



Notas de la versión de VMware NSX-T Data Center 2.5

VMware NSX-T Data Center 2.5 | 19 de septiembre de 2019 | Compilación 14663974

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](#)
- [Cambios en el comportamiento general](#)
- [Obsolescencias de la API y cambios del comportamiento](#)
- [Idiomas disponibles](#)
- [Recursos de CLI y API](#)
- [Historial de revisión](#)
- [Problemas resueltos](#)
- [Problemas conocidos](#)

Novedades

NSX-T Data Center 2.5 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 incluyen una nueva interfaz de usuario de redes basada en intenciones, un firewall con reconocimiento de contexto, funciones de introspección de red y de invitado, soporte de IPv6, una administración en clúster de alta disponibilidad, una instalación de NSX basada en perfiles para clústeres de proceso de vSphere, y mejoras en el coordinador de migración para migrar de NSX Data Center for vSphere a NSX-T Data Center.

NSX Intelligence

NSX-T Data Center 2.5 presenta NSX Intelligence 1.0, un nuevo componente de NSX Analytics. NSX Intelligence proporciona una interfaz de usuario a través de un único panel de administración dentro de NSX Manager con las siguientes funciones:

- Cerca de la información de flujo en tiempo real de las cargas de trabajo en su entorno.
- NSX Intelligence correlaciona flujos activos o históricos, configuraciones de usuario e inventario de cargas de trabajo.
- Capacidad para ver la información anterior sobre los flujos, las configuraciones de los usuarios y el inventario de cargas de trabajo.
- Planificación automatizada de microsegmentación mediante la recomendación de los servicios, los grupos y las reglas de firewall.

Soporte de la API de contenedor

Nuevo soporte de la API para el inventario de contenedores. Consulte la documentación de la API.

Redes de Capa 2

- **Mejoras en el puentes de Edge:** el puente de Edge ahora permite conectar el mismo segmento a varios perfiles de puente, lo que ofrece la posibilidad de unir un segmento varias veces a redes VLAN en la infraestructura física. Esta nueva funcionalidad reemplaza y deja obsoleto el puente ESXi original de versiones anteriores de NSX-T Data Center. **Precaución:** Utilice esta función bajo su cuenta y riesgo. Presenta el riesgo de crear un bucle de puente conectando el mismo segmento dos veces al mismo dominio de Capa 2 en la red física. No hay ningún mecanismo de mitigación de bucles.
- **Comprobación de estado de MTU/VLAN:** desde el punto de vista de las operaciones, los problemas de conectividad de red causados por errores de configuración suelen ser difíciles de identificar. Entre los casos más comunes se incluyen aquellos en los que los administradores de redes virtuales utilizan NSX Manager, mientras que los administradores de redes físicas utilizan conmutadores de red física.
 - **Comprobación de estado de VLAN:** comprueba si la configuración de la VLAN de N-VDS coincide con la configuración del puerto troncal en los puertos del conmutador físico adyacente.
 - **Comprobación de estado de MTU:** comprueba si la configuración de la MTU del puerto de conmutador de acceso físico basado en la VLAN coincide con la configuración de la MTU de N-VDS.
- **Etiquetado entre VLAN invitadas:** N-VDS de ruta de datos mejorada permite a los usuarios asignar una etiqueta de VLAN invitada a un segmento. Esta capacidad supera la limitación de 10 VNIC por máquina virtual y permite que la infraestructura de NSX enrute el tráfico etiquetado de VLAN invitado (asignado a diferentes segmentos).

Redes de Capa 3

- **Ubicación de nivel 1 dentro del clúster de Edge en función del dominio de errores:** permite que NSX-T ubique automáticamente las puertas de enlace de nivel 1 en función de los dominios de errores definidos por el usuario. Esto aumenta la fiabilidad de las puertas de enlace de nivel 1 en las zonas de disponibilidad, los bastidores o los hosts, incluso cuando se utiliza la ubicación automática de las puertas de enlace de nivel 1.
- **Uso compartido de la carga asimétrica después de un error en el enrutador en la topología de ECMP:** en la puerta de enlace de nivel 0 activa/activa, cuando un enrutador de servicio defectuoso dejaba de funcionar, otro enrutador retomaba el tráfico de enrutador defectuoso, doblando el tráfico que pasaba por el enrutador de servicio. 30 minutos después de error del enrutador, la dirección IP del enrutador defectuosa se elimina de la lista de saltos siguientes, lo que evita que se envíe tráfico adicional a un enrutador específico.
- **Obtener las rutas de BGP anunciadas y recibidas por cada par a través de la API:** simplifica las operaciones de BGP evitando el uso de la CLI para verificar las rutas recibidas y enviadas a los pares de BGP.
- **Soporte de comunidades grandes de BGP:** ofrece la opción de utilizar comunidades junto con ASN de 4 bytes como se define en RFC8092.
- **Opción del modo de aplicación auxiliar de reinicio estable de BGP por par:** ofrece la opción de puerta de enlace de nivel 0 para ayudar a mantener el enrutador de los enrutadores físicos en dirección norte con un plano de control redundante sin comprometer el tiempo de conmutación por error entre enrutadores de nivel 0.
- **API masiva para crear varias reglas NAT:** mejora la API NAT existente para empaquetar la creación de un número elevado de reglas NAT en una sola llamada API.

Plataforma Edge

- **Soporte de Mellanox ConnectX-4 y ConnectX-4 LX en el nodo de Edge sin sistema operativo:** los nodos de Edge sin sistema operativo ahora admiten las NIC físicas Mellanox ConnectX-4 y ConnectX-4 LX en 10/25/40/50/100 Gbps.
- **Administración de PNIC Edge sin sistema operativo:** proporciona la opción para seleccionar las NIC físicas que se utilizarán como NIC de plano de datos (fastpath). También aumenta el número de

NIC físicas admitidas en el nodo de Edge sin sistema operativo de 8 a 16 PNIC.

Soporte de IPv6 mejorado

NSX-T 2.5 continúa mejorando el conjunto de funciones de enrutamiento/reenvío de IPv6. Esto incluye soporte para:

- IPv6 SLAAC (configuración automática de direcciones sin estado), que proporciona automáticamente direcciones IPv6 a máquinas virtuales.
- Anuncio de enrutador IPv6, la puerta de enlace de NSX-T proporciona parámetros IPv6 a través del anuncio de enrutador.
- Direcciones IPv6 DAD, las puertas de enlace NSX-T detectan la asignación de direcciones IPv6 duplicadas.

Mejoras del firewall

Compatibilidad con AppID de capa 7

NSX-T 2.5 agrega más funciones de capa 7 para el firewall distribuido y de puerta de enlace. Esto incluye soporte para:

- Soporte de AppID de capa 7 para el firewall distribuido en KVM.
- Soporte de AppID de capa 7 para el firewall de puerta de enlace.
- Varias configuraciones de AppID de capa 7 en una sola regla de firewall.

Mejoras de filtrado de URL/FQDN

NSX-T 2.5 incluye mejoras menores en la compatibilidad con el filtrado de FQDN, entre las que se incluyen:

- Configurar temporizadores de TTL para las entradas de DNS.
- Soporte con cargas de trabajo que se ejecutan en el hipervisor de KVM.

Se mejoraron las operaciones de firewall con las siguientes funciones:

- **Función para guardar configuración automáticamente y revertir:** el sistema crea una copia de la configuración cuando se publica. Esta configuración se puede volver a implementar para volver a un estado anterior.
- **Borradores manuales:** los usuarios ahora pueden guardar borradores de sus reglas antes de publicar esos conjuntos de reglas para su aplicación. Los usuarios pueden realizar copias intermedias de las reglas en los borradores manuales. El sistema permite que varios usuarios trabajen en el mismo borrador con un mecanismo de bloqueo para deshabilitar la anulación de reglas de diferentes usuarios.
- **Temporizadores de sesión:** los usuarios pueden configurar temporizadores de sesión para las sesiones TCP, UDP e ICMP.
- **Protección contra inundación:** tanto el firewall distribuido como el firewall de puerta de enlace pueden tener protección de SynFlood. Los usuarios pueden proporcionar umbrales para alertar, registrar y descartar el tráfico para convertirlo en flujos de trabajo personalizados.
- **El sistema genera automáticamente dos grupos** cuando se crea NSX LoadBalancer y se implementan servidores virtuales. Un grupo contiene el grupo de servidores mientras que el otro contiene la dirección IP del servidor virtual. Estos grupos se pueden utilizar en el firewall distribuido o el firewall de puerta de enlace para permitir o denegar el tráfico a los administradores del firewall. Estos grupos registran los cambios de configuración del equilibrador de carga de NSX.
- El número de direcciones IP detectadas por VM-vNIC se incrementó de 128 a 256.

