

Si las LIF de DLR están configuradas en el host, pero la capa de VXLAN subyacente no está completamente preparada, puede verse afectada la conectividad de algunas LIF de DLR. No se puede establecer la comunicación con algunas de las máquinas virtuales que pertenecen al DLR. Es posible que haya registros de tipo "Error al crear estado troncal de VXLAN: Bloquearía" (*Failed to Create VXLAN trunk status: Would Block*) en el archivo `/var/log/vmkernel.log`.

**Solución alternativa:** Puede eliminar las LIF y volver a crearlas. Otra posibilidad es reiniciar los hosts ESX afectados por el problema.

**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 1604514:** Falla la edición o configuración de la puerta de enlace predeterminada de un DLR no administrado después de hacer clic en Publicar (Publish)

Cuando se agrega una puerta de enlace predeterminada a un DLR no administrado, falla la publicación con el error "La distancia de enrutamiento solo se admite en NSX Edge versión 6.2.0 y posteriores con máquinas virtuales de NSX Edge implementadas" (Routing Distance is support only on NSX Edge version 6.2.0 and later with NSX Edge VMs deployed). Esto se produce a causa de la distancia administrativa predeterminada "1" rellena en la interfaz de usuario.

*Solución alternativa:* Elimine la distancia administrativa "1", que se proporciona de forma predeterminada.

**Problema 1642087:** Después de modificar el valor del parámetro `securelocaltrafficbyip` en la extensión VPN IPsec, falla el reenvío a las redes de destino

Al utilizar una puerta de enlace de servicios NSX Edge, se produce lo siguiente:

- Después de cambiar el valor `securelocaltrafficbyip` a 0 en la pantalla Editar VPN IPsec (Edit IPsec VPN) de la interfaz de usuario de NSX, no funciona el reenvío a una subred remota del túnel VPN IPsec
- Después de cambiar este parámetro, ya no se muestra la información correcta de una subred remota en la tabla de enrutamiento IP

*Solución alternativa:* Deshabilite y vuelva a habilitar el servicio VPN IPsec. A continuación, compruebe que se muestre la información de enrutamiento prevista en la CLI y la interfaz de usuario.

**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 1534603:** 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 1534799:** La convergencia es lenta si el enrutador de borde de área OSPF que tiene la dirección IP superior está apagado

La convergencia es lenta si el enrutador de borde de área (ABR) OSPF basado en NSX que tiene la dirección IP superior está apagado o reiniciado. Si un ABR que no tiene una dirección IP numéricamente superior está apagado o reiniciado, el tráfico se dirige rápidamente a otra ruta de acceso. Sin embargo, si el enrutador de borde de área (ABR) que tiene la dirección IP superior está apagado o reiniciado, el proceso para volver a dirigir el tráfico tardará varios minutos. El proceso OSPF se puede eliminar manualmente para reducir el tiempo de convergencia.

**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 1089745:** 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 1498965:** 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 1494025:** 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 1288487:** 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?vmogl=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 DVPG 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

**Nuevo Problema 1847753:** Se produce un error en el host y se muestra una pantalla de diagnóstico de color púrpura cuando se recuperan flujos para los protocolos con ALG habilitado

Después de actualizar NSX for vSphere 6.2.4 a 6.3.0 o a 6.3.1 con Flow Monitoring habilitado en el entorno, aparece una pantalla de diagnóstico de color púrpura en el host ESXi. Consulte el [artículo 2149908 de la base de conocimientos de VMware](#) para obtener más información y una solución alternativa.

**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

**Nuevo Problema 1676043:** Una máquina virtual se elimina de la lista de exclusiones después de dos adiciones simultáneas

Si dos usuarios agregan dos veces de forma simultánea la misma máquina virtual a la Lista de exclusión (Exclude List) sin actualizar la interfaz de usuario, esto provoca que las máquinas virtuales que ya están agregadas se eliminen de esta lista.

*Solución alternativa:* Actualice la interfaz de usuario de vSphere Web Client antes de agregar la máquina virtual a la Lista de exclusión (Exclude List).

