



# Notas de la versión de VMware NSX for vSphere 6.3.7

VMware NSX for vSphere 6.3.7 | Publicado el 15 de noviembre de 2018 | Compilación 10667122

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

## Contenido de las notas de la versión

Las notas de la versión contienen los siguientes temas:

- [Novedades de NSX 6.3.7](#)
- [Instalación, versiones y requisitos del sistema](#)
- [Funciones obsoletas y suspendidas](#)
- [Notas sobre la actualización](#)
- [Cumplimiento de FIPS](#)
- [Historial de revisión](#)
- [Problemas resueltos](#)
- [Problemas conocidos](#)

## Novedades de NSX 6.3.7

NSX for vSphere 6.3.7 soluciona varios errores específicos de los clientes. Consulte la sección [Problemas resueltos](#) para obtener más información.

Consulte las notas de la versión de versiones anteriores:

- NSX [6.3.6](#)
- NSX [6.3.5](#)
- NSX [6.3.4](#)
- NSX [6.3.3](#)
- NSX [6.3.2](#)
- NSX [6.3.1](#)
- NSX [6.3.0](#)

## Instalación, versiones y requisitos del sistema

Nota:

- En la siguiente tabla, se muestran las versiones recomendadas del software de VMware. Estas recomendaciones son generales y no deben sustituir ni anular las recomendaciones específicas del entorno.
- Esta información está actualizada según la fecha de publicación de este documento.
- Consulte la [matriz de interoperabilidad de productos VMware](#) para conocer las versiones mínimas admitidas de NSX y de otros productos de VMware. VMware determina las versiones mínimas admitidas basándose en pruebas internas.

- La versión mínima admitida y requerida de vSphere para la interoperabilidad de NSX varía entre NSX 6.3.2 y NSX 6.3.3. Consulte la sección [Matriz de interoperabilidad de productos de VMware](#) para obtener más información.

Producto o componente	Versión recomendada
NSX for vSphere	<p>VMware recomienda la versión más reciente de NSX para nuevas implementaciones.</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> <li>• Utilice VMware Tools 10.1.10 y versiones posteriores para garantizar su compatibilidad con Windows Server 2016.</li> </ul>

Esta versión de NSX admite las siguientes versiones de Linux:

Guest Introspection  
para Linux

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

## Requisitos del sistema e instalación

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

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

## Funciones obsoletas y suspendidas

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

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

- **NSX for vSphere 6.1.x** llegó a las etapas de fin de disponibilidad (End of Availability, EOA) y de fin de soporte técnico general (End of General Support, EOGS) el 15 de enero de 2017. (Consulte también el [artículo 2144769 de la base de conocimientos de VMware](#)).
- **NSX for vSphere 6.2.x** llegará a la etapa de fin de soporte técnico general (End of General Support, EOGS) el 20 de agosto de 2018.
- **Se eliminó NSX Data Security:** En NSX 6.3.0, la función NSX Data Security se eliminó del producto.
- **La función Supervisión de actividad (Activity Monitoring, SAM) de NSX está obsoleta:** A partir de NSX 6.3.0, no se admite la función de Supervisión de actividad (Activity Monitoring) de NSX. En su lugar, utilice la función Supervisión de endpoints (Endpoint Monitoring). Para obtener más información, consulte [Supervisión de endpoints \(Endpoint Monitoring\)](#) en la *Guía de administración de NSX*.
- **Se eliminó la función Terminal de acceso web (Web Access Terminal):** La función Terminal de acceso web (Web Access Terminal, WAT) se ha eliminado de NSX 6.3.0. No puede configurar el acceso web de SSL VPN-Plus y habilitar el acceso de URL pública a través de NSX Edge. VMware recomienda utilizar el cliente con acceso completo con implementaciones de VPN SSL para mejorar la seguridad. Si está usando la funcionalidad WAT en una versión más reciente, debe deshabilitarla antes de actualizar a 6.3.0.
- **Se eliminó IS-IS de NSX Edge:** A partir de NSX 6.3.0, no puede configurar el protocolo IS-IS desde la pestaña Enrutamiento (Routing).
- **vCNS Edge ya no es compatible.** Debe actualizar a una instancia de NSX Edge antes de actualizar a NSX 6.3.x.

### Cambios en el comportamiento general

Si cuenta con más de un vSphere Distributed Switch y si VXLAN está configurado en uno de ellos, debe conectar las interfaces del enrutador lógico distribuido a los grupos de puerto de ese vSphere Distributed Switch. A partir de NSX 6.3.6, esta configuración se aplica en la interfaz de usuario y la API. En versiones anteriores, no se evitaba la creación de una configuración no válida.