Firewall de identidad

- NSX-T 2.5 admite los servidores de Active Directory implementados en Windows 2016.
- Se admite el firewall de identidades para cargas de trabajo de Windows Server sin servicios de terminal habilitados. Esto permitirá a los clientes controlar estrictamente el movimiento lateral de

los administradores de un servidor a otro.

Inserción de servicios

- **Compatibilidad con copia de paquetes:** además de redireccionar el tráfico a través de un servicio, NSX-T ahora es compatible con el caso práctico de supervisión de red, en el que una copia de los paquetes se reenvía a una máquina virtual de servicio de partners (SVM), lo que permite la inspección, la supervisión o la recopilación de las estadísticas mientras el paquete original no pasa a través del servicio de supervisión de red.
- **Implementación automática de SVM de partners basada en host:** a partir de NSX-T 2.5, se admiten dos modos de implementación de SVM de partners: implementación en clúster, en el que las máquinas virtuales de servicio se implementan en un clúster de vSphere (servicio) dedicado, y basado en host, en el que se implementa una máquina virtual de servicio por servicio en cada host informático de un clúster determinado. En este modo, cuando se agrega un nuevo host informático a un clúster, se implementan automáticamente las SVM correspondientes.
- **Compatibilidad con las notificaciones de inserción del servicio norte-sur:** NSX-T 2.4 introdujo el marco de notificación para la inserción del servicio de este a oeste, lo que permite que los servicios de partners reciban notificaciones automáticamente sobre los cambios relevantes, como el grupo dinámico actualizaciones. Con NSX-T 2.5, este marco de notificación también se ha ampliado a la inserción del servicio N-S. Los partners pueden aprovechar este mecanismo para permitir que los clientes usen grupos dinámicos de NSX (por ejemplo, según las etiquetas, el sistema operativo y el nombre de la máquina virtual) en la directiva de partners.
- **Características adicionales de solución de problemas y visualización:** con NSX-T 2.5, se han realizado varias mejoras de capacidad de servicio para permitir una mejor solución de problemas relacionados con la inserción de servicios. Esto incluye la capacidad de comprobar el estado en tiempo de ejecución de una instancia de servicio, la capacidad para obtener las rutas de servicio disponibles a través de la API, así como la inclusión de los registros relacionados con la inserción de servicios en el paquete de soporte.

Protección de endpoints (Guest Introspection)

- **Soporte de Linux:** compatibilidad con sistemas operativos basados en Linux con protección de endpoint. Consulte la guía de administración de NSX-T de los sistemas operativos Linux compatibles con Guest Introspection.
- **Panel de control de protección de endpoints:** para la visibilidad y la supervisión del estado de configuración de las máquinas virtuales protegidas y sin protección, problemas con el agente de host y las máquinas virtuales de servicio, y las máquinas virtuales configuradas con el controlador de introspección de archivo que se instaló como parte de VMware Tools.
- **Panel de control de supervisión:** para supervisar el estado de la implementación del servicio de partners en los clústeres del sistema.

Equilibrio de carga

- **API para recuperar el estado de la capacidad de Edge de los equilibradores de carga:** se agregaron nuevas llamadas de API para permitir que el admin supervise la capacidad de Edge en cuestión de instancias de equilibrio de carga.
- **Selección inteligente de la dirección IP de comprobación de estado:** cuando la lista de direcciones IP de SNAT está configurada, la primera dirección IP de la lista se utilizará para la supervisión de estado en lugar de la dirección IP de vínculo superior de una puerta de enlace de nivel 1. La dirección IP puede ser la misma que la dirección IP del servidor virtual. Esta mejora permite que el equilibrador de carga use una única dirección IP para la supervisión de estado y NAT de origen.
- **Mejora del registro del equilibrador de carga:** con esta mejora, el equilibrador de carga puede generar un mensaje de registro enriquecido por servidor virtual para supervisión. Por ejemplo, el registro de acceso al servidor virtual incluye no solo la dirección IP del cliente, sino también una dirección IP del miembro del grupo.
- **Mejora de persistencia en las reglas de LB:** se introdujo una nueva acción denominada "Persistir"

en las reglas de LB. La acción Persistir permite que el equilibrador de carga proporcione persistencia de aplicación en función de una cookie establecida por un miembro del grupo.

- **Ajuste de LB:** una instancia de LB pequeña puede ajustarse a una máquina virtual de Edge pequeña. Una instancia de LB de tamaño medio puede ajustarse a una máquina virtual de Edge mediana. Anteriormente, la máquina virtual de Edge pequeña no era compatible con los servicios de equilibrio de carga porque el tamaño de una máquina virtual de Edge tenía que ser mayor que el tamaño de una instancia de LB.
- **Estadísticas VS/grupo/miembro:** todas las estadísticas relacionadas con LB están disponibles en la interfaz simplificada. Anteriormente, la información solo estaba disponible en la interfaz avanzada de redes y seguridad.
- **Compatibilidad con ECC (certificado de curva elíptica) para la terminación de SSL:** los certificados EC se pueden utilizar para un mayor rendimiento de SSL.
- **Cumplimiento de FIPS:** existe una configuración global a través de la API para el cumplimiento de FIPS por parte de los equilibradores de carga. Esta opción está desactivada de forma predeterminada para mejorar el rendimiento.

VPN

- **Soporte de VPN de IPsec en la puerta de enlace de nivel 1:** la VPN de IPsec se puede implementar y terminar en una puerta de enlace de nivel 1 para mejorar la escalabilidad y el aislamiento de tenants. Anteriormente, solo se admitía en la puerta de enlace de nivel 0.
- **Compatibilidad de VLAN para la VPN de capa 2 en una instancia de Edge administrada por NSX:** esta mejora permite ampliar los segmentos respaldados por VLAN. Anteriormente, solo se admitían segmentos lógicos para la extensión de capa 2. Esto incluye soporte de la troncalización de VLAN, que permite ampliar varias VLAN en una interfaz Edge y en una sesión VPN de capa 2.
- **Fijación de MSS de TCP para la VPN de IPsec:** la compresión de MSS de TCP permite al administrador aplicar el valor de MSS de todas las conexiones TCP para evitar la fragmentación de paquetes.
- **Soporte de ECC (certificado de curva elíptica) para la VPN de IPsec:** el certificado EC es necesario para habilitar varias series de cumplimiento de IPsec, como CNSA, UK Prime, etc.
- **Botón fácil para la configuración de la suite de cumplimiento:** CNSA, Suite-B-GCM, Suite-B-GMAC, Prime, Foundation y FIPS pueden configurarse con un solo clic en la interfaz de usuario o una sola llamada API.

Automatización, OpenStack y otras CMP

- **Ampliación del soporte de la versión de OpenStack:** ahora incluye las versiones de Stein y Rocky.
- **Compatibilidad del complemento OpenStack Neutron con la API de directiva:** además del complemento actual, que admite la API de administración, ahora ofrecemos un complemento de OpenStack Neutron que consume la API de la directiva de NSX-T. Este complemento es compatible con IPv6 para capas 2 y 3, el firewall y SLAAC.
- **Optimización de enrutador de OpenStack Neutron:** el complemento ahora optimiza el enrutador de OpenStack Neutron administrando la creación o eliminación del enrutador de servicio de forma dinámica. Esto permite que un cliente tenga solo un enrutador distribuido cuando no hay servicios configurados, y uno en cuanto se agregan los servicios, todo administrado por el complemento.
- **Puente de capa 2 del complemento de OpenStack Neutron:** el puente de capa 2 configurado en OpenStack ahora está configurado en el clúster de Edge y no en el clúster ESXi.
- **Soporte de OpenStack Octavia:** además de LBaaSv2, el complemento de OpenStack Neutron admite Octavia como forma de usar el equilibrio de carga.
Para obtener más información, consulte las notas de la versión del complemento de VMware NSX-T Data Center 2.5 para OpenStack Neutron.

