

# Notas de la versión de VMware NSX-T Data Center 2.4

VMware NSX-T Data Center 2.4 | 28 de febrero de 2019 | Compilación 12456646

Compruebe regularmente las adiciones y actualizaciones relativas a estas notas de la versión.

## Contenido de las notas de la versión

Las notas de la versión contienen los siguientes temas:

- [Novedades](#)
- [Compatibilidad y requisitos del sistema](#)
- [Recursos de CLI y API](#)
- [Historial de revisión](#)
- [Problemas resueltos](#)
- [Problemas conocidos](#)

## Novedades

NSX-T Data Center 2.4 ofrece diversas funciones nuevas para proporcionar nuevas funcionalidades de redes virtualizadas y seguridad para nubes híbridas, públicas y privadas. Entre los puntos más destacados se encuentran una nueva interfaz de usuario de redes basada en intenciones; un firewall con reconocimiento de contexto; funciones de introspección de red y de invitado; IPv6; una administración en clúster de alta disponibilidad; una instalación de NSX basada en perfiles para clústeres de proceso de vSphere; un modo de actualización de mantenimiento sin necesidad de reinicio de recursos informáticos de NSX for vSphere; un nuevo modo de actualización local de recursos informáticos de vSphere, y un coordinador de migración para la migración desde NSX Data Center for vSphere hasta NSX-T Data Center.

Las nuevas funciones y las mejoras de funciones siguientes están disponibles en NSX-T Data Center 2.4.

### Clúster de administración

NSX-T Data Center 2.4 ahora permite crear un clúster de instancias de Manager para garantizar la alta disponibilidad de la interfaz de usuario y la API. Dicho agrupamiento en clústeres admite tanto equilibradores externos con fines de redundancia y distribución de cargas, como IP virtuales proporcionadas mediante NSX con fines de redundancia. Además, las funciones de plano de administración y plano de control central se consolidaron en este nuevo clúster de administración para reducir el número de dispositivos virtuales que deben implementarse y gestionarse mediante la administración de NSX. El dispositivo de NSX Manager está disponible en tres tamaños diferentes para distintos escenarios de implementación: un dispositivo pequeño para implementaciones de prueba de concepto y laboratorio; un dispositivo mediano para implementaciones en 64 hosts, y un dispositivo grande para clientes que realicen implementaciones en un entorno de gran escala. Para obtener información detallada sobre los valores máximos de configuración, consulte la herramienta de valores máximos de configuración de VMware en: <https://configmax.vmware.com>

### Soporte del diseño de clúster único

Admite diseños de clúster único con las máquinas virtuales de Edge, administración y equipo contraídas, todo alimentado con un N-VDS único en un host físico único. Los diseños de referencia típicos de los clientes de SP VCF prescriben PNIC de 4x10G con dos conmutadores de host; uno para máquinas virtuales de Edge y administración, y otro para máquinas virtuales de equipo. Esto aísla de forma efectiva la comunicación entre la máquina virtual de Edge y la máquina virtual de equipo para que el tráfico salga del host y vuelva a él. Sin embargo, con la economía de tendencia de las NIC de 25G, los clientes de SP de VCF se están estandarizando en los hosts de NIC de 2x25G y, con este diseño, podrán moverse a un único N-VDS que alimenta un host con 2 pNICs. En este diseño, la máquina virtual de Edge y la máquina virtual de equipo que pertenecen a la misma subred pueden comunicarse sin que el tráfico tenga que salir de los vínculos superiores del host y volver a ellos.

## Directiva e interfaz de usuario

### Automatización y administración de NSX

- **Administración de directivas declarativas:** simplifique y automatice las configuraciones de redes y seguridad mediante instrucciones de directivas basadas en resultados. Para reducir el número de pasos de configuración, esta nueva API de directivas declarativas permite a los usuarios describir los objetivos que persiguen y, al mismo tiempo, deja que el sistema determine cuál es la mejor forma de alcanzarlos. Defina toda la topología de una red e impleméntela al mismo tiempo y de forma prescriptiva e independiente del orden.

### Mejoras de la interfaz de usuario

- **Diseños de página y navegación mejorados:** los diseños de las páginas y la barra de navegación se mejoraron para reducir el número de clics necesarios para acceder a información crítica.
- **Internacionalización:** mejor tratamiento de los elementos específicos de una configuración regional, como el formato de fecha y hora, el formato de número o la zona horaria.

**Nota:** La función Visualización de topología de la red para NSX Policy Manager, introducida en la versión 2.3, está obsoleta en esta versión.

## Firewall

El firewall distribuido y los firewalls de puerta de enlace admitirán el filtrado del tráfico IPv6 proveniente de NSX-T Data Center 2.4. Además, se incorporaron las siguientes funciones operativas al producto:

### Botón de publicación y reversión

Un único botón de publicación está disponible en toda la tabla de firewalls. Se ofrecerá tanto en el caso del firewall distribuido como en el caso del firewall de puerta de enlace. Antes de NSX-T Data Center 2.4, había un botón de publicación por cada sección. Este botón estará disponible a través de la API. Adicionalmente, tendrá la opción de revertir los cambios. Tendrá también la opción de bloquear secciones tras actualizar los cambios.

### Estadísticas de regla

Cada regla tendrá el recuento de aciertos, el recuento de paquetes, el recuento de sesiones, el recuento de bytes y el índice de popularidad. De igual modo, contará con la comparación entre los recuentos de aciertos actuales y los valores máximos mostrados. Estas estadísticas se pueden restablecer con un botón.

### Mejoras en los agrupamientos

Hay disponibles más criterios de agrupamiento según el sistema operativo para los grupos de Active Directory y de máquinas virtuales.

### Visibilidad de reglas por máquina virtual

Puede consultar la lista de reglas de firewall de una máquina virtual en concreto en el puerto de conmutador lógico asociado a cada máquina virtual.

## **Detección de IP para máquinas virtuales**

El perfil de detección de IP predeterminado se está actualizando para incluir la detección de IP basada en VMware Tools, además de la intromisión de ARP y la intromisión de DHCP. Los clientes existentes que realicen una actualización a partir de versiones anteriores deberán actualizar el perfil de detección de IP para habilitar la detección basada en VMware Tools. Asimismo, NSX-T 2.4 admite la creación de un perfil de detección de IP global. Se realizaron también los siguientes cambios:

1. Se ofrece la detección de IP de IPv6 basada en DHCPv6 y mecanismos de detección de vecinos.
2. La detección de IPv6 está deshabilitada de forma predeterminada.
3. Los enlaces de IP detectados de forma automática se pueden colocar manualmente en la lista blanca o en la lista de omitidos.
4. Las direcciones IPv4 de vínculo local se omitirán de forma predeterminada.

## **Firewall de identidad**

NSX-T Data Center 2.4 introduce reglas basadas en identidad (identificador de usuario) para el firewall distribuido. Los administradores de firewall ahora pueden configurar reglas distribuidas en máquinas virtuales con base en grupos definidos a partir de Active Directory. Gracias a esta función, los administradores de firewall pueden proporcionar reglas de firewall basadas en los usuarios que iniciaron sesión en las máquinas virtuales. NSX detectará automáticamente los usuarios que iniciaron o cerraron sesión, y se habilitarán las reglas específicas en función de esos usuarios. El firewall basado en identidad es capaz de detectar y aplicar reglas para un único usuario por máquina virtual o incluso realizar un seguimiento de varios usuarios con sesiones particulares en la misma máquina virtual. Los administradores de firewall crearán grupos de NSX-T utilizando como criterio los grupos de Active Directory. NSX-T Manager recuperará automáticamente una lista de grupos de Active Directory de los controladores de dominio provistos. Los administradores de firewall pueden controlar el acceso de este a oeste de los usuarios, especialmente en entornos de escritorio virtual o en sesiones de escritorio remoto en los que se habilitaron los servicios de terminal.

## **Firmas de aplicación de Capa 7 para firewall distribuido con reconocimiento de contexto**

NSX-T Data Center 2.4 permite usar firmas de aplicación basadas en Capa 7 en las reglas de firewall distribuido. Los usuarios pueden utilizar una combinación de reglas de Capa 3 o Capa 4 con las firmas de aplicación de Capa 7, o bien crear únicamente reglas basadas en firmas de aplicaciones de Capa 7. Actualmente solo se admiten firmas de aplicación con varios atributos secundarios para las comunicaciones entre servidores o entre clientes y servidores. En NSX-T Data Center 2.4, esto estará disponible exclusivamente para los nodos de transporte basados en ESXi.

## **Adición de FQDN/URL a la lista blanca para firewall distribuido con reconocimiento de contexto**

NSX-T Data Center 2.4 incluye reglas basadas en la adición a listas blancas de FQDN/URL en el firewall distribuido. NSX-T Data Center presenta una innovación que hace uso de la intromisión de DNS distribuida para permitir que cada conexión procedente de cada máquina virtual tenga su propia resolución de FQDN/URL. Los administradores de firewall pueden utilizar dominios de URL predefinidos y aplicarlos a las reglas de un firewall distribuido. Las aplicaciones de naturaleza híbrida que accedan a servicios SaaS o a servicios basados en la nube pueden microsegmentar en función de las direcciones URL a las que se accedieron. El acceso de los exploradores o las aplicaciones cliente que acceden a las aplicaciones SaaS se puede conceder de forma granular. En NSX-T Data Center 2.4, esto estará disponible exclusivamente para los nodos de transporte basados en ESXi.

## **Inserción de servicios**

NSX-T Data Center 2.4 presenta una amplia gama de funcionalidades de seguridad nativas (como la identidad de aplicaciones de Capa 7, las listas blancas de FQDN y el firewall de identidad) que permiten una microsegmentación aún más granular. Además de los controles de seguridad nativos que el firewall distribuido y el firewall de puerta de enlace proporcionan, el marco de inserción de servicios de NSX permite que diversos tipos de servicios de partners (como soluciones de supervisión de red, IDS/IPS y NGFW) se puedan insertar de forma transparente en la ruta de datos y que se puedan consumir desde NSX sin tener que cambiar la topología.

En NSX-T Data Center 2.4, la inserción de servicios ahora admite el tráfico de este a oeste (es decir, el tráfico entre las máquinas virtuales del centro de datos). Todo el tráfico entre las máquinas virtuales en el centro de datos se puede redirigir a una cadena dinámica de servicios de partners.

El plano de servicio de este a oeste proporciona su propio mecanismo de reenvío que permite el redireccionamiento basado en directivas del tráfico en cadenas de servicios. La plataforma automatiza por completo el reenvío en el plano de servicio: se detectan errores y los flujos nuevos/existentes se redirigen según corresponda; los flujos se anclan para brindar soporte a servicios con estado, y hay varias directivas de selección de rutas de acceso disponibles para optimizar el rendimiento, la latencia o la densidad.

## Guest Introspection

NSX-T Data Center 2.4 incluye la plataforma de servicios de Guest Introspection para partners de VMware con el fin de proporcionar capacidades de descarga antivirus y antimalware sin agente basadas en directivas para las cargas de trabajo de máquinas virtuales invitadas basadas en Windows en hipervisores de vSphere ESXi.

En NSX-T Data Center 2.4, la plataforma de Guest Introspection proporciona lo siguiente:

- Una implementación y una administración del ciclo de vida simplificadas mediante la consolidación de la implementación de Guest Introspection en la instalación de preparación del host del agente NSX, y la eliminación del requisito que obligaba a implementar la máquina virtual del servicio universal de Guest Introspection en cada hipervisor de ESXi.
- Servicios coherentes basados en directivas en varias instancias de vCenter.
- Mejoras en la escala de partners de VMware a través del dimensionamiento de máquinas virtuales de servicio (Service Virtual Machine, SVM) del partner (es decir, dispositivos de partner "pequeños", "medianos" o "grandes").

## Redes de Capa 2

### Varias instancias de N-VDS por host

Además de proporcionar flexibilidad para organizar el tráfico de las máquinas virtuales, esta nueva capacidad (que permite admitir varias instancias de N-VDS por host) facilita el cumplimiento de la norma de PCI, la cual exige un aislamiento estricto del tráfico de máquinas virtuales.