# Eliminaciones de la API y cambios del comportamiento

## Cambios en el control de errores de API

NSX 6.3.5 introduce estos cambios en el control de errores:

- Si una solicitud de API da como resultado una excepción de base de datos en NSX Manager, la respuesta es *500 Error interno del servidor* (500 Internal server error). En versiones anteriores, NSX Manager respondía con *200 Correcto* (200 OK), aunque se produjera un error en la solicitud.
- Si envía una solicitud de API con el cuerpo vacío y se espera que este tenga contenido, la respuesta es *400 solicitud incorrecta* (400 Bad request). En versiones anteriores, NSX Manager respondía con *500 Error interno del servidor* (500 Internal server error).
- Si especifica un grupo de seguridad incorrecto en esta API, GET `/api/2.0/services/policy/securitygroup/{ID}/securitypolicies`, la respuesta es *404 No encontrado* (404 Not found). En versiones anteriores, NSX Manager respondía con *200 Correcto* (200 OK).

## Cambios en los valores predeterminados de las API de restablecimiento y de copia de seguridad

A partir de la versión 6.3.3, los valores predeterminados de los dos parámetros de restablecimiento y de copia de seguridad cambiaron para que coincidan con los valores predeterminados de la IU. Antes, el valor predeterminado de `passiveMode` y `useEPSV` era *falso* (false). Ahora, su valor es *verdadero* (true). Esto afecta a las siguientes API:

- PUT `/api/1.0/appliance-management/backupstore/backupsettings`
- PUT `/api/1.0/appliance-management/backupstore/backupsettings/ftpsettings`

## Eliminar la configuración del firewall o una sección predeterminada

- A partir de la versión 6.3.0, esta solicitud 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}`

## Parámetro `defaultOriginate`:

A partir de NSX 6.3.0, se eliminó el parámetro `defaultOriginate` de los siguientes métodos únicamente para los dispositivos NSX Edge del enrutador lógico (distribuido):

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

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

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

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

## Cambios de comportamiento y eliminaciones de la CLI

## No utilice comandos no admitidos en nodos de NSX Controller

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

# Notas sobre la actualización

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

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

## Notas generales sobre la actualización

- Para actualizar NSX, debe realizar una actualización completa de NSX, incluido el clúster del host (que actualiza los VIB del host). Para obtener instrucciones, acceda a la [Guía de actualización de NSX](#), donde se encuentra la sección sobre [cómo actualizar los clústeres del host](#).
- **Requisitos del sistema:** Si desea obtener información sobre los requisitos del sistema para la instalación y actualización de NSX, consulte la sección [Requisitos del sistema para NSX](#) de la documentación de NSX.
- **Ruta de acceso de actualización desde NSX 6.x:** La [matriz de interoperabilidad de productos VMware](#) proporciona los detalles sobre las rutas de acceso de actualización desde VMware NSX.
- Encontrará información sobre la actualización de Cross-vCenter NSX en la [Guía de actualización de NSX](#).
- **Las versiones anteriores no son compatibles:**
  - Realice siempre una copia de seguridad de NSX Manager antes de realizar una actualización.
  - Una vez que NSX se actualice correctamente, no podrá volver a utilizar una versión anterior.
- Para validar que su actualización a NSX 6.3.x se realizó correctamente, consulte el [artículo de la base de conocimientos 2134525](#).
- No existe compatibilidad para las actualizaciones de vCloud Networking and Security con NSX 6.3.x. En primer lugar, debe actualizar a una versión compatible con la versión 6.2.x.
- **Interoperabilidad:** Consulte la sección [Matriz de interoperabilidad de productos de VMware](#) para obtener información sobre todos los productos de VMware relevantes antes de actualizar.
  - **Actualizar a vSphere 6.5a o a una versión posterior:** Al actualizar de vSphere 5.5 o 6.0 a vSphere 6.5a o a una versión posterior, debe actualizar primero a NSX 6.3.x. Consulte [cómo actualizar vSphere en un entorno de NSX](#) en la [Guía de actualización de NSX](#).  
**Nota:** NSX 6.2.x no es compatible con vSphere 6.5.
  - **Actualizar a NSX 6.3.3 o una versión posterior:** La versión mínima admitida de vSphere para la interoperabilidad de NSX varía entre NSX 6.3.2 y NSX 6.3.3. Consulte la sección [Matriz de interoperabilidad de productos de VMware](#) para obtener más información.
- **Compatibilidad con servicios de partner:** Si su sitio web utiliza servicios de partners de VMware para Guest Introspection o para Network Introspection, consulte la [Guía de compatibilidad de VMware](#) antes de realizar la actualización para comprobar que el servicio del proveedor sea compatible con esta versión de NSX.
- **Complemento de Redes y seguridad:** Después de actualizar NSX Manager, debe cerrar sesión y volver a iniciarla en vSphere Web Client. Si el complemento de NSX no se muestra correctamente, borre el historial y la memoria caché del explorador. Si el complemento de Redes y seguridad no aparece en vSphere Web Client, restablezca el servidor de vSphere Web Client como se explica en la [Guía de actualización de NSX](#).

- **Entornos sin estado:** En las actualizaciones de NSX en un entorno de host sin estado, los VIB nuevos se agregan previamente al perfil de imagen del host durante el proceso de actualización de NSX. Como resultado, el proceso de actualización de NSX en hosts sin estado sigue esta secuencia: Antes de NSX 6.2.0, había una sola URL en NSX Manager a partir de la cual podían encontrarse los VIB para una versión determinada del host ESX. Esto significa que el administrador solo necesitaba conocer una sola URL, independientemente de la versión de NSX. En NSX 6.2.0 y posteriores, los VIB de NSX nuevos están disponibles en distintas URL. Para encontrar los VIB correctos, debe realizar los pasos siguientes:

1. Busque la URL de VIB nueva en `https://<NSXManager>/bin/vdn/nwfabric.properties`.
2. Obtenga los VIB de la versión de host ESX requerida desde la URL correspondiente.
3. Agréguelos al perfil de imagen del host.