NSX Cloud

- **Nuevo modo de operación:** NSX Cloud ahora tiene dos modos de operación, lo que convierte oficialmente a NSX Cloud en la única solución de nube híbrida del mercado que admite los modos de funcionamiento con agente y sin agente.

- **Modo forzado de NSX (con agente):** proporciona un marco de directiva "consistente" entre las instalaciones y cualquier nube pública. La aplicación de la directiva de NSX se realiza con NSX Tools, que se instala en cada carga de trabajo. Esto proporciona granularidad a nivel de máquina virtual, y todas las máquinas virtuales etiquetadas estarán administradas por NSX. Este modo supera las diferencias y limitaciones de los proveedores de nube pública individuales y proporcionará un marco de directivas coherente entre la carga de trabajo de nube pública y local.
- **Modo de aplicación nativa en la nube (sin agente):** proporciona un marco de directivas "común" entre las instalaciones y cualquier nube pública. Este modo no requiere la instalación de NSX Tools en las cargas de trabajo. Las políticas de seguridad de NSX se convierten en las construcciones de seguridad de proveedores de nube nativas. Por lo tanto, se aplican todas las limitaciones de escalado y funciones de la nube pública seleccionada. La granularidad del control está en el nivel de VPC/VPNET, y todas las cargas de trabajo dentro de una VPC o VNET administrada serán administradas por NSX, a menos que esté en la lista blanca. Ambos modos proporcionan la pertenencia a grupos dinámicos y un amplio conjunto de abstracciones para los criterios de pertenencia a grupos de NSX.
- **Compatibilidad con la visibilidad y la seguridad de los servicios nativos de la nube pública desde NSX Cloud:** a partir de esta versión, será posible programar los grupos de seguridad de servicios SaaS nativos en Azure y AWS que tengan un endpoint de VPC/VNET local y un grupo de seguridad asociado con él. La idea principal es detectar y proteger los endpoints de servicio nativos de nube con reglas especificadas por el usuario en la directiva de NSX. Los siguientes servicios se admitirán en AWS (ELB, RDS y DynamoDB) y Azure (Azure Storage, Azure LB, Azure SQL Server y CosmosDB) en esta versión. Futuras versiones de NSX-T agregarán soporte para más servicios.
- **Nuevos sistemas operativos compatibles:**
 - Compatibilidad con Windows Server 2019
 - Windows 10 1809
 - Compatibilidad con Ubuntu 18.04
- **Directiva de cuarentena mejorada y lista blanca de VM:** a partir de NSX 2.5, NSX Cloud permite a los usuarios visualizar máquinas virtuales de la lista blanca desde la interfaz de CSM. En la lista blanca, NSX no administra los grupos de seguridad de nube de estas máquinas virtuales, y los usuarios pueden poner las máquinas virtuales en los grupos de seguridad de nube que deseen.
- **Informe de errores mejorado en la interfaz de CSM:** habilita la solución más rápida.

Operaciones

- **Compatibilidad con vSphere HA de NSX Manager:** el clúster de administración de NSX ahora se puede proteger mediante vSphere HA. Esto permite que se recupere un nodo del clúster de administración de NSX si se produce un error en el host que lo ejecuta. También permite que se recupere todo el clúster de administración de NSX en un sitio alternativo si se produce un error a nivel de sitio. Consulte la guía de instalación de NSX-T para obtener más información sobre los escenarios admitidos.
- **Mejoras del panel de capacidad:** las métricas nuevas y mejoradas del panel de capacidad muestran el número de objetos que configuró un cliente en relación con el máximo admitido en el producto. Para obtener una lista completa de los valores máximos de configuración de NSX-T Data Center, consulte la herramienta de valores máximos de configuración de VMware.
- **Soporte del modo de bloqueo de vSphere:** habilite más opciones de implementación para los clientes proporcionando la capacidad de instalar, actualizar y operar NSX-T en el modo de bloqueo de vSphere.
- **Mejora del registro:** se redujo el impacto del servicio durante la solución de problemas al habilitar el cambio dinámico de los niveles de registro a través de la interfaz de línea de comandos de NSX para los agentes de espacio del usuario de NSX.
- **Soporte de SNMPv3:** cumplimiento de seguridad mejorado al permitir configurar SNMPv3 para dispositivos de NSX Edge y Manager.
- **Nueva función de Traceflow para solucionar problemas de resolución de direcciones de máquinas virtuales:** ahora es posible inyectar paquetes ARP/NDP a través de Traceflow para detectar problemas de conectividad mientras se realiza la resolución de direcciones para un destino IP.

- **Cambio de orden de actualización:** al actualizar a NSX-T 2.5, los componentes de Edge se actualizan antes que los componentes del host. Esta mejora ofrece beneficios significativos al actualizar la infraestructura de nube, ya que permite que las optimizaciones reduzcan la ventana de mantenimiento general.
- **Mejora del paquete de contenido de Log Insight:** se agregó compatibilidad con las alertas de registro integradas con el nuevo paquete de contenido de NSX-T compatible con NSX-T 2.5.

Seguridad de la plataforma

- **FIPS:** ahora, los usuarios pueden generar informes de cumplimiento de FIPS, incluida la capacidad de configurar y administrar las implementaciones de NSX en modo conforme con FIPS. Los módulos criptográficos se validan según los estándares de FIPS, lo que ofrece garantía de seguridad para los clientes que deseen cumplir las regulaciones federales o que funcionen con NSX de forma segura y cumplen los estándares de FIPS prescritos. Con las excepciones indicadas, todos los módulos criptográficos de NSX-T 2.5 tienen la certificación FIPS. Para ver las certificaciones concedidas para los módulos validados por FIPS, consulte <https://www.vmware.com/security/certifications/fips.html>.
- **Mejoras en la administración de contraseñas:** los usuarios ahora pueden ampliar la duración de caducidad de contraseña (número de días) desde la última vez que se cambió la contraseña, incluso después de la actualización. Las notificaciones de caducidad de treinta días y las notificaciones de caducidad de contraseña aparecen ahora en la interfaz, la CLI y los syslog.

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 para VxRail y otras soluciones de host de proveedor de nube prescriben 4 pNIC de 10G con dos conmutadores de host. Un conmutador está dedicado a Edge y administración (VDS), mientras que el otro está dedicado a las máquinas virtuales de equipo (N-VDS). Dos conmutadores de host separan de forma efectiva el tráfico de administración del tráfico de equipos. Sin embargo, con la economía de tendencia de las NIC de 10 y 25G, muchos centros de datos y clientes de proveedores de nube pequeños están estandarizando el uso de hosts de dos pNIC. Con este factor de forma, los centros de datos y los clientes de los proveedores de nube pequeños pueden crear una solución basada en NSX-T con un solo N-VDS y alimentar todos los componentes con dos pNIC.

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

- **Mejoras en el coordinador de migración:** el coordinador de migración incluye varias mejoras de uso que mejoran el flujo de trabajo del proceso necesario para migrar de NSX Data Center for vSphere a NSX-T Data Center, incluidas mejoras para que usuarios proporcionen sus comentarios durante la migración.

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](#).

Cambios en el comportamiento general

Cambios en el puerto de comunicación del sistema NSX-T Data Center

A partir de NSX-T Data Center 2.5, el puerto TCP del canal de mensajería de NSX de todos los nodos de transporte y Edge a NSX Manager ha cambiado del puerto TCP 5671 al puerto 1234. Tras este cambio, asegúrese de que todos los nodos de transporte y Edge de NSX-T puedan comunicarse en el puerto TCP 1234 con NSX Manager y el puerto TCP 1235 con las instancias de NSX Controller antes de actualizar a NSX-T Data Center 2.5. Asegúrese también de mantener el puerto 5671 abierto durante el proceso de actualización.

Redes de Capa 2

Como resultado de las mejoras de los puentes de Capa 2, el puente ESXi quedará obsoleto. NSX-T incluía inicialmente la capacidad de dedicar un host ESXi como puente para extender un segmento superpuesto a una VLAN. Este modelo está obsoleto en esta versión porque el nuevo puente Edge lo reemplaza en lo que respecta a las funciones, no requiere un host ESXi dedicado y se beneficia de la ruta de acceso de datos optimizada del nodo de Edge. Consulte la sección de novedades para obtener más información.

Obsolescencias de la API y cambios del comportamiento

Las API de la plantilla del nodo de transporte están obsoletas en esta versión. En su lugar, se recomienda utilizar las API de perfiles del nodo de transporte. Puede consultar una lista de métodos y tipos obsoletos en la [guía de la API](#).