**Nuevo Problema 1770259:** El campo `appliedTo` de la regla de DFW no se puede modificar de forma que tenga varios objetos `appliedTo`

Cuando aplica la regla de DFW a un grupo de vNIC, de máquinas virtuales, de clústeres o de centros de datos, la publica y, posteriormente, desea modificarla agregando objetos adicionales al campo `appliedTo`, los nuevos cambios no tendrán efecto aunque se publiquen con éxito.

*Solución alternativa:* Ninguna.

**Nuevo Problema 1798779:** Tras actualizar NSX de la versión 6.2.x a la versión 6.3.0, la GUI de vSphere Web Client le permite de forma errónea agregar una etiqueta de seguridad universal. La versión 6.3.0 introduce las etiquetas de seguridad universales. Al intentar agregar un grupo de etiquetas de seguridad universal que se creó en 6.2.x antes de la actualización a NSX 6.3.0, la operación falla con el error "El miembro solicitado no es un miembro válido" (The requested member is not a valid member). Este error es correcto porque no puede agregar una etiqueta de seguridad universal a un grupo de seguridad universal de NSX 6.2.x. La GUI da lugar a confusión.

*Solución alternativa:* Tras realizar la actualización, cree un grupo de seguridad universal NSX 6.3.0 y agregue las etiquetas de seguridad universales a ese grupo.

**Nuevo 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.

**Nuevo Problema 1786780:** Reordenar/mover las directivas en la UI de Service Composer requiere mucho tiempo y consume mucha CPU.

Reordenar o recolocar las directivas de la UI de Service Composer puede tardar mucho tiempo y consumir una gran cantidad de recursos de la CPU.

*Solución alternativa:* Los siguientes pasos sirven de ayuda:

- Al crear la directiva, intente concederle la precedencia (peso) adecuada a fin de que se coloque en la posición adecuada desde el principio, para no tener que reordenar las directivas.
- Si tiene que cambiar la posición de una directiva, edítela y establezca un valor adecuado de precedencia (peso). Esto dará lugar a la modificación de una única directiva y a un final rápido.

**Nuevo 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, etiquete 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 1462027:** En las implementaciones de Cross vCenter NSX, se replican varias versiones de las configuraciones de firewall guardadas en las instancias de NSX Manager secundarias

La sincronización universal guarda varias copias de la configuración universal en las instancias de NSX Manager secundarias. La lista de configuraciones guardadas contiene varios borradores creados por la sincronización a través de los NSX Manager con el mismo nombre y en el mismo momento o con una diferencia de 1 segundo.

*Solución alternativa:* Ejecute la llamada API para eliminar los borradores duplicados.

DELETE : <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/>

Busque los borradores que se deben eliminar; para ello vea todos los borradores:

GET: <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts>

En los resultados de muestra siguientes, los borradores 143 y 144 tienen el mismo nombre y se crearon a la misma hora, por lo tanto, son duplicados. Lo mismo sucede con los borradores 127 y 128: tienen el mismo nombre y una diferencia de 1 segundo; también son duplicados.

```
<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
timestamp="1438808882608">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
timestamp="1438808881750">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
</firewallDrafts>
```

**Problema 1449611:** Cuando una directiva de firewall en Service Composer no está sincronizada debido a un grupo de seguridad eliminado, no se puede solucionar la regla de firewall en la interfaz de usuario

*Solución alternativa:* En la interfaz de usuario, puede eliminar la regla de firewall no válida y, a continuación, volver a agregarla. O, en la API, puede solucionar la regla de firewall eliminando el grupo de seguridad no válido. Después, 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, modifique las reglas de firewall para que no refieran a los grupos de seguridad antes de eliminar los grupos de seguridad.

**Problema 1557880:** Es posible que falten las reglas de la Capa 2 (L2) si se modificó la dirección MAC de una máquina virtual utilizada en las reglas

Dado que la optimización de reglas de L2 está activada de forma predeterminada, las reglas de L2 con los campos de origen y de destino especificados (otra opción distinta a "cualquiera" ["any"]) se aplicarán a los vNIC (o filtros) solo si la dirección MAC del vNIC coincide con la lista de direcciones MAC de origen o destino. No se aplicarán estas reglas de L2 en los hosts con máquinas virtuales que no coincidan con las direcciones MAC de origen o destino.