## Notas sobre la actualización de los componentes de NSX

### Actualización de NSX Manager

- **Importante:** Si actualiza NSX 6.2.0, 6.2.1 o 6.2.2 a NSX 6.3.5 o una versión posterior, deberá completar una solución alternativa antes de iniciar la actualización. Consulte [el artículo 000051624 de la base de conocimientos de VMware](#) para obtener más detalles.
- Si utiliza SFTP para realizar copias de seguridad de NSX, cambie a `hmac-sha2-256` después de actualizar a 6.3.x, porque no se admite `hmac-sha1`. Consulte el [artículo 2149282 de la base de conocimientos de VMware](#) para obtener una lista de los algoritmos de seguridad que se admiten en 6.3.x.
- Si desea actualizar de NSX 6.3.3 a NSX 6.3.4 o a una versión posterior, primero debe seguir las instrucciones de solución alternativa del [artículo 2151719 de la base de conocimientos de VMware](#).
- Cuando actualiza NSX Manager a NSX 6.3.6 o una versión posterior, se realiza una copia de seguridad automáticamente y se guarda de forma local como parte del proceso de actualización. Para obtener más información, consulte [Actualizar NSX Manager](#).

### Actualización de Controller

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

Cuando se eliminan los controladores, también se eliminan las reglas de antiafinidad de DRS asociadas. Debe crear nuevas reglas antiafinidad en vCenter para evitar que las nuevas máquinas virtuales de controlador residan en el mismo host.

Para obtener más información sobre actualizaciones de los controladores, consulte [Actualizar el clúster de NSX Controller](#).

### Actualización del clúster del host

- En NSX 6.3.3, cambian los nombres de VIB de NSX. Los VIB `esx-vsip` y `esx-vxlan` se sustituyen por `esx-nsxv` si tiene NSX 6.3.3 o una versión posterior.

- **Desinstalación y actualización sin reinicio en los hosts:** A partir de vSphere 6.0, una vez que actualizó a NSX 6.3.x, no será necesario reiniciar después de realizar cambios en el VIB de NSX. En su lugar, los hosts deben entrar en modo de mantenimiento para completar el cambio de VIB.

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

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

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

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

Se necesita un reinicio del host durante las siguientes tareas:

- Las actualizaciones de NSX 6.2.x o versiones anteriores a NSX 6.3.x (cualquier versión de ESXi).
- Las actualizaciones de NSX 6.3.0 a NSX 6.3.x en ESXi 5.5.
- La instalación del VIB de NSX 6.3.x que se necesita después de actualizar ESXi 5.5 a 6.0 o versiones posteriores.
- La desinstalación del VIB de NSX 6.3.x en ESXi 5.5.

- **Es posible que el host se bloquee en el estado de instalación:** Durante actualizaciones grandes de NSX, es posible que un host se bloquee en el estado de instalación durante un periodo de tiempo prolongado. Esto puede ocurrir debido a problemas originados al desinstalar los VIB anteriores de NSX. En este caso, el subproceso EAM asociado a este host aparecerá como bloqueado en la lista de tareas del cliente VI.

*Solución alternativa:* Haga lo siguiente:

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

## Actualización de NSX Edge

- En NSX 6.3.0 cambiaron los tamaños del disco del dispositivo de NSX Edge:
  - **Compacto, grande, cuádruple:** 1 disco de 584 MB + 1 disco de 512 MB
  - **Extra grande:** 1 disco de 584 MB + 1 disco de 2 GB + 1 disco de 256 MB
- **Los clústeres del host deben estar preparados para NSX antes de actualizar los dispositivos de NSX Edge:** A partir de la versión 6.3.0, no se admite la comunicación en el plano de administración entre NSX Manager y Edge a través del canal VIX. Solo se admite el canal del bus de mensajería. Cuando actualiza de NSX 6.2.x o una versión anterior a NSX 6.3.0 o una versión posterior, debe verificar que los clústeres del host donde se implementan los dispositivos NSX Edge estén preparados para NSX y que el estado de la infraestructura de mensajería sea de color VERDE. Si los clústeres del host no están preparados para NSX, se producirá un error en la actualización del dispositivo de NSX Edge. Consulte [Actualizar NSX Edge](#) en la *Guía de actualización de NSX* para obtener más información.

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

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

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

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



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

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

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

PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>

para asegurarse de que los valores de `edgeVCpuReservationPercentage` y `edgeMemoryReservationPercentage` se encuentran dentro de los recursos disponibles para el factor de forma (consulte la tabla anterior para ver los valores predeterminados).