Gracias a la inclusión de esta función, ahora los enlaces ascendentes de ENS se pueden distinguir de los que no son de ENS. Esta funcionalidad resulta útil porque ENS actualmente carece de paridad de funciones con N-VDS, por lo que las cargas de trabajo con tecnología ENS obtendrán un método rápido, pero pocas funciones.

### Visualización de N-VDS

Esta funcionalidad proporciona la capacidad de administrar la instancia de N-VDS como un objeto independiente, con la posibilidad de explorar en profundidad para ver los hosts conectados, etc. Al consultar un host específico, se verá una cuadrícula de interfaz de usuario que indica cómo está conectado a la instancia de N-VDS. Las interfaces lógicas (como las interfaces de kernel de máquina virtual) también estarán visibles como parte de la instancia de N-VDS. Esto supone una mejora considerable con respecto a la vista de host, y muestra en una misma vista una lista de interfaces en la que figuran todas las NIC físicas, las interfaces de kernel de máquina virtual y todos los puertos de OVS.

## Compatibilidad con LLDP en NIC físicas

Esta función acaba con las diferencias a la hora de implementar LLDP para NSX. Así, proporciona capacidad de depuración en la conectividad del conmutador físico. La posibilidad de descifrar qué puertos físicos están conectados a qué interfaces en un host contribuye a solucionar fácilmente problemas de cableado. El ámbito de esta función se aplica a todos los hosts físicos (ESXi, KVM, hosts de Linux nativos y Edge nativo) que participan en el plano de datos de NSX.

## Compatibilidad con el proxy de ARP en el nodo de Edge

Cuando los clientes externos acceden a servicios como el equilibrador de carga, IKE, etc. con las mismas direcciones de subred, se activa el enrutamiento de dispositivos. Envían consultas de ARP relativas a esas direcciones enlazadas a puertos de bucle invertido, pero los puertos de bucle invertido del enrutador lógico carecen de direcciones MAC, por lo que no responden a esas consultas de ARP. Esto provoca problemas de acceso.

Actualmente, la solución alternativa consiste en configurar un enrutamiento de tipo /32 en esos clientes (como IP bucle invertido/32 → enlace ascendente/CSP), de forma que el tráfico se pueda reenviar a puertos de enlace ascendente/CSP y, a continuación, dirigirse al puerto de bucle invertido correcto. El proxy de ARP es la solución correcta para acabar con este inconveniente.

## Redes de Capa 3

### Mejoras en la configuración de MTU

NSX-T 2.4 ofrece dos nuevos parámetros globales de unidad de transmisión máxima (Maximum Transmission Unit, MTU):

- MTU de vínculo superior físico global, que configura el valor de MTU de todas las instancias de N-VDS en el dominio de NSX. Esto se puede describir como el tamaño de trama máximo de las tramas encapsuladas GENEVE o MTU de TEP.
  - El MTU de perfil de enlace ascendente puede reemplazar el parámetro de enlace ascendente físico en un host específico.
- MTU de interfaz lógica global, que configura el valor de MTU de todas las interfaces de enrutador lógico.
  - El MTU de enlace ascendente de enrutador lógico y el MTU del puerto CSP pueden reemplazar el MTU de interfaz lógica global en un puerto concreto si es necesario.

Esto permite que puedan establecerse comunicaciones de extremo a extremo en máquinas virtuales configuradas con un valor de MTU superior a 1.500 bytes en el tráfico de este a oeste y de norte a sur.

### Enrutamiento Inter-SR

Ahora, los enrutadores lógicos de nivel 0 en modo activo/activo pueden establecer automáticamente intercambios de tráfico iBGP de malla completa entre todos los enrutadores de servicio (Service Router, SR) que formen parte de un determinado enrutador lógico de nivel 0. Esto evita que se produzcan caídas en el tráfico en caso de que haya SR configurados con varios enlaces ascendentes y se produzca un error en solo uno de ellos. Un SR en este escenario de error ahora reenviará el tráfico a otro SR si el destino no está disponible en sus propios enlaces ascendentes.

### Mejoras en el reenviador de DNS

- Ahora, la función de reenviador de DNS se puede habilitar o deshabilitar sin que se pierda su configuración actual.
- Esta función muestra también estadísticas, eventos y alarmas a través de la API y la interfaz de usuario.

### Compatibilidad con SNAT entre enlaces ascendentes

NSX-T 2.4 incluye compatibilidad con la traducción de direcciones de red de origen (Source Network Address Translation, SNAT) en situaciones en las que el tráfico entra en un enrutador lógico de nivel 0 a través de un enlace ascendente y sale de ese mismo enrutador lógico a través de otro enlace ascendente. Esta función resulta útil cuando hay varios enrutadores lógicos de nivel 0 conectados entre sí.

### Compatibilidad con el proxy de ARP en el enrutador lógico de nivel 0

NSX-T 2.4 incluye compatibilidad con el proxy de ARP en los enlaces ascendentes de enrutador lógico de nivel 0. Esto permite implementar NSX-T en entornos donde el enrutamiento no se puede configurar en los enrutadores en sentido norte del enrutador lógico de nivel 0. Con esta función se puede configurar NAT, el equilibrador de carga o cualquier otro servicio con estado que tenga una dirección IP que pertenezca a la red del enlace ascendente de nivel 0.

### Mejoras del nodo de Edge

- NSX-T 2.4 incorpora la opción de nodo de Edge sin sistema operativo para admitir la administración en las NIC de método rápido, con lo cual se puede prescindir de una NIC de administración dedicada.
- El nodo de Edge sin sistema operativo también admite NIC de Intel XXV710 de 25 Gbps.
- El nodo de Edge admite varios endpoints de túnel (Tunnel EndPoint, TEP) de GENEVE. Gracias a ello, los nodos de Edge no se ven forzados a usar grupos de adición de vínculos (Link Aggregation Groups, LAG) con fines de alta disponibilidad en el tráfico de superposición.

### Mejoras de BGP

- A partir de NSX-T 2.4, los enrutadores lógicos de nivel 0 admiten el intercambio de tráfico iBGP con enrutadores físicos en sentido norte.
- NSX-T 2.4 incluye una opción para habilitar ECMP entre elementos eBGP del mismo nivel situados en ASN distintos (comando as-path multipath-relax) y, asimismo, admite el enrutador lógico de nivel 0 para que su propio ASN pueda usarse en el comando as-path (allowas-in).

## IPv6

NSX-T 2.4 incorpora seguridad y funciones de reenvío/enrutamiento IPv6. Esto incluye compatibilidad con lo siguiente:

- Rutas estáticas IPv6
- Detección de vecinos IPv6
- Retransmisiones DHCPv6
- Firewall distribuido (Distributed Firewall, DFW) IPv6
- Firewall de Edge IPv6
- Familia de direcciones IPv6 para MP-BGP y comandos prefix-list/route-map asociados
- Seguridad de conmutadores IPv6
- Detección de direcciones IPv6
- Herramientas de opciones IPv6

## Operaciones

### Mejoras de Traceflow

Traceflow amplía la compatibilidad a más capacidades de visualización y solución de problemas. En NSX-T 2.4, Traceflow proporciona observaciones sobre servicios centralizados como el firewall de Edge, el equilibrador de carga, NAT y las redes privadas virtuales (Virtual Private Networks, VPN) basadas en rutas.

### Mejoras de instalación

- NSX permite realizar implementaciones más sencillas mediante una nueva instalación basada en perfiles de componentes de NSX de clústeres de informáticos de vSphere. Esta función hace

posible unas implementaciones más rápidas, logra una configuración coherente, evita los errores manuales y facilita un método por el cual "se define una vez y se reutiliza varias veces".

- Posibilidad de realizar una instalación y agrupamiento automatizados de nodos de NSX Manager desde la interfaz de usuario.
- Compatibilidad con más configuraciones de implementación que permiten crear varios conmutadores de N-VDS y migrar puertos de VMKernel y adaptadores físicos a través de perfiles.

## Mejoras de actualización

- Se incluyeron mejoras para ofrecer actualizaciones de hosts ESXi totalmente organizadas sin incurrir en el coste derivado de reiniciar el host mediante la actualización de NSX de modo de mantenimiento predeterminada.
- Se incluye un nuevo modo de actualización de NSX llamado actualización "local". Esta función ayuda a simplificar las operaciones y hace que las actualizaciones sean más rápidas. Si este modo se utiliza, los componentes de NSX en los hosts ESXi se actualizan sin que haya que apagar cargas de trabajo ni migrarlas a otro hipervisor.
- Se introdujo un nuevo marco y se proporcionaron pruebas inmediatas para realizar comprobaciones previas y posteriores durante la actualización de NSX, que pueden servir para revelar problemas subyacentes latentes antes de comenzar la actualización de facto o inmediatamente después de esta.

## Copia de seguridad de NSX en la detección de cambios

NSX mejora su solución de recuperación ante desastres, ya que ofrece la posibilidad de detectar cambios de configuración y hacer copias de estos de forma proactiva para guardarlos de un modo seguro. Esta función permite a los clientes tener mejores SLA relativos a las copias de seguridad de configuraciones, todo ello sin incurrir en el coste derivado de hacer copias de seguridad de archivos innecesarios en el servidor de almacenamiento.

## NFV

Ahora, el conmutador de N-VDS admitirá las siguientes mejoras en el modo de ruta de datos mejorada (Enhanced Data Path, EDP).

- Firewall distribuido
- Detección de IP
- Spoofguard
- IPFIX
- IPv6
- Mejor rendimiento de la máquina virtual de Edge, que ahora logra un rendimiento hasta cinco veces mayor en el modo EDP.
- Redundancia de las rutas de acceso en aplicaciones de hosts múltiples. La posibilidad de fijar una máquina virtual en un enlace ascendente específico permite crear actualmente una ruta de acceso redundante de hosts múltiples en NSX con endpoints de túnel virtual (Virtual Tunnel Endpoints, VTEP).

## Operaciones: AAA/RBAC y seguridad de la plataforma

### Operaciones

- **Mejoras en la identidad de entidades de seguridad:** los usuarios de identidad de entidades de seguridad pueden registrar e instalar componentes de NSX. Se agregó compatibilidad de interfaz de usuario para crear usuarios de identidad de entidades de seguridad y asignar funciones.
- **Mejoras en la directiva de contraseña:** se obliga a usar contraseñas predeterminadas con una longitud mínima de 12 caracteres. Se contempla la posibilidad de establecer fechas de caducidad de la contraseña y se emiten alarmas cuando la contraseña está a punto de caducar. De forma predeterminada, las contraseñas caducan a los 90 días. Consulte el artículo [70691](#) de la base de conocimientos para obtener instrucciones sobre cómo restablecer contraseñas y ajustar su caducidad.

- **Administración de certificados:** se incluye la posibilidad comprobar el estado de revocación de un certificado.

## VPN

NSX-T 2.4 agregó las siguientes capacidades relativas a los servicios de VPN:

- Hay disponibles una GUI y una API de directivas para los servicios de VPN tanto de Capa 3 como de Capa 2.
- Los servicios de VPN de Capa 3 admiten la autenticación basada en certificados, lo que mejora la administración de la seguridad.
- El modo de cliente de VPN de Capa 2 está disponible para dar cabida a la extensión de Capa 2 de NSX-T SDDC a NSX-T SDDC.
- Los grupos de Diffie-Hellman (DH) 19, 20 y 21 están disponibles para satisfacer los requisitos de alta seguridad.