Recursos de CLI y API

Consulte 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**.

Idiomas disponibles

NSX-T Data Center se ha localizado a varios idiomas: inglés, alemán, francés, japonés, chino simplificado, coreano, chino tradicional y español. Como la localización de NSX-T Data Center utiliza la configuración de idioma del navegador, asegúrese de que la configuración coincida con el idioma deseado.

Historial de revisión del documento

19 de septiembre de 2019. Primera edición.

23 de septiembre de 2019. Se agregaron los problemas conocidos 2424818 y 2419246. Se agregaron los problemas resueltos 2364756, 2406018 y 2383328.

24 de septiembre de 2019. Elementos de novedades actualizados.

3 de octubre de 2019. Se agregó el problema resuelto 2313673.

12 de noviembre de 2019. Se agregaron los problemas conocidos 2362688 y 2436302. Se corrigió el problema 2282798 y se movió a la sección de problemas resueltos.

17 de diciembre de 2019. Se agregó el problema conocido 2444170.

14 de enero de 2020. Se agregó el problema resuelto 2399994.

18 de febrero de 2020. Se actualizó el problema conocido 2436302 con un vínculo a un artículo de la base de conocimientos.

14 mayo 2020. Se agregó el problema conocido 2467479.

25 de septiembre de 2020. Se agregó el problema conocido 2586606.

15 de marzo de 2021. Se agregó el problema conocido 2730634.

Problemas resueltos

- Problema solucionado 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.

- **Problema solucionado 2334442:** el usuario no tiene permiso para editar ni eliminar los objetos creados después de cambiar el nombre del usuario admin.
El usuario no tiene permiso para editar ni eliminar los objetos creados después de cambiar el nombre del usuario admin. No se puede cambiar el nombre de los usuarios admin/audit.
- **Problema solucionado 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.
- **Problema solucionado 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.
- **Problema solucionado 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.
- **Problema solucionado 2277742:** la invocación de PUT `https://<nsx-manager>/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://<nsx-manager>/api/v1/configs/management` no se puede invocar si hay un FQDN configurado.
- **Problema solucionado 2279249:** una 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.
- **Problema solucionado 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.
- **Problema solucionado 2268406:** el cuadro de diálogo de etiquetas de anclaje no muestra todas las etiquetas cuando se agrega un número máximo de etiquetas.
El cuadro de diálogo de etiquetas de anclaje no muestra todas las etiquetas cuando se agrega un número máximo de etiquetas y no se puede ni redimensionar ni desplazar. Sin embargo, el usuario puede ver todas las etiquetas en la página Resumen. No se pierde ningún dato.
- **Problema solucionado 2282798:** Se puede producir un error de registro del host cuando se intentan registrar demasiados hosts o solicitudes con NSX Manager de forma simultánea.

Este problema hace que el nodo de tejido se encuentre en un estado con ERRORES. La llamada API de estado del nodo de tejido muestra el mensaje "El cliente aún no respondió a ningún latido". El archivo `/etc/vmware/nsx-mpa/mpaconfig.json` del host también está vacío.

- **Problema solucionado 2383867:** se produce un error en la recopilación del paquete de registros para uno de los nodos del plano de administración.
El proceso de recopilación de registros genera un error al copiar el paquete de soporte en el servidor remoto.
- **Problema solucionado 2332397:** la API permite la creación de directivas de DFW en un dominio inexistente.
Tras crear una directiva de este tipo en un dominio inexistente, la interfaz deja de responder cuando el usuario abre una pestaña de seguridad de DFW. El registro relevante es `/var/log/policy/policy.log`.
- **Problema solucionado 2410818:** después de actualizar a la versión 2.4.2, los servidores virtuales creados en NSX-T 2.3.x pueden dejar de funcionar después de que se creen más servidores virtuales.
En algunas implementaciones, los servidores virtuales creados en la versión 2.3.x dejan de funcionar después de actualizar a la versión 2.4.2 y después de que se creen más servidores virtuales.
- **Problema solucionado 2310650:** la interfaz muestra el mensaje de error "Se agotó el tiempo de espera de la solicitud".
Varias páginas de la interfaz muestran el siguiente mensaje: "Se agotó el tiempo de espera de la solicitud. Esto puede ocurrir cuando el sistema está bajo carga o bajo la carga de recursos".
- **Problema solucionado 2314537:** el estado de la conexión es desactivado tras actualizar el certificado vCenter y la huella digital.
No se producirán errores en las nuevas actualizaciones de vCenter Sync con NSX y todas las consultas a pedido para obtener datos de vCenter. Los usuarios no pueden implementar nuevas máquinas virtuales de Edge o de servicio. Los usuarios no pueden preparar nuevos clústeres ni hosts agregados en vCenter. Ubicaciones de registro: `/var/log/cm-Inventory/cm-Inventory.log` y `/var/log/Proton/nsxapi.log` en el nodo de NSX Manager.
- **Problema solucionado 2316943:** la carga de trabajo se desprotegió brevemente durante vMotion.
VMware Tools tarda unos segundos en informar del nombre de equipo correcto para la máquina virtual después de vMotion. Como resultado, las máquinas virtuales agregadas a grupos NSGroups con el nombre de equipo se desprotegen durante unos segundos después de vMotion.
- **Problema solucionado 2318525:** las rutas IPv6 de salto siguiente como la dirección IP del mismo nivel de eBGP cambian a su propia IP.
En el caso de las sesiones de IP4 de eBGP, en las rutas IPv4 anunciadas que tienen el par eBGP como salto siguiente, el salto siguiente de la ruta NO se cambia en el lado remitente a su propia dirección IP. Esto funciona para IPv4, pero para las sesiones de IPv6, el salto siguiente de la ruta se cambia en el lado del remitente a su propia dirección IP. Este comportamiento puede producir bucles de rutas.
- **Problema solucionado 2320147:** VTEP falta en el host afectado.
Si se elimina un `LogSwitchStateMsg`, se agrega en la misma transacción y el plano de control central procesa esta operación antes de que el plano de administración envíe el conmutador lógico, el estado del conmutador lógico no se actualizará. Como resultado, el tráfico no puede fluir hacia ni desde el VTEP que falta.
- **Problema solucionado 2320855:** no se crea una nueva etiqueta de seguridad de máquina virtual si el usuario no hace clic en el botón Agregar/Comprobar.

Problema de interfaz. Si el usuario agrega una nueva etiqueta de seguridad a un inventario u objeto de directiva y hace clic en Guardar sin antes hacer clic en el botón **Agregar/Comprobar** situado junto al campo par Tag-Scope, no se crea el nuevo par de etiquetas.

- **Problema solucionado 2331683:** el formulario Agregar equilibrador de carga de la interfaz de usuario avanzada no muestra la capacidad actualizada de la versión 2.4.
Al abrir el formulario Agregar equilibrador de carga, la capacidad del factor de forma que se muestra en la interfaz de usuario avanzada no se actualiza a partir de la versión 2.4. La capacidad que se muestra pertenece a la versión anterior.
- **Problema solucionado 2295819:** el puente de Capa 2 se bloquea en el estado "Detenido" aunque la máquina virtual de Edge y la PNIC estén activas.
Es posible que el puente de Capa 2 se bloquee en el estado "Detenido" aunque la máquina virtual de Edge y la PNIC que respalda el puerto de puente de Capa 2 estén activas. Esto se debe a que Edge LCP no puede actualizar el estado de PNIC en la memoria caché local, por lo que se asume que la PNIC está inactiva.
- **Problema solucionado 2243415:** un cliente no puede implementar un servicio de EPP usando el conmutador lógico (como una red de administración).
En la pantalla de implementación de EPP, 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".
- **Problema solucionado 2364756:** se produce un error en la aplicación del perfil debido a una prioridad duplicada.
En las configuraciones a gran escala, cuando el usuario asocia vRNI con NSX IPFIX, el perfil no se aplica en el plano de administración y se producen errores de aplicación.
- **Problema solucionado 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.
- **Problema solucionado 2307551:** El host NSX-T puede perder la conectividad de la red de administración al migrar todos los pNIC al N-VDS.
El problema se debe a que la migración del host vuelve a intentar eliminar todos los pNIC en el N-VDS que tiene vmkO configurado. La primera migración del host migró todos los pNIC y vmkO al N-VDS, pero se produjo un error después. Al volver a intentar la migración, se eliminan todos los pNIC del N-VDS. Como resultado, los usuarios no pueden acceder al host a través de la red; todas las máquinas virtuales del host también pierden conectividad de red, por lo que no se puede procesar sus servicios.
- **Problema solucionado 2369792:** El proceso de CBM se bloquea de forma repetida debido a la saturación de la memoria del proceso de CBM.
Los procesos de CSM y CBM en el dispositivo de Cloud Service Manager no compactan la base de datos. Como resultado, la saturación de la memoria del proceso de CBM hace que el proceso de CMB se bloquee repetidamente.
- **Problema solucionado 2361892:** el dispositivo de NSX Edge experimenta una fuga de memoria, lo que provoca un bloqueo/reinicio del proceso.
Durante un período de tiempo prolongado, el dispositivo de NSX Edge puede experimentar una pérdida de memoria debido a la búsqueda de reglas repetidas, lo que provoca un error en el proceso de bloqueo/reinicio. Se detectó una fuga de memoria cada vez que se ejecutó una búsqueda de regla. Cuando se borra la memoria caché de flujo, no se elimina la interfaz VIF, lo que provoca una acumulación en la memoria.
- **Problema solucionado 2364529:** Fuga de memoria del equilibrador de carga después de la reconfiguración.