- Deshabilite la opción Iniciar máquina virtual (Virtual Machine Startup) de vSphere cuando vSphere HA está habilitado y los Edges están implementados. Tras actualizar NSX Edge 6.2.4 a la versión 6.2.5 u otras posteriores, debe desactivar la opción para iniciar la máquina virtual de vSphere en cada NSX Edge que se encuentre en un clúster en el que esté habilitado vSphere HA y en el que se hayan implementado Edges. Para ello, abra vSphere Web Client, busque el host ESXi donde se encuentra la máquina virtual de NSX Edge, haga clic en Administrar (Manage) > Configuración (Settings) y, en Máquinas virtuales (Virtual Machines), seleccione Inicio y apagado automático de la máquina virtual (VM Startup/Shutdown), haga clic en Editar (Edit) y asegúrese de que las máquinas virtuales estén en modo Manual (es decir, asegúrese de que no se añadiera a la lista de inicio/apagado automático).
- Antes de actualizar a NSX 6.2.5 o una versión posterior, asegúrese de que todas las listas de cifrados del equilibrador de carga estén separadas por dos puntos. Si su lista de cifrados utiliza otro separador, como, por ejemplo, comas, realice una llamada PUT a [https://nsxmgr\\_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles](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"
}
```

## Actualización de Guest Introspection

- Las máquinas virtuales de Guest Introspection ahora contienen información adicional para identificar los hosts en un archivo XML de la máquina. Al iniciar sesión en la máquina virtual de Guest Introspection, el archivo "/opt/vmware/etc/vami/ovfEnv.xml" debe incluir información para identificar los hosts.

## Notas sobre la actualización de FIPS

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

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

## Cumplimiento de FIPS

- NSS y OpenSwan: IPsec VPN de NSX Edge utiliza el módulo de cifrado de Mozilla NSS. Debido a problemas de seguridad críticos, esta versión de NSX utiliza una versión más reciente de NSS que no cuenta con la validación de FIPS 140-2. Aunque VMware afirma que el módulo funciona correctamente, ya no está validado formalmente.
- NSS y entrada de contraseña: El hash de contraseñas de NSX Edge utiliza el módulo de cifrado de Mozilla NSS. Debido a problemas de seguridad críticos, esta versión de NSX utiliza una versión más reciente de NSS que no cuenta con la validación de FIPS 140-2. Aunque VMware afirma que el

módulo funciona correctamente, ya no está validado formalmente.

- **Controller y VPN de agrupación en clústeres:** NSX Controller utiliza IPsec VPN para conectarse a los clústeres de Controller. IPsec VPN utiliza el módulo de cifrado del kernel de Linux para VMware (entorno Photon 1), que está en proceso de ser validado mediante CMVP.

## Historial de revisión del documento

15 de noviembre de 2018: Primera edición.

3 de marzo de 2019: Segunda edición. Se agregó el problema resuelto 2249307.

13 mayo 2019. Tercera edición. Se actualizó la sección Actualización del clúster del host.

## Problemas resueltos

Los problemas resueltos se agrupan del siguiente modo:

- [Problemas resueltos de NSX Edge y redes lógicas](#)
- [Problemas conocidos resueltos](#)
- [Problemas de NSX Controller resueltos](#)
- [Problemas de NSX Manager resueltos](#)
- [Problemas de instalación y actualización resueltos](#)
- [Problemas de servicios de seguridad resueltos](#)

### Problemas resueltos de NSX Edge y redes lógicas

- **Problema solucionado 2207483:** Latencia alta para el tráfico enrutado de norte a sur y de este a oeste  
El TxWorld de la máquina virtual que genera el tráfico enrutado utiliza el 100 % de la CPU, lo que resulta en una latencia alta.
- **Problema solucionado 2188666:** No se puede conectar a la puerta de enlace con un número de puerta de 5 dígitos usando la CLI SSLVPN cliente de Linux  
Tiene que usar la GUI SSLVPN cliente en Linux para conectarse a la puerta de enlace cuyo nombre tiene 5 dígitos, ya que esta funciona con la GUI, pero la CLI SSLVPN de Linux funciona con números de puertas que tengan hasta 4 dígitos.
- **Problema solucionado 2185457:** Aumento de la latencia de red para cargas de trabajo en puente  
Las cargas de trabajo con un tráfico (pps) elevado en redes en puente pueden causar latencia entre VLAN y VXLAN.
- **Problema solucionado 2182874:** No se puede identificar el ID de VDR si existen ID de VDR que se superpongan en los sitios  
El rango de segmentos de un sitio se debe cambiar si varios sitios tienen un rango de segmentos que se superpongan cuando intente agregar este sitio a multi-vc.
- **Problema solucionado 2181650:** Aceptar GARP como una respuesta válida al enviar la solicitud de ARP para actualizar la entrada de ARP  
Algunos dispositivos antiguos envían GARP como respuesta a la solicitud de ARP.
- **Problema solucionado 2181435:** En ESX 5.5, Hostd se bloquea durante el sondeo de las estadísticas  
En ESX 5.5, Hostd se bloquea durante el sondeo de las estadísticas. Hostd debe reiniciarse.
- **Problema solucionado 2179054:** No reinicie el controlador IXGBE durante la instalación y las actualizaciones de NSX  
Hay una interrupción de red de 5 a 10 segundos para los servicios del host.