## Equilibrio de carga

NSX-T 2.4 agregó las siguientes capacidades relativas a los servicios de equilibrio de carga:

- Hay disponibles una API de directivas y una nueva GUI. La GUI de equilibrador de carga anterior sigue estando disponible en la pestaña Redes y seguridad avanzadas.
- Las VIP de un SR independiente pueden pertenecer a la misma subred que el puerto de servicio centralizado (Centralized Service Port, CSP). Antes de esta versión, si se quería crear a una VIP en la misma subred que la red del CSP, había que usar la dirección IP del CSP como VIP. De lo contrario, había que crear a una VIP en otra red.
- El firewall de Edge y DNAT se admiten en los flujos de tráfico del equilibrador de carga en la misma puerta de enlace de nivel 1. Antes de esta versión, los flujos de tráfico del equilibrador de carga pasaban por alto el firewall de Edge.
- Las reglas de equilibrador de carga admiten encabezados HTTP que empiecen por "\_". Con esta mejora, el equilibrador de carga de NSX se puede implementar para vIDM y AirWatch.
- Se puede utilizar una VIP como dirección IP de origen de la SNAT de equilibrador de carga.
- El tamaño máximo del encabezado de respuesta HTTP se puede establecer en hasta 64 KB. El tamaño predeterminado seguirá siendo el mismo que el de la versión anterior (4 KB).
- Una máquina virtual de Edge grande admite una instancia del equilibrador de carga grande. Antes de esta versión, las máquinas virtuales de Edge grandes admitían como máximo una instancia del equilibrador de carga mediana.

## Migración de NSX Data Center for vSphere a NSX-T Data Center

Ahora, NSX-T 2.4 cuenta con un coordinador de migración que puede ser de ayuda al migrar de NSX Data Center for vSphere a NSX-T Data Center. Esta función está pensada para migrar los hosts existentes prescindiendo de vMotion. El coordinador de migración admite la migración de redes de Capa 2, redes de Capa 3, firewall, equilibrio de carga y VPN. En la *Guía del coordinador de migración de NSX-T Data Center* encontrará más detalles sobre la herramienta.

No es necesario que haya recursos informáticos adicionales aparte de simplemente la implementación de las instancias de NSX-T Manager y los nodos de Edge. Una vez completada la migración, un cliente puede desinstalar NSX for vSphere, así como las instancias de Manager y Controller y los nodos de Edge asociados correspondientes. Tenga en cuenta que esta migración repercute en el tráfico del plano de datos y está diseñada para completarse en un mismo periodo de cambio.

## Automatización, OpenStack y otras CMP

NSX-T 2.4 ofrece las siguientes capacidades para poder usar OpenStack a través de su complemento de Neutron:

- Compatibilidad con Rocky y Queens



- Posibilidad de agrupamiento en clúster del plano de administración  
El complemento OpenStack Neutron utiliza esta nueva capacidad para tener un clúster de instancias de Manager. Así, puede consumir los extremos de API de REST de las tres instancias de Manager sin necesidad de una VIP externa para lograr un rendimiento y una disponibilidad mayores.
- Compatibilidad con Barbican  
Ahora, el complemento OpenStack Neutron admite Barbican. Barbican es una API de REST pensada para el almacenamiento seguro, el aprovisionamiento y la administración de información confidencial como contraseñas, claves de cifrado y certificados X.509. Esto permite administrar un certificado del equilibrador de carga como servicio para la terminación HTTPS. En la actualidad, esta función se admite únicamente en entornos de E/S virtual (Virtual Input/Output, VIO).

El proveedor de Terraform de NSX-T agrega las siguientes capacidades a las ya existentes en NSX-T 2.4 (creación de conmutadores lógicos, enrutadores, reglas de firewall, etc.):

- Capacidad para admitir CRAE en el equilibrador de carga y en la configuración del equilibrador de carga (supervisión, grupos, etc.).
- Capacidad para admitir CRAE en los servidores DHCP.
- Capacidad para admitir CRAE en la IPAM de NSX-T (bloque de direcciones IP, grupo de direcciones IP).

## NSX Cloud

NSX-T 2.4 para NSX Cloud tiene muchas características nuevas que facilitan la adopción/implementación por parte de un cliente y proporcionan más opciones relativas a cómo un cliente puede realizar una inserción de servicios o una terminación de VPN, administrar sus entornos de infraestructura de escritorios virtuales (Virtual Desktop Infrastructure, VDI) y, en definitiva, administrar una auténtica implementación híbrida con varias regiones y varias nubes.

Estas son algunas de las funciones principales de NSX Cloud con NSX-T 2.4:

- Puerta de enlace compartida en el canal de puerto o red virtual (VPC/VNET) de tránsito para una incorporación y consolidación más rápidas y sencillas
- VPN para el tráfico de retroceso que vuelve al controlador de dominio (Domain Controller, DC) local
- Integración de partners e inserción de servicios de norte a sur selectivas
- Microsegmentación en Horizon Cloud para Azure
- Directiva basada en finalidad para cargas de trabajo híbridas

**Arquitectura de VPC/VNET de tránsito simplificada:** A partir de la versión 2.4, los clientes pueden instalar una sola puerta de enlace de NSX Cloud en una VPC o VNET de tránsito y administrar hasta 10 VPC/VNET de equipo. Esto simplifica la arquitectura de tránsito hub y radio/equipo, y permite el enrutamiento transitivo entre las VPC de equipo, incluso cuando no tienen una conexión de emparejamiento. Con el túnel superpuesto de NSX, el tráfico entre las VPC ahora se puede enviar en un túnel de superposición. Las directivas de redireccionamiento se pueden configurar en el nivel de las máquinas virtuales para determinar si el tráfico debe encapsularse y enviarse en la superposición, o bien si debe enviarse en la red subyacente del proveedor de nube pública. Todas estas características ofrecen más flexibilidad a los usuarios para enrutar el tráfico dentro y fuera de su red de nube pública.

**VPN para el tráfico de retroceso:** ahora, NSX Cloud dispone de compatibilidad integrada para tener túneles de VPN para el tráfico de retroceso desde la nube pública a un centro de datos local. Ahora, las VPN del centro de datos local pueden terminar directamente en la puerta de enlace de NSX Cloud en la nube pública. Los clientes no necesitan la puerta de enlace virtual (Virtual Gateway, VGW) proporcionada por proveedores de nube pública y esto reduce el coste. También se reducen los gastos de administración, dado que la puerta de enlace de NSX Cloud propaga automáticamente las rutas a través de BGP. NSX Cloud constituye una enorme mejora también en la capacidad de ancho de banda: los flujos de tráfico entre VPC pueden llegar hasta los 5 Gbps a través de VPC del mismo nivel, en comparación con el apenas 1 Gbps que se alcanza a través de una VGW.

**Integración de partners e inserción de servicios de norte a sur selectivas:** los clientes pueden implementar un servicio de partners directamente desde el catálogo de nube pública en la arquitectura de servicios compartidos/tránsito. La puerta de enlace de NSX Cloud presente en la instancia de VPC/VNET de tránsito se puede programar para que el tráfico se enrute de forma selectiva al dispositivo de servicio de partners, dependiendo de las directivas de NSX. Esto puede suponer un enorme ahorro económico para un cliente, ya que no se verá obligado a dirigir todo el tráfico a través de un dispositivo de firewall de Capa 7 virtual que haya adquirido para la nube pública, y que se cobra en función del tráfico que lo atraviese. Y, por si esto fuera poco, la inserción de servicios con NSX Cloud no requiere que una VPN calcule el número de VPC/VNET. El ahorro económico es mayor y se necesitarán menos operaciones.

**Microsegmentación en Horizon Cloud para Azure:** ahora, NSX Cloud tiene una solución combinada con Horizon Cloud para Azure. NSX Cloud proporcionará la microsegmentación necesaria y protegerá el entorno de VDI de aquellos clientes que decidan tener un entorno de VDI de Horizon implementado en Azure.

**Directiva basada en finalidad para cargas de trabajo híbridas:** Cloud Service Manager (CSM) ahora está integrado con NSX Manager. Los clientes podrán definir una única directiva basada en finalidad en Policy Manager sin tener que preocuparse de dónde se van a implementar las cargas de trabajo o a dónde se trasladarán en un futuro. NSX Cloud aplicará esta directiva de manera uniforme en el controlador de dominio local, Azure y AWS.

## Compatibilidad y requisitos del sistema

Para obtener información sobre los requisitos de sistema y compatibilidad, consulte la [Guía de instalación de NSX-T Data Center](#).

## Recursos de CLI y API

Consulte [code.vmware.com](https://code.vmware.com) para usar las API o las CLI de NSX-T Data Center para la automatización.

La documentación de la API está disponible en la pestaña **Referencia de la API**. La documentación de la CLI está disponible en la pestaña **Documentación**.

## Historial de revisión del documento

28 de febrero de 2019. Primera edición.

2 de abril de 2019. Segunda edición. Se agregaron los siguientes problemas conocidos: 2273651, 2279326, 2281095 y 2296888. Se agregó el problema solucionado: 2199785.

10 de abril de 2019. Tercera edición. Se agregaron los siguientes problemas conocidos: 2203863, 2248186, 2252738, 2277543, 2276398, 2279326, 2281537, 2287124, 2290688, 2294178, 2295592, 2296430, 2297157, 2297918 y 2298499. Se actualizó la sección Novedades para incluir la compatibilidad con el diseño de clúster único.

20 de junio de 2019. Cuarta edición. Se agregó el problema conocido 2261818. Se agregó el problema solucionado 2182745.

23 de agosto de 2019. Quinta edición. Se agregaron los problemas conocidos 2362688, 2395334 y 2392093.

## Problemas resueltos

- Problema solucionado 1842511: No se admiten los saltos entre redes BGP en las rutas estáticas

En la versión 2.0 de NSX-T, se puede habilitar el protocolo de detección de envío bidireccional (BFD) para un vecino de salto entre redes BGP (MH-BGP). No se puede configurar la capacidad de respaldar una ruta estática de salto entre redes con BFD en NSX-T 2.0. Esto solo es posible con BGP. Tenga en cuenta que, si configura un vecino de salto entre redes BGP respaldado por un BFD y, además, configura la ruta estática de salto entre redes correspondiente con el mismo salto siguiente que el vecino BGP, el estado de la sesión BFD afecta tanto a la sesión BGP como a la ruta estática.

- **Problema solucionado 2279326:** No se muestra ningún error al crear un recopilador de IPFIX L2 con más de 4 combinaciones IP:PUERTO.

No se muestra ningún mensaje de error para el número máximo permitido de combinaciones IP:puerto. No se produce ningún daño, ya que la interfaz de usuario restringe la creación de etiquetas si se supera el límite máximo.

- **Problema solucionado 1931707:** La función de nodo de transporte requiere que todos los host del clúster tengan la misma configuración de PNIC

Cuando se habilita la función de nodo de transporte automático para un clúster, se crea una plantilla de nodo de transporte para aplicarla a todos los hosts del clúster. Todas las PNIC de la plantilla deben estar libres en todos los host de configuración del nodo de transporte. Si no es así, es posible que se produzca un error en la configuración de los hosts cuyas PNIC falten o estén ocupadas.

- **Problema solucionado 1909703:** El administrador de NSX puede crear nuevas rutas estáticas, reglas NAT y puertos en un enrutador creado por OpenStack directamente desde el servidor backend

Como parte de la función RBAC de NSX-T 2.0, el administrador de NSX no puede eliminar ni modificar recursos, tales como interruptores, enrutadores o grupos de seguridad creados por el complemento OpenStack directamente desde la API o la interfaz de usuario de NSX. Dichos recursos solo pueden modificarse o eliminarse desde las API enviadas a través del componente OpenStack. Esta función tiene una limitación. Actualmente, lo único que no puede hacer el administrador de NSX es eliminar o modificar los recursos creados por OpenStack. Sin embargo, sí puede crear nuevos recursos, como rutas estáticas o reglas NAT, en los recursos creados por OpenStack.

- **Problema solucionado 1989407:** Los usuarios de vIDM con la función de administrador empresarial no pueden reemplazar la protección del objeto

Un usuario de vIDM con la función de administrador empresarial no puede reemplazar la protección del objeto y no puede crear ni eliminar identidades de entidades de seguridad.

- **Problema solucionado 2030784:** No se puede iniciar sesión en NSX Manager con un nombre de usuario remoto que contiene caracteres que no son ASCII

No se puede iniciar sesión en el dispositivo de NSX Manager como un usuario remoto cuyo nombre de usuario contiene caracteres que no son ASCII.