*Solución alternativa:* Para que se apliquen las reglas de Capa 2 a todos los vNIC (o filtros), establezca uno de los campos de fuente o destino en "cualquiera" (any).

**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.

**Problema 1626233:** Cuando la máquina virtual de servicio (SVM) de NetX coloca paquetes, Traceflow no genera observaciones de colocación

La sesión de Traceflow se inicia después de enviar el paquete a la máquina virtual de servicio (SVM) de NetX. Cuando la SVM coloca paquetes, Traceflow no genera observaciones de colocación.

*Solución alternativa:* No hay solución. Si el paquete de Traceflow no se vuelve a insertar, se puede asumir que la SVM colocó el paquete.

## 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.

## Problemas conocidos de NSX Controller

**Problema 1765354:** <deployType> es una propiedad obligatoria, pero no se usa  
<deployType> es una propiedad obligatoria, pero no se usa y no tiene ningún significado.

## Problema 1516207: Es posible que los controladores se aíslen cuando se vuelva a habilitar la comunicación IPsec en un clúster de NSX Controller

Si el clúster de un controlador de NSX está configurado para permitir comunicaciones entre controladores de forma clara (IPsec está deshabilitado) y posteriormente se vuelve a habilitar la comunicación IPsec, es posible que una o varios controladores se aíslen del clúster debido principalmente a que no coincide la clave previamente compartida ("PSK"). Cuando esto ocurre, es posible que la API de NSX no pueda cambiar la configuración de IPsec de los controladores.

### *Solución alternativa:*

Siga estos pasos para solucionar este problema:

#### 1. Deshabilite IPsec a través de NSX API.

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>false</ipSecEnabled>
</controllerNodeConfig>
```

#### 2. Vuelva a habilitar IPsec mediante NSX API.

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>true</ipSecEnabled>
</controllerNodeConfig>
```

Aplique estas prácticas recomendadas para evitar este problema:

- Use siempre NSX API para deshabilitar IPsec. No se admite el uso de la CLI de NSX Controller para deshabilitar IPsec.
- Verifique siempre que todos los controladores estén activos antes de usar la API para cambiar la configuración de IPsec.

## Problema 1306408: Los registros de NSX Controller se deben descargar secuencialmente

Los registros de NSX Controller no se pueden descargar simultáneamente. Incluso cuando se realiza una descarga desde varios controladores, se debe esperar a que la descarga del controlador actual finalice antes de iniciar la descarga del controlador siguiente. Además, se debe tener en cuenta que no se puede cancelar una descarga de registro una vez que se inició.

*Solución alternativa:* Espere a que finalice la descarga del registro del controlador actual antes de iniciar otra descarga de registro.

# Problemas resueltos

## Nuevo Problemas resueltos en NSX 6.3.0

Los problemas resueltos en la versión 6.3.0 de NSX se agrupan de la siguiente manera:

- [Problemas conocidos resueltos en NSX 6.3.0](#)
- [Problemas de instalación y actualización resueltos en NSX 6.3.0](#)
- [Problemas de NSX Manager resueltos en NSX 6.3.0](#)
- [Problemas de servicios Edge y de redes resueltos en NSX 6.3.0](#)
- [Problemas de servicios de seguridad resueltos en NSX 6.3.0](#)
- [Problemas de interoperabilidad de soluciones resueltos en NSX 6.3.0](#)

## Problemas conocidos resueltos en NSX 6.3.0

**Problema solucionado 1497389:** Los usuarios con privilegios de administrador de NSX pueden cambiar esos privilegios a los de administrador empresarial, que es una función de usuario más alta. A partir de NSX 6.3.0, los usuarios con privilegios de administrador de NSX no pueden administrar los usuarios; solo pueden hacerlo aquellos con privilegios de administrador empresarial. *Solucionado en NSX 6.3.0.*

**Problemas solucionados 1575342, 1719402:** En un entorno NSX for vSphere 6.x, cuando una máquina virtual de servicios (SVM) se migra con vMotion/SvMotion, es posible que se produzca alguna interrupción en el servicio o que se bloquee el host ESXi

A partir de la versión 6.3.0, no es posible migrar una máquina virtual de servicios (SVM) usando vMotion/SvMotion. Para que las máquinas virtuales de servicios funcionen correctamente, se deben mantener en el host en el que se implementaron.