- **Problema solucionado 2178950:** Se interrumpe el tráfico en más de dos máquinas virtuales de

### **vCenter en el mismo Edge cuando HA está habilitado**

Se detecta la interrupción de tráfico en más de dos máquinas virtuales de vCenter en el mismo Edge cuando HA está habilitado. La restauración que se hace al editar los dispositivos o al cambiar la ubicación de estos provoca que las máquinas virtuales estén en mal estado y causan una interrupción de red.

- **Problema solucionado 2177514:** En algunos casos, se devuelve el ping DaD, lo que provoca que el proceso DaD detecte direcciones IP duplicadas  
Los eventos del sistema notifican que se detectaron IP duplicadas falsas.
- **Problema solucionado 2176316:** El nombre de Edge no se actualiza en la regla del firewall  
Después de cambiar el nombre de Edge en la interfaz de usuario de Edge, la interfaz de usuario del firewall sigue mostrando el nombre anterior.
- **Problema solucionado 2172005:** La vecindad BGP oscila cuando se utiliza el comando "show ip bgp" de la CLI  
Cuando BGP detecta rutas con AS\_PATH superiores a 126 caracteres y se utiliza el comando "show ip bgp", la pila de enrutamientos se reinicia. La renovación de las rutas y el tráfico posible se interrumpen hasta que BGP vuelve a converger.
- **Problema solucionado 2171616:** El proceso cliente de Windows SSL VPN se bloquea cuando no se puede resolver el nombre del host de la ESG.  
Cuando el proxy HTTP está configurado y el nombre del host de la ESG no se puede resolver, se bloquea el proceso cliente.
- **Problema solucionado 2167176:** Los Edge de DLR que cuentan con la partición tmpfs con HA habilitado se completan  
El directorio /var/run (tmpfs) se rellena completamente cuando HA está habilitado. Si está completo, las configuraciones podrían no funcionar.
- **Problema solucionado 2164068:** La partición tmpfs de Edge se completa después de un tiempo cuando HA está habilitado  
Rsync se utiliza para sincronizar archivos entre máquinas virtuales de Edge en un par HA. Debido a la forma en la que rsync se compiló, cada invocación periódica de rsync generó mensajes de error de registro que se guardaron en un archivo de registro en la partición tmpfs. Después de un tiempo, la partición se podría completar, lo que afecta gravemente al funcionamiento normal de Edge.
- **Problema solucionado 2156094:** No se puede conectar a la puerta de enlace con un número de puerta de cinco dígitos usando la CLI SSL VPN cliente de Linux  
Tiene que usar la GUI SSL VPN cliente en Linux para conectarse a la puerta de enlace cuyo nombre tiene cinco dígitos, ya que esta funciona con la GUI, pero la CLI SSL VPN de Linux funciona con números de puertas que tienen hasta cuatro dígitos.
- **Problema solucionado 2152060:** El motor de servicio de supervisión (Nagios) en Edge tiene una pérdida de memoria  
El equilibrador de carga no funcionará bien si su configuración usa el servicio de supervisión sin memoria.
- **Problema solucionado 2140512:** Después de actualizar a 6.3.x o una versión posterior, las entradas TransportZone (vdscope) que faltan en la base de datos de MP provocan errores en VXLAN y en redes lógicas  
Aparecen errores en VXLAN y en redes lógicas en clústeres preparados para NSX.
- **Problema solucionado 2134760:** La instalación del cliente Mac SSL VPN se realiza correctamente, pero no puede ejecutar la aplicación  
El cliente no se abrirá aunque se instaló correctamente.
- **Problema solucionado 2100704:** NSX Edge puede perder conexiones VMCI a NSX Manager en algunos escenarios

Las instancias Edge no se pueden administrar, lo que impide que se publiquen configuraciones en los Edge.

- **Problema solucionado 2092516:** Varios trabajadores de supervisión actualizan el estado de los miembros del grupo al mismo tiempo  
El equilibrador de carga no funciona correctamente, envía tráfico lento al servidor en mal estado o el servidor en buen estado nunca tiene tráfico que gestionar.
- **Problema solucionado 2078866:** Al reiniciar el host, se produce un error `refreshHostdNetstackCache()` en `nsxv-vib`  
El rendimiento de VXLAN Rx se puede degradar.
- **Problema solucionado 2028337:** Los cinco procesos principales que consumen CPU no aparecen cuando el uso de CPU de Edge supera el 90 %  
Cuando el uso de CPU es superior al 90 %, se envía una notificación al administrador con una lista de los cinco procesos principales que consumen CPU desde que Edge se inició. Es muy probable que esta lista no muestre los cinco usuarios principales de CPU en ese instante, lo que dificulta la detección de problemas de uso de CPU.
- **Problema solucionado 1983497:** Aparece una pantalla de color púrpura cuando la conmutación por error del puente y la configuración de este cambian al mismo tiempo  
Cuando se cambian al mismo tiempo la conmutación por error y la configuración del puente, es posible que se produzca un interbloqueo y aparezca una pantalla de color púrpura. Las posibilidades de que se produzca un interbloqueo son bajas.
- **Problema solucionado 2181633:** Error de supresión de ARP en las direcciones IP de subinterfaz de máquinas virtuales invitadas  