- **Problema solucionado 2111047:** Application Discovery no es compatible en hosts de VMware vSphere 6.7 en NSX-T 2.2

Al ejecutar Application Discovery en un grupo de seguridad en el que se ejecutan máquinas virtuales en un host de vSphere 6.7, se produce un error en la sesión de detección.

- **Problema solucionado 2157370:** Al configurar el analizador de puerto conmutado (Switched Port Analyzer, SPAN) de Capa 3 con truncamiento, el conmutador físico específico descarta los paquetes reflejados

Al configurar el intervalo de SPAN de Capa 3 que incluye GRE/ERSPAN con truncamiento, se descartan los paquetes reflejados truncados debido a la directiva de conmutador físico. Una causa puede ser que el puerto está recibiendo paquetes donde la cantidad de bytes en la carga útil no es igual al campo de longitud de escritura.

- **Problema solucionado 2174583:** En el asistente de primeros pasos, el botón Configurar nodos de transporte no funciona correctamente en el explorador Microsoft Edge

En el asistente de primeros pasos, después de hacer clic en el botón Configurar nodos de transporte, el explorador web de Microsoft Edge presenta un error de JavaScript.

- **Problema solucionado 2114756:** En algunos casos, los VIB no se quitan cuando se quita un host del clúster preparado de NSX-T  
Cuando se quita un host del clúster preparado de NSX-T, es posible que algunos VIB permanezcan en el host.
- **Problema solucionado 2059414:** Se produce un error en la instalación del paquete de LCP de RHEL debido a una versión anterior del RPM python-gevent  
Si un host RHEL contiene una versión más reciente de python-gevent RPM, la instalación del paquete de LCP de RHEL presenta un error porque el RPM de NSX-T Data Center contiene una versión anterior del RPM python-gevent.
- **Problema solucionado 2142755:** Los módulos kernel OVS no se pueden instalar en función de qué versión de RHEL 7.4 menor se está ejecutando  
Los módulos kernel OVS no se pueden instalar en un host RHEL 7.4 que ejecuta una versión 17.1 de kernel o superior menor. El error de instalación hace que las rutas de acceso de datos kernel dejen de funcionar, lo que da lugar a que la consola de administración del dispositivo no esté disponible.
- **Problema solucionado 2125725:** Después de restaurar implementaciones de topología de gran tamaño, los datos de búsqueda se desincronizan y varias páginas de NSX Manager dejan de responder  
Después de restaurar NSX Manager con implementaciones de topología de gran tamaño, los datos de búsqueda se desincronizan y varias páginas de NSX Manager muestran el mensaje de error "Se produjo un error irrecuperable".
- **Problema solucionado 2187888:** La instancia de NSX Edge implementada automáticamente desde la interfaz de usuario de NSX Manager permanece en el estado Registro pendiente de manera indefinida  
La instancia de NSX Edge implementada automáticamente desde la interfaz de usuario de NSX Manager permanece en el estado Registro pendiente de manera indefinida. Este estado hace que la instancia de NSX Edge deje de estar disponible para una configuración adicional.
- **Problema solucionado 2077145:** Intentar forzar la eliminación del nodo de transporte en algunos casos puede provocar nodos de transporte huérfanos  
Al intentar forzar la eliminación del nodo de transporte mediante una llamada API en la que, por ejemplo, hay un error de hardware y los hosts se vuelven irrecuperables, el estado del nodo de transporte cambia a huérfano.
- **Problema solucionado 2099530:** Se interrumpe el tráfico al cambiar la dirección IP de VTEP del nodo de puente  
Cuando se cambia la dirección IP de VTEP del nodo de puente, la tabla de MAC de VLAN a la superposición no se actualiza en los hipervisores remotos, lo que provoca una interrupción del tráfico de hasta 10 minutos.
- **Problema solucionado 2106176:** La instalación automática de NSX Controller se detiene durante el paso de instalación Esperando el registro  
Durante la instalación automática de instancias de NSX Controller mediante la API o la interfaz de usuario de NSX Manager, el estado de una de las instancias de NSX Controller en curso se detiene y se muestra de manera indefinida como Esperando el registro.
- **Problema solucionado 2125514:** Después de la conmutación por error del puente de capa 2, es posible que el conmutador lógico en algunas máquinas virtuales de NSX Edge haga una replicación de BUM de cada uno de los paquetes hasta que se vuelva a conocer la MAC  
Después de la conmutación por error del puente de capa 2, es posible que el conmutador lógico en algunas máquinas virtuales de NSX Edge haga una replicación de BUM de cada uno de los paquetes durante casi 10 minutos hasta que se vuelva a conocer la MAC del endpoint. El sistema se recupera a sí mismo después de que los endpoints generen la siguiente instancia de ARP.

- **Problema solucionado 2183549:** Cuando se edita un puerto de servicio centralizado, no se puede ver un conmutador lógico de VLAN recién creado  
En la interfaz de usuario de Manager, después de crear un puerto de servicio centralizado y un nuevo conmutador lógico de VLAN, si edita el puerto de servicio centralizado, no puede ver el conmutador lógico de VLAN recién creado.
- **Problema solucionado 2186040:** Si un nodo de transporte no está entre los 250 perfiles de vínculo superior principales en el sistema, se deshabilita el menú desplegable de vínculo superior de las NIC físicas en la interfaz de usuario  
Si un nodo de transporte no está entre los 250 perfiles de vínculo superior principales en el sistema, se deshabilita el menú desplegable de vínculo superior de las NIC físicas en la interfaz de usuario. Al guardar los resultados de los nodos de transporte se elimina el nombre del vínculo superior del nodo de transporte.
- **Problemas solucionados 2106635:** Durante la creación de rutas estáticas, el cambio de la distancia administrativa de las rutas NULL hace que la configuración NULL de salto siguiente desaparezca de la interfaz de usuario  
Durante la creación de rutas estáticas, cuando se establece el próximo salto en NULL y se cambia la distancia administrativa de las rutas NULL, la configuración de salto siguiente NULL desaparece de la interfaz de usuario.
- **Problema solucionado 1928376:** El estado del nodo miembro del clúster del controlador se degradó tras restaurar NSX Manager  
Es posible que el nodo miembro del clúster del controlador se vuelva inestable y presente un estado degradado si NSX Manager se restaura en la imagen de la copia de seguridad que se creó antes de que este nodo se separara del clúster.
- **Problema solucionado 2128361:** El comando de la CLI para establecer el nivel de registro de NSX Manager en el modo de depuración no funciona correctamente  
Al utilizar el comando de la CLI `set service manager logging-level debug` para establecer el nivel de registro de NSX Manager como modo de depuración, no se recopila la información del registro de depuración.
- **Problema solucionado 1940046:** Cuando se agrega la misma ruta estática y se anuncia en varios enrutadores lógicos de nivel 1, se produce un error en el tráfico de este a oeste  
Si se agrega la misma ruta estática y se anuncia en varios enrutadores lógicos de nivel 1, se produce un error en el tráfico de este a oeste.
- **Problema solucionado 2160634:** Cambiar la dirección IP en un bucle invertido puede cambiar la dirección IP del identificador del enrutador en un vínculo superior  
Si se cambia la dirección IP en el bucle invertido, el NSX Edge selecciona la dirección IP en el vínculo superior como el identificador de enrutador. La dirección IP del vínculo superior que se asigna como identificador del enrutador no se puede cambiar.
- **Problema solucionado 2199785:** Se observa el núcleo de NGINX al agregar un monitor de estado (sin número de puerto) al grupo dinámico (con número de puerto)  
Cuando se configura el equilibrio de carga con miembros dinámicos del grupo de servidores (con el número de puerto) y, a continuación, se intenta asociar un monitor de estado que no tiene ningún puerto de supervisión configurado, es posible que nginx se bloquee.
- **Problema solucionado 2182745:** Antes, los modificadores `le/ge` de las reglas de redistribución no se validaban en el administrador y no funcionaban correctamente  
Las reglas de redistribución admiten `le/ge` en instancias de `prefixlist`.

## Problemas conocidos

Los problemas conocidos se dividen del siguiente modo.

- Problemas conocidos generales
- Problemas conocidos de instalación
- Problemas conocidos de NSX Manager
- Problemas conocidos de NSX Edge
- Problemas conocidos de las redes lógicas
- Problemas conocidos de los servicios de seguridad
- Problemas conocidos de las redes de KVM
- Problemas conocidos del equilibrador de carga
- Problemas conocidos de interoperabilidad de soluciones
- Problemas conocidos de las operaciones y los servicios de supervisión
- Problemas conocidos de actualización
- Problemas conocidos de la API
- Problemas conocidos de NSX Policy Manager
- Problemas conocidos de NSX Cloud

## Problemas conocidos generales

- **Problema 2239365: Se produce un error "No autorizado"**

Este error puede producirse debido a que el usuario intenta abrir varias sesiones de autenticación en el mismo tipo de explorador. Como resultado, aparecerá este error de inicio de sesión y el usuario no podrá autenticarse. Ubicación de registro: `/var/log/proxy/reverse-proxy.log`  
`/var/log/syslog`

Solución alternativa: Cerrar todas las ventanas/pestañas de autenticación e intentar autenticarse de nuevo.

- **Problema 2287482: La tabla de enlaces detectados automáticamente puede incluir enlaces no detectados actualmente**

Puede que los enlaces señalados como duplicados en la tabla de enlaces detectados automáticamente ya no se detecten.

Solución alternativa: Ninguna.

- **Problema 2278142: El perfil global de IPFIX del conmutador no es editable**

Si hay perfiles globales disponibles en el sistema, no se pueden modificar ni eliminar a través de la interfaz, ya que no existe ningún flujo de trabajo relativo a perfiles globales.

Solución alternativa: Elimine el perfil global mediante la API.

- **Problema 2292222: En la pantalla Resolver error, no se avisa al usuario de que la huella digital es incorrecta**

Si se produce un error en una operación de preparación del host, el usuario puede solucionar este problema haciendo clic en el error de instalación de NSX, en cuyo caso será necesario proporcionar un nombre de usuario, una contraseña y la huella digital del host. Si el usuario proporciona una huella digital incorrecta, los sistemas no le avisarán y el problema seguirá sin estar resuelto.

No hay ninguna forma clara de saber que la huella digital no es correcta. Consulte el registro donde se reflejó la excepción `ThumbPrintValidationFailedException`.

Solución alternativa: Proporcione la huella digital adecuada.

- **Problema 2252487: No se guarda el estado del nodo de transporte de Edge sin sistema operativo si se agregan varios nodos de transporte en paralelo**

El estado del nodo de transporte no se muestra correctamente en la interfaz de usuario del plano de administración.

Solución alternativa:

1. Reinicie Proton. El estado de todos los nodos de transporte se puede actualizar correctamente.

2. También puede recurrir a la API <https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime> para consultar el estado del nodo de transporte.

- **Problema 2285117: No se puede actualizar el kernel de las máquinas virtuales administradas con NSX**

En algunas imágenes del catálogo de Linux Ubuntu, el kernel se actualiza a sí mismo automáticamente al reiniciar la máquina virtual. Debido a ello, el agente NSX no funciona según lo esperado. A pesar de que el agente NSX parece funcionar, habrá algunas directivas de redes que no se apliquen, lo que afecta al agente NSX. El agente reintentará aplicar estas directivas una y otra vez, lo que provoca un uso elevado de la CPU.

Solución alternativa: Si es necesario actualizar el kernel, primero deberá descargar los encabezados de Linux correspondientes a ese kernel más reciente y volver a compilar el paquete `openvswitch-datapath-dkms`.

- **Problema 2285544: Ya no se admiten hashes MD5 al invocar las API de NSX que requieren que se especifique un valor de `ssh_fingerprint`**

NSX-T 2.4 dejó de admitir algoritmos de cifrado que no sean FIPS, hashes, etc., lo que engloba invocar las API de NSX de copia de seguridad/restauración, de almacén de archivos y de paquete de soporte, y especificar un hash MD5 como valor de `ssh_fingerprint`. Como resultado, ya no se pueden usar hashes MD5.