Puede que el equilibrador de carga de NSX sufra una fuga de memoria cuando se producen eventos de configuración consecutivos/repetidos, provocando el volcado de núcleo del proceso nginx.

- **Problema solucionado 2378876: PSOD en los hosts ESXi con los errores "Error de uso en dlmalloc" y "Excepción de PF 14 en world 3916803:VSIP PF Purg IP".**
ESXi se bloqueó (PSOD) después de ejecutar el tráfico durante unos días. No se observó ningún otro síntoma antes del bloqueo. El problema se identificó finalmente en el tráfico de ALG (FTP, SunRPC, Oracle, DCERPC, tftp), donde el contador de incrementos no atomizados provocó condiciones de carrera, dañando la estructura del árbol de ALG.
- **Problema solucionado 2384922: BGPD consume el 100 % del uso de CPU en el nodo de Edge.**
El proceso de BGPD en la instancia de Edge de NSX-T puede consumir el 100 % de la CPU cuando tiene varias sesiones abiertas con VTYSH.
- **Problema solucionado 2386738: las reglas NAT se omitieron en el tráfico a través del puerto vinculado.**
Los servicios NAT no están habilitados en el tipo de puerto de enrutador vinculado que conecta los enrutadores lógicos de nivel 0 y nivel 1.
- **Problema solucionado 2363618: Los usuarios de VMware Identity Manager no pueden acceder a las páginas de directivas en el panel de control de NSX Manager.**
Los usuarios con funciones asignadas a permisos de grupo en VMware Identity Manager no pueden acceder a las páginas de directivas en el panel de control de NSX Manager. Los permisos de la asignación de grupo se ignoran.
- **Problema solucionado 2298274: el grupo de directivas se puede crear o actualizar con un nombre de dominio no válido o parcial a través de REST API.**
La interfaz permitió la creación de grupos con expresiones de identidad que contienen un grupo de Active Directory no válido o miembros de grupos individuales para un solo contenido válido. Sin embargo, cada miembro solo es válido si tiene exactamente un grupo de LDAP asociado al nombre de dominio. Como resultado, en dichos grupos creados en una versión anterior de NSX-T, este error no se marcarán en el proceso de actualización, lo que permite que los grupos no válidos persistan en las versiones posteriores. Problema solucionado en la versión 2.5.
- **Problema solucionado 2317147: los usuarios no pueden ver las máquinas virtuales efectivas de un grupo cuya pertenencia se basa en direcciones IP o MAC.**
Si un usuario crea un grupo que solo contiene direcciones IP o MAC en el grupo, no se incluirá ninguna máquina virtual cuando se llame a la pertenencia efectiva de ese grupo desde la API. El funcionamiento no se ve afectado. La directiva crea correctamente un grupo NSGroup en el plano de administración, y la lista de direcciones IP y MAC se envía directamente al plano de control central.
- **Problema solucionado 2327201: las actualizaciones de las máquinas virtuales en hipervisores de KVM no se sincronizan inmediatamente.**
Las actualizaciones de máquina virtual en hipervisores de KVM pueden tardar un par de horas en sincronizarse en NSX-T. Como resultado, no se pueden agregar nuevas máquinas virtuales creadas en hipervisores de KVM a NSGroups y no se pueden aplicar reglas de firewall en dichas máquinas virtuales. No se puede actualizar el hipervisor de KVM porque el estado de energía de la máquina virtual no se ha actualizado.
- **Problema solucionado 2329443: no se ha inicializado el clúster de control debido al tiempo de espera de forcesync.**
El clúster de control no se está inicializando debido a un tiempo de espera de forcesync cuando el rango de IPV4 en Ipset empieza en 0.0.0.0 (por ejemplo 0.0.0.0-1.1.1.20). Esto se debe a un problema en el IPSetFullSyncMessageProvider, que se bloquea en un bucle infinito. Como el plano de control central no se inicia, los usuarios no pueden implementar nuevas cargas de trabajo.
- **Problema solucionado 2337839: los widgets de copia de seguridad de NSX-T muestran**

nombres de campo incorrectos.

Específicamente, los widgets de copia de seguridad de NSX-T no muestran el número correcto de errores de copia de seguridad. Como resultado, el cliente debe revisar la pestaña de copia de seguridad de NSX Manager para ver el recuento exacto de los errores de copia de seguridad.

- **Problema solucionado 2341552: Edge no arranca cuando el sistema tiene demasiadas NIC admitidas.**
No se puede ver ningún servicio o conectividad de la ruta de acceso, el servicio de la ruta de acceso está inactivo y el nodo de Edge se encuentra en estado degradado. Esto da como resultado una pérdida de conectividad parcial o total si la instancia de Edge es obligatoria.
- **Problema solucionado 2390374: NSX Manager se vuelve muy lento o deja de responder, y los registros muestran muchas excepciones de corfu.**
También es posible que NSX no se inicie. Las excepciones de corfu indican que la escala de los miembros de Active Directory es demasiado grande y supera los límites probados.
- **Problema solucionado 2371150: no se pueden configurar las reglas de firewall de capa 7 en los nodos de Edge sin sistema operativo.**
Las reglas de firewall de capa 7 en nodos de Edge sin sistema operativo no se admiten en NSX-T 2.5. Hay un comando interno que permiten estas reglas, pero solo está disponible para las pruebas de concepto.
- **Problema solucionado 2361238: el enrutador de vínculo inferior no se empareja con el enrutador de servicios.**
Las reglas NAT no surten efecto en el enrutador de vínculo inferior después de que un enrutador de servicios que se haya emparejado con un enrutador de vínculo inferior se volviera a crear después de eliminarse.
- **Problema solucionado 2363248: el estado de mantenimiento de la instancia de servicio en la interfaz aparece inactivo, aunque la llamada API se muestra conectada.**
Este informe inconsistente puede provocar una falsa alarma.

Este problema y la solución se describen de forma más detallada en el [artículo 67165 de la base de conocimientos: El estado de la instancia del servicio se muestra como inactivo cuando no hay máquinas virtuales que proteger en NSX-T](#).
- **Problema solucionado 2359936: los registros de cfgAgent se acumulan con frecuencia en el host ESX.**
Acumular registros con frecuencia puede conllevar la pérdida de información útil en cfgAgent.log para depurar hosts y solucionar problemas relativos a estos.
- **Problema solucionado 2332938: cuando la memoria caché SYN está habilitada en el perfil de seguridad de la protección de inundación, el límite de conexiones semiabiertas TCP real puede ser mayor que el que está configurado en la NSX Manager.**
NSX-T calcula automáticamente un límite óptimo de conexiones semiabiertas de TCP en función del límite configurado. Este límite calculado puede ser mayor que el límite configurado y se basa en la fórmula Límite = (Potencia de 2 * Profundidad), donde la potencia de 2 no puede ser inferior a 64 y la profundidad debe ser un número entero menor o igual que 32.
- **Problema solucionado 2376336: la familia de direcciones en la redistribución de rutas no es compatible con la directiva y con Edge.**
La familia de direcciones en la redistribución no funciona o no se utiliza en la aplicación.
- **Problema solucionado 2412842: limita los registros de métricas a 40 MB en ESX para admitir hosts con ramdisk.**
Este problema se aborda con detalle en el [artículo 74574 de la base de conocimientos](#).
- **Problema solucionado 2385070: la detección de IP y DFW tienen comportamientos opuestos relacionados con la subred IPv6.**

La detección de direcciones IP considera 2001::1/64 como una IP de host, mientras que DFW la considera una subred IPv6.