En versiones anteriores, era posible migrar a otro host, pero esta operación no se admitía, lo que provocaba que se interrumpiera el servicio y que se produjeran problemas con el host.

Consulte el [artículo 2141410 de la base de conocimientos de VMware](#) para obtener más información.

*Solucionado en NSX 6.3.0.*

**Problema solucionado 1708769:** Aumentó la latencia en la máquina virtual segura (máquina virtual de servicios) tras ejecutar una instantánea en NSX

Este problema se produce porque al ejecutar una instantánea en una máquina virtual de servicios (máquina virtual segura) se puede producir una latencia adicional en la red. En algunas ocasiones, las aplicaciones de copia de seguridad que se ejecutan en el entorno invocan la instantánea. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1760102:** Es posible que las máquinas virtuales no puedan comunicarse después de eliminar NSX Controller y volver a implementarlo para recuperarse de un estado de falta de almacenamiento

Es posible que un entorno de NSX Controller for vSphere 6.2.4/6.2.5 esté en modo de solo lectura si se queda sin almacenamiento. Si elimina y vuelve a implementar el controlador para que se recupere de ese estado, es posible que algunas máquinas virtuales presenten errores de comunicación. Si se produce una interrupción en el almacenamiento de un controlador, se espera que se recupere del modo de solo lectura al reiniciarlo, pero esto no sucede actualmente en NSX. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1662842:** Guest Introspection: Se pierde la conexión entre MUX y USVM cuando se intenta resolver las SID de Windows sin solución

El servicio de Guest Introspection entra en estado de advertencia y cada instancia de Guest Introspection entra y sale de dicho estado. Hasta que la máquina virtual de Guest Introspection se vuelva a conectar, los eventos de la red no se enviarán a NSX Manager. Esto afectará tanto a la supervisión de la actividad como al firewall de ID si se detectan eventos de inicio de sesión a través de la ruta de Guest Introspection.

*Solucionado en NSX 6.3.0.*

**Problema solucionado 1752051:** El estado del servicio de Guest Introspection aparece como "No listo" (Not Ready) cuando se alcanza el tiempo de espera de la comunicación de NSX Manager con USVM.

Puede aparecer un mensaje de error similar a "Inicio de sesión PLAIN rechazada: usuario 'usvm-admin-host-14' - credenciales no válidas" para las Universal SVM de Guest Introspection cuando no se realice con éxito el proceso de cambio de contraseña con NSX Manager en el bus de mensajería interna (rabbit MQ). *Solucionado en NSX 6.3.0.*

**Problema solucionado 1716328:** Si se elimina un host que está en modo de mantenimiento, puede aparecer un error en la preparación del clúster

Si un administrador establece un host ESXi compatible con NSX en modo de mantenimiento y lo elimina de un clúster preparado con NSX, NSX no puede eliminar los registros del número ID del host eliminado. Después de que se realice la instalación en este estado, si existe otro host con el mismo ID en otro clúster o si este host se agrega a otro clúster, se producirá un error en el proceso de preparación de dicho clúster. *Solucionado en NSX 6.3.0.*



**Problema solucionado 1710624:** El servidor de registro de eventos Windows 2008 se agregó como "TIPO" ("TYPE") de "WIN2K3", si serverType no está especificado en el cuerpo de solicitud de la API REST

Si crea la solicitud de la API del servidor EventLog, el servidor se agregará como "TIPO" ("TYPE") de "WIN2K3". Si usa el servidor EventLog solo para IDFW, es posible que este firewall no funcione correctamente. *Solucionado en NSX 6.3.0.*

## Problemas de instalación y actualización resueltos en NSX 6.3.0

**Problema solucionado 1463767:** En una implementación de Cross vCenter, es posible que una sección de configuración de firewall universal esté bajo (subordinada a) una sección de configuración local

Si se traslada una instancia de NSX Manager secundaria al estado independiente (tránsito) y, a continuación, se la regresa al estado secundario, cualquier cambio en la configuración local que se haya hecho mientras se encontraba de forma temporal en modo independiente puede aparecer sobre las secciones de configuración universal replicadas heredadas de la instancia de NSX Manager principal. Esto genera la condición de error la sección universal debe estar sobre todas las demás secciones en las instancias de NSX Manager secundarias (universal section has to be on top of all other sections on secondary NSX Managers).