Solución alternativa: Especifique otro hash calculado mediante otro algoritmo hash (por ejemplo, SHA256).

- **Problema 2256709: Una máquina virtual de clon instantáneo o máquina virtual revertida a partir una instantánea pierde la protección antivirus brevemente durante vMotion**

La instantánea de una máquina virtual se revierte y migra la máquina virtual a otro host. La consola de partners no muestra ninguna protección antivirus en la máquina virtual de clon instantáneo migrada. Hay una breve pérdida de protección antivirus.

Solución alternativa: Ninguna.

- **Problema 2261431: Se requiere una lista filtrada de almacenes de datos en función del resto de parámetros de implementación**

Se muestra el correspondiente error en la interfaz de usuario si se seleccionó la opción incorrecta. Un cliente puede eliminar esta implementación y crear otra para recuperarse del error.

Solución alternativa: Si va a crear una implementación agrupada en clúster, seleccione un almacén de datos compartido.

- **Problema 2266553: En el dispositivo de NSX, un servicio puede no inicializarse al arrancar por primera vez**

El nodo implementado no puede procesar solicitudes o no puede formar un clúster.

Solución alternativa: Pruebe a reiniciar el servicio con el error.

- **Problema 2267632: Pérdida de la configuración de protección de Guest Introspection**

La regla de protección de invitados publicada en la interfaz de usuario de la directiva muestra un estado correcto. El cambio correspondiente en el comportamiento no se refleja en la máquina virtual invitada. Al mismo tiempo, los registros de `opsAgent` indican que se reinicie. Pérdida de protección de máquina virtual invitada.

Solución alternativa: Reproduzca el cambio de configuración manualmente.

- **Problema 2269901: La interfaz de VMK no se incluye en la CLI de captura de paquetes**  
Este comando no se puede emitir.

Solución alternativa: Utilice `pktcap-uw` para llevar a cabo lo mismo.

- **Problema 2274988: Las cadenas de servicio no admiten perfiles de servicio consecutivos**

#### **procedentes del mismo servicio**

El tráfico no atraviesa una cadena de servicio y se descarta cuando la cadena tiene dos perfiles de servicio consecutivos que pertenecen al mismo servicio.

Solución alternativa: Agregue un perfil de servicio procedente de otro servicio para asegurarse de que no haya dos perfiles de servicio consecutivos pertenecientes al mismo servicio. También puede definir un tercer perfil de servicio para que realice las mismas operaciones que los dos perfiles originales concatenados y, de este modo, utilizar ese tercer perfil solo en la cadena de servicio.

- **Problema 2275285:** Un nodo realiza una segunda solicitud para unir un mismo clúster antes de que finalice la primera solicitud y de que el clúster sea estable

El clúster puede no funcionar correctamente y los comandos de la CLI para obtener el estado del clúster y la configuración del clúster podrían devolver un error.

Solución alternativa: No emita ningún comando de unión nueva para unir el mismo clúster durante los 10 minutos siguientes a la primera solicitud de unión.

- **Problema 2275388:** Las rutas de interfaz de bucle invertido/interfaz conectada podrían redistribuirse antes de que se agreguen filtros para denegar rutas

Las actualizaciones de rutas innecesarias podrían provocar que el tráfico se desvíe entre unos segundos y un minuto.

Solución alternativa: Ninguna.

- **Problema 2275708:** No se puede importar un certificado con su correspondiente clave privada cuando la clave privada tiene una frase de contraseña

El mensaje devuelto es "Se recibieron datos PEM no válidos para el certificado. (Código de error: 2002)". No se puede importar un nuevo certificado con una clave privada.

Solución alternativa:

1. Cree un certificado con una clave privada. Cuando se le solicite, no introduzca una nueva frase de contraseña. En su lugar, presione Entrar.
2. Seleccione "Importar certificado" y seleccione el archivo de certificado y el archivo de clave privada.

Abra el archivo de clave para comprobarlo. Si se introdujo una frase de contraseña al generar la clave, la segunda línea del archivo mostrará algo parecido a "Proc-Type: 4,ENCRYPTED".

Esta línea no estará si se generó el archivo de clave sin frase de contraseña.

- **Problema 2275985:** Las vNIC no conectadas a un conmutador lógico se muestran como opciones de miembros directos de grupos NSGroup

Una vNIC que no está conectada a un conmutador lógico se agrega como miembro directo del grupo NSGroup. La operación se realiza correctamente, pero las directivas aplicadas a ese grupo no se cumplen en la vNIC.

Solución alternativa: Ninguna.

Compruebe si la vNIC en cuestión está conectada a un conmutador lógico antes de agregarla como miembro directo de un grupo NSGroup.

- **Problema 2277742:** La invocación de PUT `https://<MGR_IP>/api/v1/configs/management` con un cuerpo de solicitud que establece `publish_fqdns` en `true` puede producir un error si el dispositivo de NSX-T Manager está configurado con un nombre de dominio completo (Fully Qualified Domain Name, FQDN) en lugar de con un nombre de host

PUT `https://<MGR_IP>/api/v1/configs/management` no se puede invocar si hay un FQDN configurado.

Solución alternativa: Implemente la instancia de NSX Manager con un nombre de host en lugar de con un FQDN.



- **Problema 2279249:** La máquina virtual de clon instantáneo pierde la protección antivirus brevemente durante vMotion  
Se migró una máquina virtual de clon instantáneo de un host a otro. Inmediatamente después de la migración, el archivo eicar se deja detrás de la máquina virtual. Breve pérdida de protección antivirus.

Solución alternativa: Ninguna.

- **Problema 2290669:** A medida que el número de servidores virtuales aumenta, también lo hace el tiempo de configuración de cada uno  
A medida que el número de servidores virtuales aumenta, también lo hace el tiempo de configuración de cada uno de ellos, dada la gran cantidad de validaciones. En los primeros 100 servidores virtuales, el tiempo medio de respuesta es de alrededor de 1 segundo. Tras los primeros 250 servidores virtuales, el tiempo medio de respuesta aumenta entre 5 y 10 segundos. Tras los primeros 450 servidores virtuales, el tiempo medio de respuesta aumenta unos 30 segundos.

Solución alternativa: Ninguna. Dependiendo de la topología, puede que sea posible configurar servidores virtuales como varios servicios de equilibrador de carga; si no es así, prevea unos tiempos de respuesta más lentos al definir configuraciones a gran escala con servidores virtuales.

- **Problema 2292116:** La Capa 2 de IPFIX aplicada a un grupo de direcciones IP basado en el enrutamiento de interdominios sin clases (Classless Interdomain Routing, CIDR) no aparece en la interfaz de usuario cuando un grupo se crea a través de la página de Capa 2 de IPFIX  
Si intenta crear un grupo de direcciones IP en el cuadro de diálogo "Se aplica a" e introduce una dirección IP o un CIDR incorrectos en el cuadro de diálogo "Establecer miembros", dichos miembros no figurarán entre los grupos. Deberá volver a editar ese grupo para introducir direcciones IP válidas.

Solución alternativa: Vaya a la página donde se enumeran los grupos y agregue direcciones IP en ese grupo. De este modo, dicho grupo podrá empezar a rellenarse en el cuadro de diálogo "Se aplica a".

- **Problema 2294821:** Aparece información del dispositivo de NSX en el panel de control de supervisión del clúster con el error "No se pudo eliminar el nodo" sin ninguna instrucción para el usuario sobre cómo procesar la situación  
Este problema se observa después de que el usuario intenta eliminar el nodo de implementación automática mediante la interfaz y se produce un error en el apagado del nodo. Si el clúster pierde un nodo, deberá agregar un nuevo nodo manualmente y borrar los estados de configuración mediante la siguiente solución alternativa.

Solución alternativa: Tras el error de eliminación del dispositivo a través de la API/interfaz de usuario, elimine ese dispositivo manualmente mediante la API para forzar la eliminación. Así:

```
POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?
action=delete&force_delete=true
```

A continuación destruya la máquina virtual de la instancia de vCenter.

- **Problema 2281095:** Cuando se vuelve a agregar al mismo clúster un host en el que se implementó la SVM, no se activa la devolución de llamada desde EAM  
Todas las máquinas virtuales invitadas podrían estar desprotegidas. La interfaz de usuario de NSX no se saldrá del estado en curso.

Solución alternativa: Quite la SVM del host y, a continuación, agréguela al clúster.

- **Problema 1957072:** El perfil de vínculo superior para el nodo de puente siempre debe usar LAG para más de un vínculo superior  
Al utilizar varios vínculos superiores que no se incluyen en un LAG, no se equilibra la carga del tráfico y es posible que este no funcione correctamente.

Solución alternativa: Utilice LAG para varios vínculos superiores en nodos de puente.

- **Problema 1970750:** El perfil N-VDS de nodo de transporte que utiliza LACP con temporizadores rápidos no se aplica a hosts vSphere ESXi  
Cuando se configura un perfil de enlace ascendente de LACP con velocidades rápidas y se aplica a un nodo de transporte de vSphere ESXi en NSX Manager, NSX Manager muestra que el perfil se aplica correctamente, pero el host vSphere ESXi utiliza el temporizador lento predeterminado de LACP. En el hipervisor de vSphere, no puede ver el efecto del valor de lacp-timeout (Lento/Rápido [SLOW/FAST]) cuando el perfil de conmutador distribuido administrado por NSX (N-VDS) de LACP se utiliza en el nodo de transporte desde NSX Manager.

Solución alternativa: Ninguna.

- **Problema 2261818:** Las rutas obtenidas del vecino eBGP se anuncian al mismo vecino  
Al habilitar los registros de depuración de BGP, se indicarán los paquetes que se reciben y los que se descartan con un mensaje de error. El proceso BGP consumirá recursos de CPU adicionales al descartar los mensajes de actualización enviados a los pares. Si hay un número elevado de rutas y pares, eso puede afectar la convergencia de las rutas.

Solución alternativa: Ninguna.

### Problemas conocidos de instalación

- **Problema 2238093:** Solución inviable si los paquetes de NSX se eliminaron de manera forzada  
Para desinstalar NSX del host, los paquetes de NSX se eliminan de manera forzada. Esto puede dañar los paquetes de NSX. La solución para instalar paquetes de NSX puede no funcionar correctamente si, antes de aplicarla, los paquetes de NSX se eliminaron de manera forzada.  
Ubicación de registro: `/var/log/proton/nsxapi.log`

Solución alternativa: Ninguna.

No elimine paquetes de NSX de manera forzada. Desinstale los componentes de NSX mediante los procedimientos habituales descritos en la documentación de NSX.

- **Problema 2288872:** El estado de la instalación indica que el nodo no está listo  
El nodo de Edge no se incorpora. El estado de configuración del nodo de transporte es Pendiente, y como tal no se podrá agregar a un clúster de Edge. Ubicación de registro:  
`/var/log/proton/nsxapi.log`

Solución alternativa: Intente registrar el nodo de Edge de nuevo. Opcionalmente, apague el nodo de Edge. Cuando se inicie, establecerá el canal MP-MPA.

- **Problema 2252776:** Un perfil de nodo de transporte no se puede aplicar en uno de los hosts miembro del clúster, aun cuando el error de validación que se produjo anteriormente en el host ya está resuelto  
El perfil de nodo de transporte se aplica en el clúster. No obstante, el perfil de nodo de transporte no se puede aplicar en uno de los hosts miembros del clúster debido a que alguna de las validaciones no se superó (p. ej., hay máquinas virtuales encendidas en el host). El usuario resuelve el problema, pero el error de validación sigue apareciendo en la interfaz de usuario y el perfil de nodo de transporte no se aplica automáticamente al host en cuestión.

Solución alternativa: Saque el host del clúster y vuelva a agregarlo. Esto activará la actividad para aplicar un perfil de nodo de transporte al host.

- **Problema 2284683:** No se puede eliminar un dispositivo implementado automáticamente cuando un administrador de equipo registrado se elimina y se vuelve a agregar  
Al eliminar un dispositivo, se produce el error "Error al apagar" y se informa de que no se puede encontrar el administrador de equipo.