- **Problema solucionado 2394896:** el host no se puede actualizar de NSX-T Data Center 2.4.x a 2.5.

El host no se puede actualizarse de NSX-T Data Center 2.4.0, 2.4.1 y 2.4.2 a la versión 2.5. Esto puede deberse a un error de descarga del módulo KCP.

Este problema se describe con mayor detalle en el [artículo 74674 de la base de conocimientos](#).

- **Problema solucionado 2406018:** se activa un evento o una alarma si la contraseña va a caducar en los próximos 30 días.

Se activa un evento o una alarma en relación con la caducidad de la contraseña si esta va a caducar en los próximos 30 días, aunque la caducidad de la contraseña esté deshabilitada.

- **Problema solucionado 2383328:** solicitud de una utilidad que represente los datos de las métricas en lenguaje natural.

NSX-T Data Center recopila y guarda los datos de las métricas en formato binario; los usuarios han solicitado poder ver estos datos en lenguaje natural. Este problema hace un seguimiento de esa solicitud.

- **Problema solucionado 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.

- **Problema solucionado 2313673 (nodos de transporte de Edge basados en máquinas virtuales):** los usuarios no pueden conectar vínculos superiores a segmentos/conmutadores lógicos de NSX-T.

Para los nodos de transporte de Edge basados en máquinas virtuales, los usuarios no pueden conectar vínculos superiores de nodos de transporte de Edge a segmentos/conmutadores lógicos de NSX-T. Solo pueden conectarlos al DVPG de vCenter. En la pantalla Configurar NSX de los flujos para agregar/editar nodos de transporte de Edge basados en máquinas virtuales, se presenta a los usuarios la opción de asignar los vínculos superiores solo con el DVPG de vCenter. Falta la opción para asignar los vínculos superiores a los segmentos/conmutadores lógicos de NSX-T.

- **Problema solucionado 2424394:** los paquetes DHCP retransmitidos por el DR de NSX-T no pueden alcanzar más de 10 saltos.

Cuando el servidor DHCP está a más de 10 saltos, los paquetes DHCP retransmitidos no pueden acceder al servidor.

- **Problema solucionado 2399994:** las rutas redistribuidas faltan de forma intermitente.

El tráfico de red puede verse afectado, ya que la ruta al nivel 1 no está disponible durante algún tiempo.

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 del equilibrador de carga](#)
- [Problemas conocidos de interoperabilidad de soluciones](#)
- [Problemas conocidos de NSX Intelligence](#)
- [Problemas conocidos de las operaciones y los servicios de supervisión](#)

- [Problemas conocidos de actualización](#)
- [Problemas conocidos de la API](#)
- [Problemas conocidos de NSX Cloud](#)

Problemas conocidos generales

- **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.

- **Problema 2390624:** La regla de antiafinidad evita que la máquina virtual de servicio use el proceso de vMotion cuando el host está en modo de mantenimiento.
Si se implementa una máquina virtual de servicio en un clúster con dos hosts exactamente, el par de HA con la regla de antiafinidad evitará que las máquinas virtuales usen el proceso vMotion con el otro host durante cualquier tarea del modo de mantenimiento. Esto puede impedir que el host entre en modo de mantenimiento automáticamente.

Solución alternativa: Apague la máquina virtual de servicio en el host antes de que se inicie la tarea del modo de mantenimiento en vCenter.

- **Problema 2329273:** no existe conectividad entre redes VLAN conectadas al mismo segmento por el mismo nodo de Edge.
No puede conectar un segmento con puente dos veces en el mismo nodo de Edge. Sin embargo, es posible conectar dos VLAN al mismo segmento en dos nodos Edge diferentes.

Solución alternativa: Ninguno

- **Problema 2239365:** se muestra el 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 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 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 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 2320529:** Se produjo el error "La implementación del servicio no puede acceder al almacenamiento proporcionado" tras agregar máquinas virtuales de terceros a almacenes de datos recién agregados.

Se produjo el error "La implementación del servicio no puede acceder al almacenamiento proporcionado" tras agregar máquinas virtuales de terceros a almacenes de datos recién agregados, aunque se pueda acceder al almacenamiento desde todos los hosts del clúster. Este estado de error persiste durante un máximo de treinta minutos.

Solución alternativa: Vuelva a intentarlo después de treinta minutos. Como alternativa, realice la siguiente llamada API para actualizar la entrada de la memoria caché del almacén de datos:

https://<nsx-manager>/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?uniform_cluster_access=true&source=realtime

donde <nsx-manager> es la dirección IP de NSX Manager en la que se produjo un error en la API de implementación de servicio y donde CC Ext ID es el identificador en NSX del clúster en el que se intenta la implementación.

- **Problema 2328126:** Sin sistema operativo: La interfaz de enlace del sistema operativo Linux devuelve el error cuando se utiliza en el perfil de vínculo superior de NSX.

Al crear una interfaz de enlace en el sistema operativo Linux y, a continuación, utilizar esta interfaz en el perfil de vínculo superior de NSX, aparece este mensaje de error: "La creación del nodo de transporte puede generar un error". Este problema se produce porque VMware no admite la vinculación del sistema operativo Linux. Sin embargo, VMware es compatible con la vinculación Open vSwitch (OVS) para los nodos de transporte de servidor sin sistema operativo.

Solución alternativa: Si surge este problema, consulte el artículo 67835 de la base de conocimientos [El servidor sin sistema operativo admite vinculación OVS para la configuración del nodo de transporte en NSX-T](#).

- **Problema 2370555:** el usuario puede eliminar ciertos objetos de la interfaz avanzada, pero esas eliminaciones no se reflejan en la interfaz simplificada.

Específicamente, los grupos que se agregan como parte de una lista de exclusión del firewall distribuido se pueden eliminar en la configuración avanzada de la lista de exclusión del firewall distribuido de la interfaz. Esto provoca un comportamiento inconsistente en la interfaz.

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

- Añada un objeto a una lista de exclusión en la interfaz simplificada.
- Compruebe que aparece en la lista de exclusión del firewall distribuido en la interfaz avanzada.
- Elimine el objeto de la lista de exclusión del firewall distribuido en la interfaz avanzada.
- Vuelva a la interfaz simplificada, agregue un segundo objeto a la lista de exclusión y aplíquela.
- Compruebe que el nuevo objeto aparece en la interfaz avanzada.
- **Problema 2377217:** después del reinicio del host KVM, es posible que los flujos de tráfico entre las máquinas virtuales no funcionen según lo esperado.

El reinicio del host KVM puede provocar problemas de disponibilidad entre las máquinas virtuales.

Solución alternativa: Después de reiniciar el host, reinicie el servicio NSX-Agent con el siguiente comando:

```
# systemctl restart nsx-agent.service
```

- **Problema 2371251:** la interfaz del panel parpadea cuando se accede a la página Copia de seguridad y restauración.
- Esto se observó solo en el navegador Firefox y en algunas implementaciones.

Solución alternativa: Actualice la página de forma manual o utilice otro navegador compatible.

- **Problema 2408453:** VMware Tools 10.3.5 se bloquea cuando el controlador de NSX Guest Introspection está instalado.
- VMware Tools 10.3.5 se bloquea de forma irregular en máquinas virtuales Windows, de forma más evidente cuando la sesión remota está desconectada o la máquina virtual invitada se está apagando.

Solución alternativa: Consulte el [artículo 70543 de la base de conocimientos](#) para obtener más información.

- **Problema 2267964:** si se elimina vCenter, no se advierte al usuario de la pérdida de servicios que se ejecutan en vCenter.
- Si un usuario elimina el administrador de equipos (vCenter) en el que se implementan servicios como Guest Introspection, no se notifica al usuario acerca de la posible pérdida de estos servicios.

Solución alternativa: Este problema puede evitarse si el usuario sigue el procedimiento correcto para agregar una nueva instancia de vCenter como administrador de equipos.