La resolución de ARP de estas interfaces tarda un poco más de lo habitual (1 segundo) la primera vez.
- **Problema solucionado 2170329:** La configuración DNS no se puede aplicar en la interfaz cliente Windows SSLVPN  
Se produce un error en la consulta DNS que afecta al acceso.

#### Problemas conocidos resueltos

- **Problema solucionado 2183198:** La interfaz de usuario muestra un error al recuperar un puerto de un conmutador ToR que no tiene puerto  
Si un conmutador físico de una puerta de enlace de hardware no tiene ningún puerto, la interfaz de usuario de NSX devuelve un error al intentar obtener el puerto del conmutador. Aparece el error "No se puede recuperar la información del inventario" ("Unable to fetch inventory information") en la interfaz de usuario al intentar recuperar la información del puerto.
- **Problema solucionado 2176000:** La diferencia de codificación en los mensajes que envía el plano de administración y que espera el host resulta en nombres de puertos de vínculo superior no válidos de DVS, lo que provoca un error en la resolución de MAC  
DLR no puede resolver las direcciones Mac de las máquinas virtuales en los diferentes hosts ESXi.
- **Problema solucionado 2170413:** La API `/api/3.0/ai/directorygroup` no funciona  
El backend envía `NullPointerException` y se produce un error en la API. No se puede automatizar el flujo de trabajo.
- **Problema solucionado 2170395:** `domain_object` no está sincronizado con la tabla `ai_group`  
Cuando la página de Service Composer se carga, aparece `SQLGrammarException` debido a que SQL contiene una lista vacía de ID de grupo.
- **Problema solucionado 2131680:** Cuando coinciden con una regla de firewall de rechazo, los paquetes de multidifusión provocan un registro excesivo en `vmkernel`  
El registro excesivo en `vmkernel` causa que el host deje de realizar registros.

- **Problema solucionado 2129177:** Si la SVM de GI se elimina o se quita durante el proceso de actualización y con el modo de compatibilidad con versiones anteriores, el firewall de identidad a través de Guest Introspection (GI) no funcionará a menos que se actualice el clúster de GI. El firewall de identidad no funcionará y no se podrá ver ningún registro relacionado con el firewall de identidad. La protección del firewall de identidad se suspenderá a menos que se actualice el clúster.
- **Problema solucionado 2105632:** Las USVM intentan sincronizar la hora con servidores (externos) NTP de Google  
Se modificó el servicio de sincronización de hora para evitar este comportamiento.
- **Problema solucionado 2003396:** Las rutas y las LIF de DLR desaparecen tras reiniciar o en una nueva unión de hosts si existe un elevado número de rutas configuradas  
Las rutas no aparecen como configuradas.
- **Problema 1960383:** Error al crear la red debido al tiempo de espera cuando un número elevado de objetos del inventario se elimina en un breve espacio de tiempo  
Se produce el tiempo de espera en la creación de red debido a un retraso en la creación de dvpg en NSX.
- **Problema solucionado 2058770:** Se activaron demasiados eventos de inicio de sesión en vCenter y el servidor de SSO de vCenter sufre una gran carga  
El servidor de SSO de vCenter experimenta demasiados eventos de inicio de sesión y una gran carga cuando los usuarios de SSO de vCenter realizan muchas solicitudes de API de NSX en un breve espacio de tiempo. Esto puede dar lugar a un comportamiento lento.
- **Problema solucionado 2046427:** Cambiar la directiva de formación de equipos Vmknics o LS dvs portgroup puede provocar una interrupción de DP  
Durante la preparación del host (VXLAN), si el usuario establece la directiva de formación de equipos vmknics, la directiva de formación de equipos de vínculo ascendente en DVS se configura según corresponda. Los nuevos conmutadores lógicos dvs pg que se crean también reciben esta directiva de formación de equipos.
- **Problema solucionado 2178339:** rsyslog 8.15.0-7.ph1 eliminó la línea ExecReload en el archivo de servicio systemd, lo que provoca que /var/log/syslog y /var/log/messages no utilicen la propiedad logrotate correctamente  
Esto provoca que la partición /var/log ocupe el 100 % del espacio de disco, por lo que no se pueden escribir registros nuevos.
- **Problema solucionado 2146879:** En una configuración independiente, la sincronización forzada no sincroniza ToR ni los enlaces ToR  
En una configuración independiente, cuando la configuración de los enlaces de hardware o el nodo de transporte de hardware no están sincronizados entre el plano de administración y el controlador, la sincronización forzada no puede sincronizar la configuración. Las configuraciones ToR no se puede sincronizar con el controlador si los enlaces ToR no están sincronizados.
- **Problema solucionado 2146749:** El host ESXi pierde la configuración del ID local después del reinicio  
El host recibe el localeld erróneo y las rutas correspondientes se purgan.
- **Problema solucionado 2200396:** Las instancias de VDR se vuelven a crear en el host ESXi del sitio secundario tras una conmutación por error  