Solución alternativa: Tras el error de eliminación del dispositivo a través de la API/interfaz de usuario, elimine ese dispositivo manualmente mediante la API para forzar la eliminación. Así: `POST api/v1/cluster/nodes/deployments/<node-id>?action=delete&force_delete=true`. Destruya la máquina virtual de la instancia de vCenter

- **Problema 1957059: Se produce un error al deshacer la preparación de un host si este se agregó con vibs al clúster**

Si no se eliminan completamente los vibs antes de agregar los hosts al clúster, se produce un error en la operación para deshacer la preparación.

Solución alternativa: Asegúrese de que los vibs de los hosts se eliminaron completamente y reinicie el host.

- **Problema 2296888: La configuración de nodo de transporte (TN)/perfil de nodo de transporte (TNP) no puede tener la marca de Migración solamente de PNIC establecida en true y, al mismo tiempo, las asignaciones de VMK para instalación rellenas en los diferentes conmutadores de host**

Cuando se produce un error de coincidencia de configuración (la marca de Migración solamente de PNIC establecida en true y las asignaciones de VMK para instalación rellenas en los diferentes conmutadores de host) durante la creación, se muestra la siguiente excepción:

Se produjo el siguiente error en la migración de VMK del host b17afc36-bbdc-491a-b944-21f73cf91585: [com.vmware.nsx.management.switching.common.exceptions.SwitchingException: El nodo de transporte [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585] no se puede actualizar o eliminar durante la migración de la interfaz de VMK de ESX a [null].]. (Código de error: 9418)

Cuando se produce un error de coincidencia de configuración durante la actualización, se muestra la siguiente excepción:

Error general (código de error: 400)

Se muestra una excepción cuando se aplica la configuración de TN/TNP, que contiene la marca de Migración solamente de PNIC establecida en true y una asignación de migración de VMK.

Solución alternativa: Cada configuración enviada al host puede tener una marca de Migración solamente de PNIC establecida en true o las asignaciones de VMK para instalación rellenas, pero no ambas.

1. Envíe la configuración de TN con los conmutadores de host que requieren que la marca de Migración solamente de PNIC esté establecida en true.
2. Para actualizar la configuración de TN, establezca todas las marcas de Migración solamente de PNIC en false y rellene las asignaciones de VMK para instalación como desee. En otras palabras, asegúrese de que la configuración enviada a TN tenga la marca de Migración solamente de PNIC establecida en true o las asignaciones de VMK para instalación rellenas en los diferentes conmutadores de host. Deben realizarse dos llamadas de configuración independientes para cualquier configuración que requiera ambas.

- **Problema 2273651: Después de eliminar el nodo de transporte, el usuario no puede enviar el SSH al host.**

Detectado en las implementaciones de KVM. El usuario elimina un nodo de transporte y recibe un mensaje que indica que la eliminación se realizó correctamente. Sin embargo, después el usuario no puede acceder al mismo host a través de SSH. Es probable que el problema se deba a la presencia de un conmutador virtual abierto (OVS) que no está administrado por NSX-T y que, probablemente, se preinstaló como parte de la plantilla de KVM.

Solución alternativa: Identifique los OVS problemáticos antes de eliminar el nodo de transporte.

1. Ejecute `ovs-vsctl show` para identificar el OVS.
2. Migre cualquier interfaz de máquina virtual de carga de trabajo desde el OVS hasta el puente Linux.

3. Elimine el nodo de transporte de la siguiente forma:

```
DELETE api/v1/transport-nodes/<uuid>
```

- **Problema 2281537:** Después de la migración, el nodo de transporte de ESXi con varios VTEP no inicia sesión en BFD.

Después de migrar un nodo de NSX-V a NSX-T, el nodo de transporte de ESXi con varios VTEP no puede iniciar la sesión en BFD en todos los nodos de VTEP a Edge.

Solución alternativa: Reinicie el servicio netcpa.

#### Problemas conocidos de NSX Manager

- **Problema 2285306:** El estado de implementación de servicio de los servicios de Guest Introspection puede seguir apareciendo como "Desconocido" hasta que la máquina virtual del servicio se enciende

Después de crear una implementación de servicio y de que esta se muestre en la cuadrícula de implementaciones de servicio, es posible que el estado no se muestre inmediatamente como "En curso", sino que permanezca como "Desconocido" hasta que la cuadrícula se actualice.

Solución alternativa: Ninguna. Actualice la página transcurridos diez segundos. El estado debería actualizarse.

- **Problema 2292526:** Al agregar un host, aparece un mensaje que indica que no se puede acceder el host

Al agregar un host ESXi, aparece un mensaje que indica que no se puede acceder él, pero no se dice por qué. Lo más probable es que se usaran unas credenciales incorrectas.

Solución alternativa: Revise la configuración del host, vuelva a crear las credenciales e intente agregar el host de nuevo.

- **Problema 2292701:** El usuario no puede actualizar el número de secuencia en un mapa de enlaces

El usuario no puede cambiar el orden ni la prioridad de los perfiles aplicados a una entidad actualizando el número de secuencia.

Solución alternativa: Elimine el mapa de enlaces y vuelva a crearlo con el nuevo número de secuencia que quiera.

- **Problema 2294345:** Se puede producir un error al ejecutar una clasificación de Application Discovery en un grupo que tiene máquinas virtuales alojadas tanto en ESXi como en KVM  
La función de Application Discovery solo se puede usar en hipervisores de ESXi. Los resultados de una clasificación de Application Discovery no estarán garantizados en grupos de máquinas virtuales que se encuentren en diferentes hosts (hosts no compatibles inclusive).

Solución alternativa: Ninguna.

#### Problemas conocidos de NSX Edge

- **Problema 2248345:** Tras instalar NSX-T Edge, la máquina se inicia y muestra una pantalla negra vacía

NSX-T Edge no se puede instalar en una máquina HPE ProLiant DL380 Gen9.

Solución alternativa: Use otra máquina o implemente NSX-T Edge como una máquina virtual en un hipervisor.

- **Problema 2283559:** Las API del plano de administración /routing-table y /forwarding-table devuelven un error si la instancia de Edge tiene más de 65.000 rutas para RIB y más de 100.000 rutas para FIB

Si la instancia de Edge tiene más de 65.000 rutas para RIB y más de 100.000 rutas para FIB, la solicitud del plano de administración a la instancia de Edge tarda más de 10 segundos y hace que el tiempo de espera se agote. Estas API son de solo lectura y tienen impacto solo si es necesario descargar las más de 65.000 rutas para RIB y más de 100.000 rutas para FIB mediante una API/interfaz de usuario.

Solución alternativa: Existen dos formas de recuperar rutas de RIB/FIB.

- Estas API admiten opciones de filtrado en función de los prefijos de red o del tipo de ruta. Utilice estas opciones para descargar las rutas que sean de su interés.
- Compatibilidad de CLI en caso de que se necesite toda la tabla de FIB/RIB y no haya tiempo de espera para ello.

## Problemas conocidos de las redes lógicas

- **Problema 2243415: Un cliente no puede implementar un servicio de NXGI usando el conmutador lógico (como una red de administración)**

En la pantalla de implementación de NXGI, el usuario no ve un conmutador lógico en el control de selección de la red. Si la API se utiliza directamente con el citado conmutador lógico como una red de administración, el usuario verá el siguiente error: "La implementación del servicio no puede acceder a la red especificada".

Solución alternativa: Realice la implementación usando otro tipo de conmutador, como uno local o distribuido.

- **Problema 2264386: La eliminación del nodo de transporte sucede aun cuando dicho nodo de transporte forme parte del grupo NSGroup**

La eliminación del nodo de transporte es posible incluso cuando el nodo forma parte de un grupo NSGroup. Esta eliminación debe evitarse. Si surge este problema, deberá volver a crear los grupos NSGroup y reconstruir las relaciones con sus correspondientes nodos de transporte.

Solución alternativa: Para evitar este problema, compruebe manualmente si hay un nodo de transporte asociado con un grupo NSGroup. En la interfaz del plano de administración, desplácese hasta **Opciones avanzadas de redes y seguridad > Inventario > Grupos** o hasta **Sistema > Nodos > Nodos de transporte > Relacionado > Grupo NSGroup**.

- **Problema 2292997: Puede que algunas interfaces de enrutador lógico no puedan crear la subinterfaz de la pila de red de Linux**

Puede que algunas interfaces de enrutador lógico no puedan crear la subinterfaz de la pila de red de Linux y se devuelva el siguiente error: `errorCode="EDG0100002". Error al crear subinterfaz: se superó el máximo de subinterfaces`. Como resultado, es posible que el tráfico que reenvía el enrutador de servicio de nivel 0 (Tier0 Service Router, TO SR) se descarte debido a que faltan rutas.

Solución alternativa: Reinicie el nodo de Edge afectado.

- **Problema 228688: Si BGP se configura sobre VTI, el vecino de BGP se debe eliminar en primer lugar al eliminar la sesión base de ruta de IPsec.**

Si BGP está configurado sobre una VTI y se elimina la sesión de IPsec, ambos SR estarán en un estado inactivo, lo que hará que el tráfico se bloquee. Para reanudar el tráfico, hay que eliminar el vecino de BGP configurado para la VTI. En este escenario, solo el BGP configurado tiene lugar sobre VTI.

Solución alternativa: Elimine el vecino de BGP antes de eliminar la sesión de IPsec.

- **Problema 2288509: La propiedad MTU no es compatible con la interfaz de servicio de nivel 0 o nivel 1 (puerto de servicio central)**

La propiedad MTU no es compatible con la interfaz de servicio de nivel 0 o nivel 1 (puerto de servicio central).

Solución alternativa: Configure la propiedad MTU con la API del plano de administración, aun cuando el puerto CSP se creara mediante el flujo de trabajo de directiva.

- **Problema 2288774:** El puerto de segmento genera un error de realización debido al uso de más de 30 etiquetas (erróneamente)

La entrada de usuario intenta aplicar incorrectamente más de 30 etiquetas. Sin embargo, el flujo de trabajo de directiva no valida ni rechaza la entrada del usuario, según corresponda, y permite la configuración. Tras esto, el flujo de trabajo de directiva muestra una alarma con un mensaje de error que avisa al usuario de que no debe utilizar más de 30 etiquetas. Llegado ese momento, el usuario puede corregir este problema.

Solución alternativa: Corrija la configuración después de que el error se muestre.

- **Problema 2275412:** La conexión de puerto no funciona entre varias zonas de transporte
- La conexión de puerto solo se puede utilizar en una única zona de transporte.

Solución alternativa: Ninguna.

- **Problema 2290083:** Falta la validación al crear un segmento basado en VLAN
- Cuando se especifica una zona de transporte de VLAN con una propiedad de identificador de VLAN, el sistema no puede realizar la validación e identifica un error. Como resultado, el intento será fallido durante la realización y se generará un error.

Solución alternativa: Consulte los detalles del error de la alarma de realización para obtener instrucciones sobre cómo corregir la entrada.

- **Problema 2292096:** El comando de la CLI "get service router config route-maps" devuelve un resultado vacío

El comando de la CLI "get service router config route-maps" devuelve un resultado vacío, incluso cuando hay mapas de rutas configurados. Este es solo un problema de visualización.

Solución alternativa: Utilice el comando de la CLI `get service router config`, que devuelve la configuración de mapa de ruta como un subconjunto de resultados completos.

- **Problema 2994002:** El nivel 1 no aparece en la lista desplegable de la puerta de enlace de nivel 0 o nivel 1 para que pueda seleccionarse durante la creación de un reenviador de DNS
- En una implementación a gran escala con miles de registros, el nivel 1 no aparece en la lista desplegable de puertas de enlace de nivel 0 o nivel 1 para poder seleccionarlo en el flujo de trabajo de creación de un reenviador de DNS. En consecuencia, se debe utilizar la API para configurar la creación de reenviadores de DNS.

Solución alternativa: Defina la configuración con la API.