*Solucionado en NSX 6.3.0.*

**Problema solucionado 1402307:** Si se reinicia vCenter durante el proceso de actualización de NSX for vSphere, se muestra un estado del clúster incorrecto

Cuando se realiza la preparación del host en un entorno con varios clústeres preparados con NSX durante una actualización y vCenter Server se reinicia después de que se preparó al menos un clúster, los demás clústeres pueden mostrar el estado de clúster como No listo (Not Ready) en lugar de mostrar un vínculo de actualización. Los hosts en vCenter también pueden mostrar el estado Reinicio necesario (Reboot Required).

*Solucionado en NSX 6.3.0.*

**Problema solucionado 1495307:** Durante una actualización, las reglas de firewall L2 y L3 no se publican en los hosts

Después de publicar un cambio en la configuración de Distributed Firewall, el estado permanece `En curso` (InProgress) tanto en la interfaz de usuario como en la API de manera indefinida, y no se escribe ningún registro para las reglas L2 o L3 en el archivo vsfwd.log. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1491820:** El registro de NSX Manager recopila mensajes `WARN messagingTaskExecutor-7` después de la actualización a NSX 6.2

Después de actualizar de NSX 6.1.x a NSX 6.2, el registro de NSX Manager se llena de mensajes similares al siguiente: `WARN messagingTaskExecutor-7 ControllerInfoHandler:48 - host is unknown: host-15 return empty list`. No afectan el funcionamiento. *Solucionado en 6.3.0.*

## Problemas de NSX Manager resueltos en NSX 6.3.0

**Problema solucionado 1671067:** El complemento de NSX no aparece en vCenter Web Client, mientras que el complemento ESXTOP está también instalado

Tras implementar NSX y registrarlo correctamente en vCenter, el complemento de NSX no aparece en vCenter Web Client. Este problema está originado por un conflicto entre el complemento de NSX y el complemento ESXTOP. *Solucionado en NSX 6.3.0.*

## Problemas de servicios Edge y de redes resueltos en NSX 6.3.0

**Problema solucionado 1740231:** No se puede agregar la dirección IP en la interfaz de HA

A partir de la versión 6.3.0, puede agregar direcciones IP en la interfaz de HA de DLR. Esta funcionalidad no estaba disponible en algunas de las versiones anteriores de NSX, pero se introdujo de nuevo para que coincida con el comportamiento de la API de la interfaz de administración de HA de DLR. *Solucionado en NSX 6.3.0*

**Problema solucionado 1716333:** Cambiar el tamaño de la VM de Edge o un parámetro de colocación mientras se habilita o deshabilita la función de alta disponibilidad (HA) de Edge puede crear VM de Edge adicionales.

Las operaciones simultáneas de cambio del tamaño de la VM de Edge o un parámetro de colocación (como almacén de datos —datastore— o grupo de recursos —resource pool—), así como la habilitación o la deshabilitación de la función de alta disponibilidad (HA) de Edge pueden dañar la base de datos de objetos administrada por NSX, y de este modo descartar las VM de Edge que no se pueden utilizar. Además, en un entorno con cross-vCenter, las VM de Edge abandonadas se replicarán en el sitio secundario. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1717369:** Cuando se configuran en modo de alta disponibilidad (HA), las máquinas virtuales de Edge activas y en espera se pueden implementar en el mismo host.

Este problema se debe a que no se crearon ni aplicaron automáticamente reglas de antiafinidad en los hosts de vSphere durante las operaciones de actualización y reimplementación. Este problema no se producirá cuando se habilite alta disponibilidad en una instancia de Edge existente.