Se interrumpe el tráfico y la red durante alrededor de 40 segundos tras la conmutación por error.
- **Problema solucionado 2100296:** El complemento NSX 6.3.5 Web Client no muestra ningún NSX Manager tras deshabilitar SSL/TLS1.0 en los vCenter o PSC  
Al deshabilitar SSL/TLS1.0 en los vCenter, NSX interrumpe la comunicación con los vCenter, NSX o ESX. La aplicación vCenter no se comunicará con NSX Manager.
- **Problema solucionado 2077492:** NSX Manager crea automáticamente el ID de ipsecsite para

#### los sitios de ipsec que ya están presentes

- NSX Manager crea automáticamente el ID de ipsec para los sitios de ipsec que ya están presentes.
- La actualización de NSX for vSphere de 6.2.x a 6.3.5 o 6.4.0a puede introducir siteld duplicados para los sitios Ipsec.
- Una vez que se introducen los siteld duplicados, se produce un error en la siguiente configuración ipsec.
- Aparecerá un error similar al siguiente: [13646] [Ipsec] Se encontraron id ipsec del sitio Ipsec duplicados (Duplicate Ipsec site Ids ipsecsite-id found).
- **Problema solucionado 2177097:** Al usar la llamada de API /api/2.0/vdn/config/segments para crear un grupo con un ID de segmento, aparece el siguiente error "El id del segmento no se encuentra en el rango, el rango válido es 5000-16777215" ("Segment id is out of range, valid range is 5000-16777215").  
Cuando se utiliza la llamada de API /api/2.0/vdn/config/segments, si proporciona el mismo valor de inicio y de fin al crear un segmento de valor único, se produce un error.
- **Problema solucionado 2172267:** Eliminar NSX Edge durante la falta de respuesta del host provoca objetos huérfanos en vCenter  
La instancia de Edge en NSX Manager se elimina, pero el dispositivo Edge sigue apareciendo en vCenter Server y sirve como ruta de datos hasta que NSX Manager marca este Edge como huérfano y lo elimina en el proceso de limpieza. No es posible eliminar el dispositivo Edge de NSX Manager.
- **Problema solucionado 2097255:** Las capturas SNMP no se envían si FIPS está habilitado en el dispositivo NSX Manager  
No se reciben capturas SNMP.

#### Problemas de NSX Controller resueltos

- **Problema solucionado 2181306:** El controlador se queda sin memoria y no puede ofrecer el servicio con normalidad  
El controlador admite una interfaz ssh para solicitar el estado y la membresía del clúster. Si un cliente accede a este y no cierra las sesiones, el controlador mantiene las sesiones activas de forma indefinida. El controlador se queda sin memoria si existen bastantes sesiones activas.

#### Problemas de NSX Manager resueltos

- **Problema solucionado 2171653:** El análisis de seguridad de NSX Manager muestra lo siguiente: "No se detecta el encabezado de seguridad HTTP" ("HTTP Security Header Not Detected")  
El análisis de seguridad informa sobre este problema. Pueden producirse ataques de secuestros de clic de contadores.
- **Problema solucionado 2161066:** Se produce un error al conectar Usage Meter a NSX Manager o aparece un error de carácter XML no válido mientras se procesa una respuesta de API  
Al conectar Usage Meter a NSX Manager aparece un error.
- **Problema solucionado 2145195:** Alerta de latido para todas las USVM y el elevado uso de CPU en NSX Manager  
NSX Manager alerta que las USVM no respondieron al latido. La sesión postgres provoca un elevado uso de CPU.
- **Problema solucionado 2144825:** La partición raíz del administrador se llena debido a una gran cantidad de archivos nsx-tcserver-wrapper.log  
No se puede acceder a la interfaz de usuario de NSX y otros servicios dejan de funcionar debido a la falta de espacio.
- **Problema solucionado 2141490:** Los enlaces ToR en NSX Manager y los controladores no están sincronizados

No se puede modificar los enlaces de hardware de un conmutador lógico ni eliminar la configuración. La interfaz de usuario muestra el siguiente error: "No se pudo realizar la operación en el controlador. {0}"

- **Problema solucionado 2066631:** Aparece una ventana emergente con un mensaje de error al iniciar sesión con una función de usuario administrador y seleccionar una máquina virtual. Aparece el mensaje de error: "No tiene autoridad para acceder al objeto global y a la función library.tagging. Confirme la autoridad de la función y el ámbito de acceso del objeto" ("There is no authority to access object global and function library.tagging. Confirm the authority of the function and object access scope") como una ventana emergente.
- **Problema solucionado 2189810:** Las máquinas virtuales invitadas protegidas por PAN descartan el tráfico cuando una solución externa de inserción de servicios realiza una llamada de API a NSX Manager para recuperar todos los SecurityGroups/IPSets configurados como parte de la inserción de servicios.  
NSX Manager devuelve una configuración vacía para IPSets o SecurityGroups que contengan IPSets. Como resultado, IPSets o SecurityGroups con IPSets se envían vacíos al administrador externo. Las máquinas virtuales invitadas y protegidas por PAN u otros dispositivos firewall externos podrían descartar el tráfico, ya que ninguna regla coincide y la regla de denegación predeterminada de coincidencia. Al ejecutar la llamada de API [https://NSXMGR\\_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset](https://NSXMGR_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset), no se devuelve ninguna IP para IPSets o SecurityGroups que contienen IPSets.