- **Problema 2444170:** Los comandos de la CLI de NSX no pueden desinstalar la ruta de acceso
- El comando `del nsx` no desinstala la configuración de NSX-T y los módulos del host. Esto hace que se produzca un error al instalar o actualizar NSX-T.

Solución alternativa: Ninguna.

- **Problema 2467479:** una vez que el firewall está configurado para omitir una regla SNAT, no se puede bloquear después de cambiar de Omitir a Ninguno.
Una vez que el firewall está configurado para omitir una regla SNAT, no se puede bloquear después de cambiar de Omitir a Ninguno.

Solución alternativa: Elimine y vuelva a crear la regla SNAT.

- **Problema 2586606:** El equilibrador de carga no funciona cuando la persistencia de IP de origen está configurada en un número elevado de servidores virtuales.
Cuando la persistencia de IP de origen está configurada en un número elevado de servidores virtuales en un equilibrador de carga, consume una cantidad significativa de memoria y puede hacer que NSX Edge se quede sin memoria. Sin embargo, el problema puede volver a ocurrir al agregar más servidores virtuales.

Solución alternativa: Deshabilite la persistencia de IP de origen o mueva las VIP con persistencia de IP de origen a otros servicios del equilibrador de carga.

- **Problema 2730634:** La página del componente de red posterior a la actualización de unidifusión muestra el error "El índice está fuera de sincronización".
La página del componente de red posterior a la actualización de unidifusión muestra el error "El índice está fuera de sincronización".

Solución alternativa: Inicie sesión en NSX Manager con las credenciales de admin y ejecute el comando "start search resync policy". Los componentes de red tardarán unos minutos en cargarse.

Problemas conocidos de instalación

- **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.

Problemas conocidos de NSX Manager

- **Problema 2378970:** el ajuste Habilitar/deshabilitar en el nivel de clúster para el firewall distribuido se muestra incorrectamente como deshabilitado.
El ajuste Habilitar/Deshabilitar en el nivel de clúster para IDFW en la interfaz de usuario simplificada puede mostrarse como Deshabilitado aunque esté habilitado en el plano de administración. Después de actualizar de 2.4.x a 2.5, esta imprecisión persistirá hasta que se cambie de forma explícita.

Solución alternativa: Modifique manualmente la opción Habilitar/Deshabilitar para IDFW en la interfaz de usuario simplificada para que coincida con la del plano de administración.

Problemas conocidos de NSX Edge

- **Problema 2283559:** las API de MP <https://<nsx-manager>/api/v1/routing-table> y <https://<nsx-manager>/api/v1/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.
- **Problema 2204932:** La configuración del emparejamiento BGP puede retrasar la recuperación de conmutación por error de HA.
Si el emparejamiento BGP dinámico se configura en los enrutadores que se unen con las instancias de Edge de nivel 0 y se produce una conmutación por error en las mismas (modo activo-en espera), la vecindad BGP puede tardar hasta 120 segundos.

Solución alternativa: Configure los pares de BGP específicos para evitar el retraso.

- **Problema 2285650:** Las tablas de enrutamiento BGP se rellenan con rutas no deseadas.
Cuando la opción `allowas-in` está habilitada como parte de la configuración de BGP, las rutas anunciadas por los nodos de Edge se vuelven a recibir y se instalan en la tabla de enrutamiento de BGP. Esto da lugar a un consumo excesivo de memoria y el procesamiento de cálculo de enrutamiento. Si se configura una prioridad local mayor para las rutas sobrantes, este bucle de reenvío puede hacer que la tabla de enrutamiento de algunos enrutadores se rellene con rutas redundantes.

Por ejemplo, la ruta X se origina en el enrutador D, que se anuncia a los enrutadores A y B. El enrutador C, en el que `allowas-in` está habilitado, está emparejado con B, de modo que aprende la ruta X y la instala en la tabla de enrutamiento. Como resultado, ahora hay dos rutas para que la ruta X se anuncie en el enrutador C, lo que está generando el problema.

Solución alternativa: Para evitar los bucles de reenvío, configure el enrutador problemático (o el del mismo nivel) para bloquear las rutas que se anuncien.

- **Problema 2343954:** la interfaz de endpoint de puente de Capa 2 de Edge permite la configuración de rangos de VLAN no admitidos.
La interfaz de configuración de endpoint y de puente de Capa 2 de Edge permite configurar el rango de VLAN y varios rangos de VLAN aunque no se admitan.

Solución alternativa: No configure estos rangos de VLAN para el puente de Capa 2 de Edge y la configuración de endpoints.

Problemas conocidos de las redes lógicas

- **Problema 2389993:** El mapa de rutas se eliminó después de modificar la regla de redistribución mediante la API o la página de la directiva.
Un mapa de rutas agregado a una regla de redistribución desde la API o la interfaz del plano de administración se podría eliminar si la misma regla de redistribución se modifica posteriormente a través de la API o la interfaz de la página de la directiva. Esto se debe a que la API o la interfaz de la página de la directiva no permiten añadir mapas de rutas. Esto puede dar como resultado un anuncio de los prefijos no deseados para el par BGP.

Solución alternativa: Puede restaurar el mapa de rutas devolviendo la API o la interfaz del plano de administración para volver a agregarlo a la misma regla. Si desea incluir un mapa de rutas en una regla de redistribución, se recomienda crearlo y modificarlo siempre con la API o la interfaz del plano de administración.

- **Problema 2275412:** la conexión del puerto no funciona en varios TZ.
La conexión de puerto solo se puede utilizar en una única zona de transporte.

Solución alternativa: Ninguna.

- **Problema 2327904:** Después de usar la interfaz de enlace de Linux creada previamente como un vínculo superior, el tráfico es inestable o tiene errores.
NSX-T no es compatible con las interfaces de enlace de Linux creadas previamente como vínculo superior.

Solución alternativa: Para el vínculo superior, utilice la configuración de enlace nativo de OVS del perfil de vínculo superior.

- **Problema 2304571:** Es posible que se produzca un error crítico (PSOD) al ejecutar tráfico de Capa 3 mediante VDR.
La entrada ARP (ND) pendiente no está protegida correctamente en algunos casos, lo que puede provocar un error crítico (PSOD).

Solución alternativa: Ninguna.

- **Problema 2388158:** el usuario no puede editar la configuración de la subred de tránsito en la configuración del enrutador lógico de nivel 0.
Después de crear el enrutador lógico de nivel 0, la configuración de subred de tránsito no se puede modificar en la interfaz de NSX Manager.

Solución alternativa: Ninguna. La mejor opción es eliminar el enrutador lógico y volver a crearlo con la configuración de subred de tránsito deseada.

Problemas conocidos de los servicios de seguridad

- **Problema 2294410:** El firewall de Capa 7 detecta algunos identificadores de aplicación.
Los siguientes identificadores de aplicación de Capa 7 se detectan en función del puerto, no de la aplicación: SAP, SUNRPC y SVN. No se admiten los siguientes identificadores de aplicación de Capa 7: AD_BKUP, SKIP y AD_NSP.

Solución alternativa: Ninguna. El cliente no se ve afectado.

- **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 2366599:** no se aplican reglas para máquinas virtuales con direcciones IPv6.
Si una máquina virtual utiliza una dirección IPv6, pero no se ha habilitado la intromisión IPv6 para esa VIF a través del perfil de detección de IP, la dirección IPv6 no se rellena en la regla de esa máquina virtual en la ruta de datos. Como resultado, esa regla nunca se aplica.

Solución alternativa: Compruebe que la opción IPv6 del perfil de IPDiscovery está habilitada en el conmutador lógico o el VIF cuando se utilizan direcciones IPv6.

- **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 2379632:** se registran varios paquetes al alcanzar la regla de capa 7 en la etapa clasificada.
Se registran 2-3 paquetes (dfwpktlogs) al alcanzar la regla de capa 7 en la etapa clasificada.

Solución alternativa: Ninguna.

- **Problema 2368948:** reglas de firewall distribuido Es posible que el estado realizado de las secciones individuales no esté actualizado.
Al actualizar la vista de reglas de DFW, no se actualiza el estado realizado de las secciones individuales en esa vista. Como resultado, es posible que la información no esté actualizada.

Solución alternativa: Esto afecta solo la actualización manual. El sondeo del estado realizado es periódico y proporciona actualizaciones precisas. Los usuarios también pueden actualizar secciones individuales para obtener un estado preciso.