*Solucionado en NSX 6.3.0.* El comportamiento indicado a continuación es el esperado:

- Si se habilitó vSphere HA, se crearán reglas de antiafinidad para las máquinas virtuales de Edge de un par HA durante la actualización o reimplementación.
- Si se deshabilitó vSphere HA, no se crearán reglas de antiafinidad para las máquinas virtuales de Edge de un par HA.

**Problema solucionado 1675659:** Se prefieren enrutamientos estáticos flotantes a los dinámicos OSPF. Se introduce un enrutamiento estático flotante de forma incorrecta en una tabla de enrutamiento de Edge cuando la Redistribución del enrutamiento (Route Redistribution) aparece habilitada aunque esté disponible un enrutamiento OSPF. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1733165:** IPsec puede hacer que se eliminen rutas estáticas de la tabla de reenvío de NSX Edge

Si se usa una subred a la que se puede acceder a través de una ruta dinámica como una subred remota para la configuración de IPsec, NSX Edge la elimina de la tabla de reenvío y no vuelve a instalarla aunque esta subred se elimine de la configuración de IPsec. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1663902:** El cambio de nombre de una máquina virtual de NSX Edge interrumpe el flujo de tráfico a través de Edge

El cambio de nombre de una máquina virtual de NSX Edge interrumpe el flujo de tráfico a través de Edge. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1624663:** Después de hacer clic en "Configurar depuración avanzada" (Configure Advanced Debugging), la interfaz de usuario de vCenter se actualiza, pero el cambio no se mantiene

Después de hacer clic en el ID de una instancia concreta de Edge > Configuración > Acción > Configurar depuración avanzada (Configuration > Action > Configure Advanced Debugging), la interfaz de usuario de vCenter se actualiza, pero el cambio no se mantiene. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1706429:** Los problemas de comunicación al habilitar la alta disponibilidad (HA) después de la implementación inicial del enrutador lógico (distribuido) pueden causar que ambos dispositivos enrutadores estén activos.

Si implementa un enrutador lógico sin HA y la habilita posteriormente (al implementar un nuevo enrutador lógico) o si la deshabilita y luego la vuelve a habilitar, en algunas ocasiones, uno de los enrutadores lógicos no tiene una ruta conectada a la interfaz de HA. Esto provoca que ambos dispositivos estén en estado activo. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1542416:** La ruta de datos no funciona durante 5 minutos después de volver a implementar el borde y se produce una conmutación por error de HA con las subinterfaces

Las operaciones de conmutación por error de HA o de reimplementación sufrirán cinco minutos de interrupción si se utilizan subinterfaces. No se aprecian problemas en las interfaces. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1492547:** Aumenta el tiempo de convergencia cuando el enrutador de borde de área OSPF basado en NSX que tiene la dirección IP superior está apagado o se ha reiniciado. Si un enrutador de borde de área NSSA que no tiene la dirección IP superior está apagado o se ha reiniciado, el tráfico se dirige rápidamente a otra ruta de acceso. Si un enrutador de borde de área NSSA que tiene la dirección IP superior está apagado o se ha reiniciado, el proceso para volver a dirigir el tráfico tardará varios minutos. El proceso OSPF se puede eliminar manualmente para reducir el tiempo de convergencia. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1510724:** Las rutas predeterminadas no se rellenan en los hosts tras la creación de un enrutador lógico distribuido universal (Universal Distributed Logical Router, UDLR). Tras cambiar NSX Manager del modo independiente al principal con el propósito de configurar Cross-vCenter en NSX para vSphere 6.2.x, es posible que observe estos síntomas:

- Al crear un UDLR nuevo, las rutas predeterminadas no se rellenan en la instancia del host.
- Las rutas se rellenan en la máquina virtual de control del UDLR, pero no en la instancia del host.
- El comando *show logical-router host host-ID dlr Edge-ID route* no muestra las rutas predeterminadas debido a un error.