- **Problema 2298499:** La VPN falla entre la puerta de enlace de nube pública y el host del mismo nivel si la puerta de enlace no se implementa con la IP pública.

No se puede establecer el túnel VPN entre la puerta de enlace de nube pública (PCG) y el host del mismo nivel si se implementa la PCG sin una dirección IP pública en el vínculo superior. La razón es que, de forma predeterminada, la PCG está realizando SNAT en el tráfico de la VPN.

Solución alternativa: Al implementar la puerta de enlace de nube pública, habilite la IP pública para la interfaz de vínculo superior.

- **Problema 2392093:** El tráfico se interrumpe debido a la comprobación de RPF

La comprobación de RPF puede provocar que se interrumpa el tráfico si este se fija a través de un vínculo inferior de nivel 0, y los enrutadores de nivel 0 y nivel 1 se encuentran en el mismo nodo de Edge.

Solución alternativa: Ninguna.

- **Problema 2288523:** La descarga del controlador de NSX Guest Introspection puede conllevar problemas de seguridad

El firewall de identidad (Identity Firewall, IDFW) depende de la información de identidad del usuario proveniente del controlador de NSX Guest Introspection. Cargar el controlador puede provocar problemas de seguridad a los usuarios que iniciaron sesión desde la máquina invitada específica. Esto se muestra a través de los siguientes síntomas:

- Las reglas de firewall no se aplicaron a los usuarios que iniciaron sesión desde algunas máquinas virtuales invitadas en las que el controlador de Guest Introspection se cargó.
- El componente de IDFW no permitió el inicio de sesión de los detalles de usuario de los usuarios que inician sesión a partir de determinadas máquinas virtuales invitadas en las que el controlador de Guest Introspection se descarga.
- Los registros de MUX no muestran ninguna conexión a partir de estas máquinas virtuales invitadas, incluso si el IDFW está habilitado en el host.
- Los registros de MUX no muestran ningún evento de red de esas máquinas virtuales invitadas, incluso si el IDFW está habilitado en el host.

Como resultado, la regla predeterminada Denegar todo puede bloquear el acceso a los usuarios de las máquinas virtuales invitadas en las que el controlador de Guest Introspection se cargó.

Solución alternativa: Ninguna. El administrador de TI debe seguir las prácticas recomendadas de seguridad para asegurarse de que ningún usuario tiene privilegios para cargar controladores de Guest Introspection en máquinas virtuales invitadas.

- **Problema 2288773:** La antigua API de protocolo TLS sigue disponible, pero sobrescribe la configuración

NSX-T tiene una API nueva para configurar conjuntos de claves de cifrado y versiones de protocolo TLS de NSX, lo que hace que se actualicen todos los nodos de un clúster de NSX-T. Sin embargo, la API anterior aún está disponible. Puede utilizarse, pero la configuración global sobrescribirá la nueva configuración.

Solución alternativa: Utilice la API nueva.

- **Problema 2291872:** Un mensaje del registro muestra un mensaje de advertencia cuando se utiliza el servicio TFTP en una regla de firewall

Un mensaje del registro muestra un mensaje de advertencia irrelevante cuando se utiliza el servicio TFTP en una regla de firewall. Ubicación del registro en el nodo de ESXi: `/var/log/cfgAgent.log`.

Solución alternativa: Cree un nuevo servicio TFTP como servicio L4PortSet y úselo en la regla de firewall.

- **Problema 2203863:** No se admiten las reglas de firewall de identidad para el tráfico UDP e ICMP.

Las reglas de firewall de identidad no funcionan con las pruebas de ping. La funcionalidad actual solo admite el tráfico de TCP.

Solución alternativa: Utilice TCP para probar las reglas de firewall de identidad. No establezca nunca ANY/UDP/ICMP en la columna de servicio al configurar reglas de firewall de identidad

- **Problema 2296430:** La API de NSX-T Manager no proporciona nombres alternativos del sujeto durante la generación del certificado.

La API de NSX-T Manager no proporciona nombres alternativos del sujeto para emitir certificados, específicamente durante la generación de CSR.

Solución alternativa: Cree la CSR mediante una herramienta externa que admita las extensiones. Después de recibir el certificado firmado de la entidad de certificación, impórtelo a NSX-T Manager con la clave de la CSR.

- **Problema 2252738:** Para las reglas de nombre de dominio completo (FQDN), un paquete que no coincide con la regla tiene permiso para llegar al destino.

Cuando se crea una regla de FQDN específica, el nombre de dominio asociado a una dirección IP se agrega a la base de datos de firewall que coincide con la regla, y los paquetes enviados a ese nombre de dominio tienen permiso para acceder al servidor. Sin embargo, si un usuario cambia el nombre de dominio asociado a esa dirección IP en el servidor de nombres de dominio, la entrada de nombre de dominio no se actualiza en la base de datos del firewall (a menos que exista otra regla de FQDN que coincida con el nuevo nombre de dominio). Como resultado, los paquetes se envían al nuevo nombre de dominio aunque la regla de FQDN lo excluya.

Solución alternativa: Ninguna.

- **Problema 2395334: (Windows) paquetes descartados incorrectamente debido a la entrada contrack de reglas de firewall sin estado.**  
Las reglas de firewall sin estado no son muy compatibles con las máquinas virtuales de Windows.

Solución alternativa: En su lugar, agregue una regla de firewall con estado.

- **Problema 2458384: las páginas de la interfaz de NSX-T Manager no se cargan y se muestra el error 403.**  
Se observa en las versiones 2.4.0 y 2.4.1. Este problema afecta a los inicios de sesión de administrador y de Identity Manager. El FQDN de la NSX-T Manager utiliza el formato \*.SLD.TLD. Por ejemplo: \*.co.uk, \*.co.il, \*.com.au, etc.

Solución alternativa: Acceda a la interfaz de usuario de NSX-T Manager utilizando el nombre corto o la IP en lugar del FQDN. Consulte el artículo <https://kb.vmware.com/s/article/71217>.

#### Problemas conocidos de las redes de KVM

- **Problema 2292995: El estado de realización se establece en error, a pesar de que todas las reglas configuradas están programadas en OVS**  
La API ofrece una impresión de falso negativo incluso cuando las reglas del DFW están programadas en el plano de datos.

Solución alternativa: La actualización de cualquiera de las reglas del DFW borra esta condición de error. Por ejemplo, tan solo basta con activar el registro de reglas para forzar al módulo de DFW de KVM a borrar la condición de error.

#### Problemas conocidos del equilibrador de carga

- **Problema 2290899: IPSec VPN no funciona y se produce un error en la realización de plano de control de IPSec**  
IPSec VPN (o L2VPN) no aparece si hay habilitados más de 62 servidores de equilibrador de carga junto con el servicio IPSec en el nivel 0 en el mismo nodo de Edge.

Solución alternativa: Reduzca el número de servidores de equilibrador de carga a menos de 62.

- **Problema 2297157: El rendimiento de HTTPS de equilibrio de carga se ve afectado por el modo FIPS.**  
El rendimiento del equilibrio de carga puede verse afectado de forma negativa cuando el modo FIPS predeterminado está habilitado.

Solución alternativa: Consulte el artículo 67400 de la base de conocimientos [El servicio de equilibrio de carga de NSX-T 2.4.0 puede tener un rendimiento bajo en HTTPS](#).

- **Problema 2362688: Si algunos miembros del grupo están inactivos en un servicio del equilibrador de carga, la interfaz de usuario muestra el estado consolidado como activo**  
Cuando un miembro del grupo está inactivo, no hay ninguna indicación en la interfaz de usuario de la directiva en la que el estado del grupo aparezca verde y activo.

Solución alternativa: Ninguna.

#### Problemas conocidos de interoperabilidad de soluciones



- **Problema 2289150:** Las llamadas de PCM a AWS empiezan a generar errores  
Si actualiza la función de puerta de enlace de nube pública (Public Cloud Gateway, PCG) de una cuenta de AWS en CSM de *old-pcg-role* a *new-pcg-role*, CSM actualizará la función de la instancia de PCG en AWS a *new-pcg-role*. Sin embargo, PCM no sabrá que la función de PCG se actualizó y, en consecuencia, seguirá usando los clientes de AWS antiguos creados mediante *old-pcg-role*. Esto hará que el examen del inventario de nube de AWS de PCM y otras llamadas de nube de AWS generen errores.

Solución alternativa: Si surge este problema, no modifique ni elimine la función de PCG anterior inmediatamente después de cambiarla a la nueva función. Espere como mínimo 6,5 horas. Si reinicia la función de PCG, se volverán a inicializar todos los clientes de AWS con nuevas credenciales de función.

## Problemas conocidos de las operaciones y los servicios de supervisión

- **Problema 2275869:** Los registros de `cfgAgent` se acumulan en menos de 1 minuto en el host ESXi si hay reglas en el host que tienen etiquetas con más de 31 caracteres  
Acumular registros con frecuencia puede conllevar la pérdida de información útil en `cfgAgent.log` para depurar hosts y solucionar problemas relativos a estos. Ubicación del registro en el host ESXi:  
`/var/log/cfgAgent.log`

Solución alternativa: Ninguna.

- **Problema 2289984:** `mux_connectivity_status` aparece como conectado, incluso después de que el servicio `nsx-context-mux` se detuviera en el host  
Cuando `nsx-context-mux` o `nsx-opsagent` no se están ejecutando en el host, el sistema (la interfaz de NSX o la API de instancia de servicio) muestra el estado de la solución y el estado del agente de Guest Introspection incorrectamente como en ejecución, con una marca de tiempo sin modificar. En consecuencia, las máquinas virtuales invitadas pueden perder la protección antivirus.

Solución alternativa: Intente iniciar manualmente MUX y opsAgent en el host si no se están ejecutando.

1. Inicie sesión en el host como raíz y ejecute los comandos siguientes:  
`/etc/init.d/nsx-opsagent start`  
`/etc/init.d/nsx-context-mux start`
2. Después de iniciar los agentes, espere unos minutos y compruebe que se actualizó la marca de tiempo del estado de mantenimiento en la interfaz de usuario.

## Problemas conocidos de actualización

- **Problema 2273737:** Después de actualizar de NSX-T 2.3 a 2.4, faltan los detalles del servidor de vIDM  
En el caso de que se emplee vIDM, en el que el servidor de vIDM está configurado únicamente en el dispositivo de directiva de NSX, el servidor de vIDM se migra durante la actualización, pero dicho servidor no aparecerá en el dispositivo combinado.

Solución alternativa: En función del momento en el que el cliente detecta este problema, hay dos opciones posibles:

- Antes de realizar la actualización de la versión 2.3 a la 2.4:  
Configure los mismos detalles del servidor de vIDM en el dispositivo de directiva de NSX y la máquina virtual de NSX Manager.
- Después de realizar la actualización de la versión 2.3 a la 2.4:  
Vuelva a configurar los mismos detalles del servidor de vIDM en el dispositivo combinado.

- **Problema 2288549:** Se produce un error de suma de comprobación en el archivo de manifiesto de RepoSync

Esto se observa en las implementaciones actualizadas recientemente a 2.4. Cuando se hace una copia de seguridad de una instalación actualizada y esa copia se restaura en una instancia de Manager implementada desde cero, la suma de comprobación del archivo de manifiesto del repositorio presente en la base de datos y la suma de comprobación del archivo de manifiesto real no coinciden. Esto hace que RepoSync se marque como con errores después de restaurar la copia de seguridad.

Solución alternativa: Para recuperarse de este error, haga lo siguiente:

1. Ejecute el comando de la CLI `get service install-upgrade`.  
Anote la dirección IP que aparece en los resultados como "Enabled on".
2. Inicie sesión con la dirección IP de NSX Manager indicada en "Enabled on" en el resultado devuelto por el comando anterior.
3. Desplácese hasta **Sistema > Descripción general** y busque el nodo con la misma dirección IP que la devuelta en "Enabled on".
4. Haga clic en **Resolver** en ese nodo.
5. Una vez que esta operación de resolución se realice correctamente, haga clic en **Resolver** en todos los nodos de la misma interfaz.