Todas máquinas virtuales invitadas y protegidas por PAN u otros dispositivos firewall externos podrían descartar el tráfico, ya que ninguna regla coincide y la regla de denegación predeterminada de coincidencia.

- **Problema solucionado 2178700:** NSX Manager no puede sincronizar la información de LIF de VDR para controlar si alguna LIF de VDR consume un cable virtual eliminado.  
Se produce un error en las operaciones de LIF de VDR, lo que impide al usuario modificar la configuración de LIF.
- **Problema solucionado 2249307:** El identificador de configuración regional del host ESXi se restablece a su valor predeterminado cuando vuelve a conectarse a NSX Manager.  
Faltan rutas de DLR. DLR ya no enruta tráfico. El host recibe el identificador de configuración regional equivocado y no se conservan las rutas de DLR deseadas.

#### Problemas de instalación y actualización resueltos

- **Problema solucionado 2133143:** Entradas antiguas del clúster en la base de datos de NSX.  
Algunas entradas antiguas del clúster aparecen en la base de datos de NSX después de actualizar de 6.2.2 a 6.2.9.
- **Problema solucionado 2112773:** Error en la actualización del controlador.  
Se produce un error en un controlador durante la actualización de 6.2.4 a 6.3.6.

#### Problemas de servicios de seguridad resueltos

- **Problema solucionado 2098645:** Se produce una excepción de puntero nulo cuando el grupo de seguridad hace referencia al grupo de AD eliminado.  
Si se elimina un grupo de AD (ai\_group) y existe un grupo de seguridad con referencia al grupo de AD eliminado, Grupo de seguridad (SG)-> Traducción de máquina virtual (VM translation) mostrará una excepción de puntero nulo. La página de Service Composer no se carga correctamente.
- **Problemas solucionados 2032988, 2032990, 2032991:** Vulnerabilidad debido a CVE-2017-5753, CVE-2017-5715 (Specter) y CVE-2017-5754 (Meltdown).  
Puede haber problemas potenciales debido a las vulnerabilidades CVE-2017-5753, CVE-2017-5715 (Specter) y CVE-2017-5754 (Meltdown).



# Problemas conocidos

Los problemas conocidos se dividen del siguiente modo.

- [Problemas conocidos de instalación y actualización](#)
- [Problemas conocidos generales](#)

## Problemas conocidos de instalación y actualización

- **Problema 2001988:** Durante la actualización del clúster de hosts de NSX, el estado de Instalación (Installation) en la pestaña Preparación del host (Host Preparation) alterna entre "no está listo" ("not ready") e "instalando" ("installing") para todo el clúster cuando se está actualizando cada uno de los hosts del clúster

Durante la actualización de NSX, al hacer clic en "actualización disponible" ("upgrade available") para el clúster preparado de NSX, se activa la actualización del host. Para los clústeres configurados con la opción DRS AUTOMÁTICO COMPLETO (DRS FULL AUTOMATIC), el estado de instalación alterna entre "instalando" ("installing") y "no está listo" ("not ready"), aunque los hosts se actualicen en segundo plano sin problemas.

Solución alternativa: Se trata de un problema de la interfaz de usuario y se puede ignorar. Espere a que se actualice el clúster de hosts para continuar.

## Problemas conocidos generales

- **Problema 2158182:** El servicio DHCP y HA con IP de vínculo local que comparten la misma vNIC provoca que se descarte el paquete de renovación DHCP

Si la dirección de HA es de vínculo local (169.x.x.x), el DR puede descartar los paquetes de unidifusión de renovación de DHCP a esta dirección de vínculo local, que puede provocar un error en la renovación del cliente DHCP.

Solución alternativa: Seleccione una vNIC sin servicio DHCP como interfaz de HA o use una dirección IP enrutable como IP de la interfaz de HA, por ejemplo: 192.168.x.x.

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

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

Solución alternativa:

1. Inicie sesión en el dispositivo virtual NSX Manager.
  2. En Administración de dispositivos (Appliance Management), haga clic en Administrar configuración de dispositivos (Manage Appliance Settings).
  3. En el panel Configuración (Settings), haga clic en Red (Network).
  4. Haga clic en Editar (Edit) junto a Servidores DNS (DNS Servers).
  5. En el campo Buscar dominios (Search Domains), reemplace todos los caracteres de espacios en blanco por comas.
  6. Haga clic en Aceptar (OK) para guardar los cambios.
- **Problema 1849042/1849043:** Se bloquea la cuenta del administrador después de configurar la caducidad de la contraseña en el dispositivo NSX Edge

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

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

- **Problema 2204383:** Se produce un error en el cliente Linux SSLVPN al verificar el certificado del servidor para versiones de Linux que usen `sql cert9.db`  
Se produce un error interno en la validación del servidor.

Solución alternativa: Ninguna.