*Solucionado en NSX 6.3.0.*

**Problema solucionado 1704540:** El gran volumen de la tabla de detección de MAC se actualiza con el puente de Capa 2 de NSX y el LACP podría ocasionar una situación de agotamiento de memoria. Si un puente de Capa 2 de NSX ve una dirección MAC en otro vínculo superior, notifica un cambio de tabla de detección de MAC a los controladores a través del proceso netcpa. Los entornos de red que utilizan el LACP conocerán la misma dirección MAC en varias interfaces, lo que dará lugar a un gran volumen de actualizaciones de tablas y potencialmente agotará la memoria que el proceso netcpa necesita para realizar la notificación. Consulte el [artículo 2147181 de la base de conocimientos de VMware](#). *Solucionado en NSX 6.3.0.*

**Problema solucionado 1716545:** Cambiar el tamaño del dispositivo de Edge no afecta a la reserva de memoria y CPU de Edge en espera.

Solo se asigna a la configuración de reserva la primera máquina virtual de Edge creada como parte de un par HA.

**Problema solucionado 1772004:** La conmutación por error de alta disponibilidad (HA) de Edge del nodo 0 al 1 tarda más de lo esperado.

La conmutación por error del nodo 0 al 1 tarda más de lo esperado en un entorno configurado en modo de alta disponibilidad de Edge. Sin embargo, la conmutación por error del tráfico del nodo 1 al 0 es normal. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1726379:** Si un rango de multidifusión IP tiene un valor de enlace superior mayor a 99 en los últimos tres octetos, se produce un error en la configuración del grupo de puertos troncal de VXLAN.

Al configurar un ID de segmento, si crea un valor de IP de multidifusión con un valor de enlace superior mayor a 99 en los últimos tres octetos, por ejemplo, 1.100.100.100, y un conmutador lógico híbrido o de multidifusión con el mismo rango, se producirá un error en la configuración del grupo de puertos troncal de VXLAN. *Solucionado en NSX 6.3.0.*

## Problemas de servicios de seguridad resueltos en NSX 6.3.0

**Problema solucionado 1767402:** Las reglas DFW con "Se aplica a" (Applied To) establecido en un "grupo de seguridad" no se publican en los hosts.

Las reglas DFW con el campo "Se aplica a" (Applied To) establecido en un grupo de seguridad no se envían a los hosts ESXi en un clúster nuevo. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1743366:** La opción Supervisar el umbral NSX (NSX Threshold Monitoring) está deshabilitada de forma predeterminada para evitar un posible bloqueo

Cuando se ejecuta el módulo Firewall, NSX deshabilita la supervisión de umbral de memoria para evitar un posible bloqueo. Cuando el host ejecuta ESX 6.5P01 o ESX 6.0U3 o una versión posterior, se habilita de forma automática la supervisión del umbral de memoria. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1491046:** La dirección IP IPv4 no se aprueba automáticamente

La dirección IP IPv4 no se aprueba automáticamente cuando la directiva SpoofGuard está establecida en Confiar en el primer uso [Trust On First Use (TOFU)] en VMware NSX for vSphere 6.2.x. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1686036:** No se pueden agregar, editar o eliminar las reglas de firewall si se elimina la sección predeterminada

Si la sección Layer2 o Layer3 predeterminadas están eliminadas, se produce un error al publicar una regla de firewall. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1717994:** Al consultar la API del estado del firewall distribuido (DFW) aparece un mensaje 500 error interno del servidor de forma intermitente

Si se realiza una consulta de API del estado del DFW mientras se agrega un nuevo host en un clúster preparado para dicho host, se produce un error de tipo "500 error interno del servidor" al intentar consultar la API varias veces y, a continuación, devuelve la respuesta correcta una vez que el host comienza a obtener los VIB instalados. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1717635:** Se produce un error en la operación de la configuración del firewall si más de un clúster están presentes en el entorno y los cambios se realizan en paralelo

En un entorno con varios clústeres, si dos o más usuarios modifican la configuración del firewall continuamente en bucle (por ejemplo, reglas o secciones Agregar o Eliminar), se puede producir un error en algunas operaciones y el usuario verá una respuesta de API similar a:

```
org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update;  
nested exception is javax.persistence.PersistenceException:  
org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update  
Solucionado en NSX 6.3.0.
```