Ahora, los tres nodos mostrarán el estado de RepoSync como **Completo**.

- **Problema 2279973:** Si se crea un grupo en blanco y la actualización del plano de administración prosigue, después de esa actualización, el grupo en blanco se muestra como no iniciado. Esto ocurre si se crea un grupo en blanco y, tras ello, la actualización prosigue.

Solución alternativa: No cree un grupo en blanco.

Lleve a cabo uno de los siguientes procedimientos:

- Elimine el grupo en blanco.
  - Haga clic en un botón **Reanudar** para finalizar la actualización.
  - Restablezca el plan.
- **Problema 2282389:** El plan de actualización de UC no está sincronizado con la pertenencia del clúster de vCenter si ESX se mueve entre clústeres.  
Cuando ESX se traslada de un clúster a otro en vCenter, el cambio no se refleja en el plan de actualización de UC. Esto puede hacer que más de un host pase al modo de mantenimiento al mismo tiempo si el usuario seleccionó "Actualizar en paralelo" en los grupos.

Solución alternativa: En la página de actualización del host, haga clic en la opción "Restablecer" para volver a crear el plan, de forma que el plan de actualización de UC esté sincronizado con los clústeres de vCenter.

- **Problema 2288921:** El estado de actualización deja de estar sincronizado si se agregan nodos de Edge de una versión anterior.  
El estado de actualización deja de estar sincronizado si el usuario agrega nodos de Edge de una versión anterior después de la actualización de Edge. Esto causa problemas a la hora de proseguir con la llamada de actualización.

Solución alternativa: En primer lugar, absténgase de agregar nodos de Edge de una versión anterior. Si surge este problema, reinicie el servicio de UC.

- **Problema 2291625:** El estado de actualización de PCG cambia de SUCCESS a NOT\_STARTED después de sincronizar el plan de actualización.  
Este problema solo se produce si el usuario actualiza la PCG y, a continuación, intenta actualizar más agentes/PCG posteriormente.  
En el flujo de trabajo recomendado, después de actualizar la PCG no hay más componentes entre nubes que actualizar a través de la interfaz de UC.

Esto no afecta a ninguna funcionalidad. El estado de la actualización de PCG completada anteriormente de forma correcta se muestra como "Ninguno" en la interfaz de usuario de la actualización.

Solución alternativa: Ninguna. La funcionalidad no debería verse afectada.

- **Problema 2293227:** Después de actualizar a la versión 2.4, las reglas de IDFW no se aplican a las máquinas virtuales que ejecutan VMware Tools 10.3.5  
Después de realizar una actualización dinámica de NSX-T, las reglas de IDFW no se aplican a las máquinas virtuales que ejecutan VMware Tools 10.3.5, lo que puede provocar una pérdida de la protección antivirus en esas máquinas virtuales.

Solución alternativa: Reinicie las máquinas virtuales afectadas.

- **Problema 2295564:** Puede que se pierda la conectividad del controlador de nodo de Edge después de actualizar de la versión 2.3 a la 2.4  
Este es un problema intermitente que afectará a parte del tráfico de norte a sur.

Solución alternativa: Habilite y deshabilite el modo de mantenimiento en el mismo nodo de Edge.

- **Problema 2294178:** La actualización de VIB de host falla al actualizar de la versión 2.3.1 a la 2.4. Al actualizar de la versión 2.3.1 a la 2.4, se puede generar el error No se pudo instalar el paquete sin conexión en el host. Más específicamente, la actualización de VIB del host falla porque el módulo de seguridad del conmutador no se puede descargar. Se sabe que el problema se produce si la función de detección de IP está habilitada en el perfil de conmutación y cuando se realiza una actualización local de NSX-T 2.3.1 a NSX-T 2.4 con un host que ejecuta ESXi-6.7EP06 (compilación 11675023).

Solución alternativa: Consulte el artículo 67445 de la base de conocimientos [Con la detección de direcciones IP habilitada, la actualización VIB del host puede generar un error al actualizar de NSX-T 2.3.1 a NSX-T 2.4.](#)

- **Problema 2277543:** La actualización de VIB del host falla durante una actualización local con el error "No se pudo instalar el paquete sin conexión en el host".  
Este error puede producirse si se implementó vMotion de almacenamiento en el host antes de realizar una actualización local de NSX-T 2.3.x a NSX-T 2.4 y los hosts ejecutan ESXi-6.5P03 (compilación 10884925). El módulo de seguridad de conmutador de la versión 2.3.x no se elimina si se implementó vMotion de almacenamiento justo antes de la actualización del host. El proceso de vMotion de almacenamiento provoca una fuga de memoria que genera un error en la descarga del módulo de seguridad del conmutador.

Solución alternativa: Consulte el artículo 67444 de la base de conocimientos [La actualización de VIB del host puede fallar al actualizar de NSX-T 2.3.x a NSX-T 2.4.0 si se aplica vMotion de almacenamiento a las máquinas virtuales antes de la actualización del host.](#)

- **Problema 2276398:** Cuando una máquina virtual de servicio de partners de AV se actualiza mediante NSX, es posible que se pierdan hasta veinte minutos de protección.  
Cuando se actualiza una máquina virtual de servicio de partners, se implementa la nueva y se elimina la antigua. Pueden aparecer errores de conexión del tipo SolutionHandler en el syslog del host.

Solución alternativa: Para solucionar este problema, elimine la entrada de la memoria caché de ARP en el host después de la actualización y, a continuación, haga ping a la IP de control del partner en el host.

- **Problema 2297918:** Después de la actualización de la versión 2.3.1 a la 2.4, no se puede eliminar NSX del clúster.  
Después de actualizar un clúster de la versión 2.3.1 a la 2.4, no se puede eliminar NSX-T y se muestra el siguiente mensaje: "No se pudo quitar NSX del clúster: Hay una recopilación de nodos de transporte o una plantilla de nodo de transporte relacionadas para esta plantilla de tejido. La plantilla de nodo de transporte o la recopilación de nodos de transporte se deben eliminar antes de eliminar o deshabilitar en esta plantilla de tejido."

Solución alternativa: Desconecte el perfil del nodo de transporte del clúster afectado y, a continuación, utilice el flujo de trabajo "Quitar NSX".

- **Problema 2286030:** la configuración del nodo de transporte muestra un estado de error al actualizar de NSX-T 2.3.x y versiones anteriores a las versiones 2.4.x.

La configuración del nodo de transporte muestra un estado de error al actualizar de NSX-T 2.3.x y versiones anteriores a las versiones 2.4.x debido a una excepción de puntero nulo. Cuando se migra el nodo de transporte de ESXi con adaptadores de VMkernel a un conmutador lógico de VLAN de N-VDS y, a continuación, se actualiza de NSX-T 2.3.x a NSX-T 2.4.x, una condición de carrera puede provocar que un estado de error de la configuración del nodo de transporte de ESXi. Sin embargo, la conectividad del nodo de transporte de ESXi con NSX Manager y los controladores permanece intacta durante la actualización, incluso después de que el nodo se marque con un estado de configuración de error.

Solución alternativa: Actualice o vuelva a enviar el nodo de transporte para restablecer el estado de la configuración a un estado correcto.

1. En NSX Manager, edite el nodo de transporte de ESXi que se muestra con un estado de error.
2. En la ventana emergente de configuración del nodo de transporte de ESXi, haga clic en **Guardar**.

Esta acción restablecerá el estado. No tiene que modificar la configuración.

## Problemas conocidos de la API

### Problemas conocidos de NSX Policy Manager

- **Problema 2291267:** La sección de directiva de puerta de enlace predeterminada creada mediante PCM no tiene asignado un número de secuencia, por lo que la directiva la establece de forma predeterminada en 0

Si un usuario crea directivas de puerta de enlace sin un número de secuencia u opciones `insert_top`, surgirá un conflicto de directiva. Ubicación de registro: `/var/log/policy/policy.log`

Solución alternativa: Para evitar este problema, cree directivas siempre con los números de secuencia pertinentes o utilice los parámetros de URL `action=revise&operation=insert_top`.

- **Problema 2289278:** La API de directiva devuelve un error, pero permite configurar varios servidores virtuales con el mismo grupo y diferente perfil de persistencia

El sistema no admite la configuración de tipos de persistencia en conflicto dentro de un mismo grupo para distintos servidores virtuales de equilibrador de carga. Sin embargo, la directiva no valida ni rechaza la entrada en conflicto, según corresponda, y permite la configuración. Posteriormente, la directiva muestra una alarma con el mensaje de error.

Solución alternativa: Si surge este problema, puede corregirlo cambiando la configuración de grupo en el servidor virtual de equilibrador de carga.

- **Problema 2248186:** El enrutador BGP instala rutas IPV6 desde su vecino con su propia interfaz como siguiente salto.

Como resultado, es posible que se produzca un error en el redireccionamiento de IPV6 a la ruta instalada y que se cree un bucle de redireccionamiento.

Solución alternativa: Para evitar este problema, configure un mapa de ruta para filtrar las direcciones conectadas de IPv6 como el salto siguiente en las actualizaciones de BGP.

### Problemas conocidos de NSX Cloud

- **Problema 2287884:** Algunas imágenes del catálogo de Centos no son compatibles con NSX Cloud

NSX Cloud admite únicamente imágenes del catálogo de Centos cuyas versiones de distribución coincidan con las versiones de kernel secundarias previstas.

Por ejemplo, se espera que las versiones de distribución y sus versiones de kernel correspondientes sean las siguientes:

- RHEL 7.5 3.10.0-862
- RHEL 7.4 3.10.0-693
- RHEL 7.3 3.10.0-514

Solución alternativa: Use únicamente distribuciones de Centos que se recomienden en la documentación.

- **Problema 2275232:** Puede que DHCP no funcione con las máquinas virtuales en la nube si la estrategia de conectividad del DFW cambia de BLACKLIST a WHITELIST  
Todas las máquinas virtuales que soliciten nuevas concesiones de DHCP podrían perder sus IP. Es necesario permitir DHCP de manera explícita para las máquinas virtuales de nube en DFW.

Solución alternativa: Permita DHCP de manera explícita para las máquinas virtuales de nube en DFW.

- **Problema 2277814:** La máquina virtual se mueve a vm-overlay-sg cuando el valor de la etiqueta nsx.network no es válido  
Las máquinas virtuales etiquetadas con una etiqueta nsx.network no válida se trasladará a vm-overlay-sg.

Solución alternativa: Quite la etiqueta no válida.

- **Problema 2280663:** La retirada de varios VPC en paralelo podría dar lugar a errores en casos excepcionales  
Se podría producir un error en la retirada de un VPC de equipo.

Solución alternativa: Borre manualmente el VPC y los grupos correspondientes en la directiva.

- **Problema solucionado 2287124:** Después de implementar PCG en una VNET de Microsoft Azure, el icono de la VNET en CSM informa erróneamente de una advertencia.  
Después de implementar PCG en una VNET de Microsoft Azure, la VNET muestra en CSM una señal de advertencia (triángulo amarillo con un signo de exclamación). Si coloca el cursor sobre el icono de advertencia, CSM informa de que el estado de MP (plano de administración) y CCP (plano de control) es desconocido. Sin embargo, es posible que no haya ningún problema de conectividad y la advertencia se muestre por error.
- **Problema 2290688:** La actualización de las máquinas virtuales de Windows 2016 en AWS falla.  
La actualización de varias máquinas virtuales de carga de trabajo de Windows en AWS falla. El estado de actualización de la máquina virtual aparece en el portal de AWS como bloqueado en "Comprobación 1/2". También se produce un error al reintentar. Este problema solo se produce en las actualizaciones de la misma versión de NSX-T.

Solución alternativa: Para solucionar este problema, haga lo siguiente:

1. Asegúrese de que la PCG se haya actualizado en los hosts afectados para que la máquina virtual pueda descargar los componentes de host más recientes.
2. Reinicie la máquina virtual para conseguir un estado correcto.
3. Ejecute manualmente `uninstall cmd`.
4. Ejecute manualmente `install cmd`.