**Problema solucionado 1707931:** El orden de las reglas de firewall distribuido cambia cuando existen directivas de servicio definidas en Service Composer y se modifica o publica una regla de firewall con un filtro aplicado en la interfaz de usuario del firewall

Al cambiar el orden, agregar o eliminar directivas de servicio creadas en Service Composer tras realizar una o varias operaciones de publicación desde Redes y seguridad > Interfaz de usuario de firewall (Networking & Security > Firewall UI), se cambiará el orden de las reglas de firewall y podría causar consecuencias involuntarias. *Solucionado en 6.3.0.*

**Problema solucionado 1682552:** No se informa sobre los eventos del umbral de la CPU, memoria o CPS de Distributed Firewall (DFW)

Aunque el umbral de DFW para la CPU, memoria y CPS esté configurado para enviar informes, no se envían los correspondientes a los eventos del umbral cuando dichos umbrales están cruzados. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1620460:** NSX no puede evitar que los usuarios creen reglas en la sección de reglas de Service Composer

En vSphere Web Client, la interfaz Redes y seguridad: La interfaz de Firewall no puede evitar que los usuarios agreguen reglas a la sección de reglas de Service Composer. Los usuarios deben poder agregar reglas antes o después de la sección Service Composer, pero no dentro de ella. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1445897:** Error al publicar reglas de Distributed Firewall (DFW) tras eliminar un objeto de referencia en VMware NSX for vSphere 6.1.x y 6.2.x *Solucionado en 6.2.3.*

**Problema solucionado 1704661 y 1739613:** Las máquinas virtuales pierden conectividad de red con el error: "No se pudo restaurar el estado de PF: Se superó el límite"

Las máquinas virtuales pierden conectividad de red con el error: "No se pudo restaurar el estado de PF: Se superó el límite." *Solucionado en NSX 6.3.0.*

## Problemas de interoperabilidad de soluciones resueltos en NSX 6.3.0

**Problema solucionado 1527402:** La máquina virtual de Windows con el controlador NSX Network Introspection pierde la conectividad TCP

En un entorno de VMware NSX for vSphere 6.x, la máquina virtual de Windows con el controlador NSX Network Introspection (vnetflt.sys) conectado a USVM (máquina virtual del servicio de Guest Introspection) pierde temporalmente la conectividad a la red TCP. *Solucionado en NSX 6.3.0.*

**Problema solucionado 1530360:** Tras la conmutación por error de una máquina virtual de NSX Manager, Site Recovery Manager (SRM) notifica de forma incorrecta un error de tiempo de espera. Tras una conmutación por error de una máquina virtual de NSX Manager, SRM notifica de forma incorrecta un error de tiempo de espera a la espera de VMware Tools. En este caso, VMware Tools está en realidad funcionando durante los 300 segundos de tiempo de espera. *Solucionado en NSX 6.3.0.*

## Historial de revisión del documento

2 de febrero de 2017: Primera edición de NSX 6.3.0.

3 de febrero de 2017: Segunda edición de NSX 6.3.0. Se agregó el problema conocido 1799543.

22 de febrero de 2017: Tercera edición de NSX 6.3.0. Se actualizó la información sobre CDO

27 de febrero de 2017: Cuarta edición para NSX 6.3.0. Se agregaron los problemas conocidos 1808478 y 1818257

30 de marzo de 2017: Quinta edición de NSX 6.3.0. Se agregaron los problemas conocidos 1474650 y 1782321

10 de abril de 2017: Sexta edición de NSX 6.3.0. Se agregó información a la sección Notas sobre la actualización.

03 de mayo de 2017: Séptima edición de NSX 6.3.0. Se agregó información sobre el desuso de vCNS Edge y VIX.

02 de junio de 2017: Octava edición de NSX 6.3.0. Se agregaron los problemas conocidos 1860583, 1781438 y 1825416.

22 de junio de 2017: Novena edición de NSX 6.3.0. Se agregó el problema conocido 1847753.

21 de agosto de 2017: Décima edición de NSX 6.3.0. Se agregó el problema solucionado 1463767 y se eliminaron algunos problemas anteriores.

2 de octubre de 2017: Undécima edición de NSX 6.3.0. Se actualizaron las versiones mínimas recomendadas.