- **Problema 2380833:** la publicación del borrador de la política con 8000 o más reglas requiere mucho tiempo.

Un borrador de directivas que contiene 8000 o más reglas puede tardar una cantidad considerable de tiempo en publicarse. Por ejemplo, un borrador de directivas con 8000 reglas puede tardar 25 minutos en publicarse.

Solución alternativa: Ninguna.

- **Problema 2424818:** los estados del firewall distribuido y de Capa 2 no se actualizan en la interfaz de NSX Manager.

Es posible que la información de estado generada por el exportador lógico en máquinas virtuales de carga de trabajo no se reenvíe al plano de administración. Como resultado, los estados de estos componentes no se actualizan correctamente.

Solución alternativa: Ninguna. Se puede acceder a la información de estado correcta a través de la CLI en las máquinas virtuales correspondientes.

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 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 fallar.

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.

- **Problema 2401715:** error al actualizar el administrador de equipos, que indica que la huella digital no es válida, aunque se proporcione la huella digital correcta.

Se observa cuando se agrega una instancia de vCenter 6.7U3 como administrador de equipos en NSX-T Manager. vSphere 6.7 admite el cambio de PNID en los que se puede cambiar el FQDN o la dirección IP. NSX-T 2.5 no admite esta función, motivo por el que se produce el problema de la huella digital.

Solución alternativa: Elimine la versión de vCenter agregada previamente y agregue el VC con el FQDN que cambió recientemente. Es posible que se produzca un error al agregar el registro, ya que la extensión anterior ya existe en vCenter. Resuelva los errores de registro para que se registre correctamente.

Problemas conocidos de NSX Intelligence

- **Problema 2410806:** se produce un error en la recomendación de publicación generada con una excepción que hace referencia al límite total de 500.

Si el número total de miembros (direcciones IP o máquinas virtuales) en un grupo recomendado supera los 500, la publicación de la recomendación generada en una configuración de directiva mostrará el mensaje de excepción "El total de expresiones de direcciones IP, expresiones de direcciones MAC, rutas de acceso en una expresión de rutas de acceso e identificadores externos en una expresión de identificadores externos no debe ser superior a 500".

Solución alternativa: Si alguna vez se conectan más de 500 clientes al equilibrador de carga o a la máquina virtual de la aplicación, puede crear una regla para microsegmentar el acceso al equilibrador de carga de la aplicación y, a continuación, seleccionar las máquinas virtuales de aplicaciones para iniciar la detección de recomendaciones. En la alternativa, puede subdividir el grupo de más de 500 miembros en varios grupos más pequeños.

- **Problema 2362865:** el filtro por nombre de regla no está disponible para la regla predeterminada.

Se observó en la página Planificar y solucionar problemas > Descubrir y realizar acción y solo afecta a las reglas creadas por la estrategia de conectividad. Este problema se debe a la ausencia de una directiva predeterminada basada en la estrategia de conectividad especificada. Se puede crear una regla predeterminada en el plano de administración, pero sin una directiva predeterminada correspondiente, el usuario no puede filtrar por dicha regla predeterminada. (El filtro de visualización de flujos utiliza el nombre de la regla para filtrar por los flujos que han alcanzado esa regla.)

Solución alternativa: No aplique un filtro de nombre de regla. En su lugar, compruebe la marca Sin protección. Esta configuración incluirá los flujos que se alcanzan con la regla predeterminada, así como cualquier regla para la que se haya especificado un origen y un destino "cualquiera".

- **Problema 2368926:** el trabajo de recomendaciones genera un error si el usuario reinicia el dispositivo mientras el trabajo está en curso.

Si el usuario reinicia el dispositivo NSX Intelligence mientras hay una tarea de recomendaciones en curso, el trabajo pasa a un estado de error. Un usuario puede iniciar una tarea de recomendación para un conjunto de máquinas virtuales de contexto. El reinicio elimina el contexto y, como resultado, el trabajo falla.

Solución alternativa: Después del reinicio, repita el trabajo de recomendaciones para el mismo conjunto de máquinas virtuales.

- **Problema 2385599:** no se admiten grupos de IP estáticas en las recomendaciones de inteligencia de NSX-T.

Las máquinas virtuales y las cargas de trabajo que no se reconocen en el inventario de NSX-T, si tienen direcciones IP de intranet, pueden seguir estando sujetas a la recomendación como un grupo de direcciones IP estáticas, incluida la recomendación de definición de reglas que contienen estos grupos. Sin embargo, NSX Intelligence no admite estos grupos y, como resultado, la visualización muestra el tráfico que se les envía como enviados a "Desconocido" en lugar del grupo recomendado.

Solución alternativa: Ninguna. Sin embargo, la recomendación funciona correctamente. Este problema solo afecta a la visualización.

- **Problema 2374231:** para los flujos de protocolo SCTP, GRE y ESP, el servicio se muestra como desconocido y el puerto como 0.

NSX Intelligence no admite el análisis de puertos de origen o de destino para los flujos de protocolos SCTP, ESP y GRE. NSX Intelligence proporciona un análisis de encabezado completo para los flujos de TCP y UDP junto con las estadísticas relacionadas con el flujo. Para otros protocolos admitidos (como GRE, ESP y SCTP) NSX Intelligence solo puede proporcionar información de IP sin puertos de origen o de destino específicos del protocolo. Para estos protocolos, el puerto de origen o de destino será cero.

Solución alternativa: Ninguna.

- **Problema 2374229: el dispositivo de NSX Intelligence se queda sin espacio en disco.**

El dispositivo de NSX Intelligence tiene un período de retención de datos predeterminado de 30 días. Si la cantidad de datos de flujo es mayor que la cantidad prevista de 30 días, el dispositivo puede quedarse sin espacio de disco de forma prematura y pasar a estar parcial o completamente no operativo.

Solución alternativa: Esto puede evitarse o mitigarse supervisando el uso de disco del dispositivo de NSX Intelligence. Si el uso del disco se está utilizando a una velocidad elevada que indica que es posible que se agote el espacio, puede modificar el período de retención de datos a un número de días inferior.

1. Ejecute SSH en el dispositivo de NSX Intelligence y acceda al archivo `/opt/vmware/pace/druid-config/druid_data_retention.properties`.
2. Busque y cambie el ajuste `correlated_flow` a un valor inferior a 30 días. Por ejemplo: `correlated_flow=P14D`
3. Guarde el archivo y aplique los cambios ejecutando el siguiente comando:
`/opt/vmware/pace/druid-config/druid-config-data-retention.sh`
NOTA: Es posible que se necesiten hasta dos horas para que los datos se eliminen físicamente.

- **Problema 2389691: el trabajo de recomendación de la publicación genera el error "el tamaño de la carga útil de solicitud supera el límite permitido; se permiten hasta 2000 objetos por solicitud."**

Si intenta publicar un solo trabajo de recomendación que contenga más de 2000 objetos, se producirá un error "el tamaño de la carga útil de solicitud supera el límite permitido; se permiten hasta 2000 objetos por solicitud".

Solución alternativa: Reduzca el número de objetos a un máximo de 2000 en el trabajo de la recomendación y vuelva a intentar la publicación.

- **Problema 2376389: las máquinas virtuales se marcan de forma incorrecta como eliminadas en la vista de 'Últimas 24 horas' en la configuración de nivel medio.**

Después de desconectar o quitar un nodo de transporte del administrador de recursos informáticos, NSX Intelligence muestra las máquinas virtuales anteriores como eliminadas, con nuevas máquinas virtuales en su lugar. Este problema se produce por las actualizaciones de inventario de seguimiento de NSX Intelligence en la base de datos de NSX, y este comportamiento refleja el modo en que el inventario controla la desconexión del nodo de transporte del administrador de equipos. Esto no afecta el recuento total de máquinas virtuales activas en NSX Intelligence, aunque es posible que vea máquinas virtuales duplicadas en NSX Intelligence.

Solución alternativa: No se requiere ninguna acción. Las máquinas virtuales duplicadas se terminan eliminando de la interfaz en función del intervalo de tiempo seleccionado.

- **Problema 2393240: se observan flujos adicionales de la máquina virtual a la dirección IP.**

El cliente ve flujos adicionales de la máquina virtual a la dirección IP-xxxx. Esto se debe a que los datos de configuración (grupos, máquinas virtuales y servicios) de NSX Policy Manager llegan al dispositivo de NSX Intelligence después de crear el flujo. Por lo tanto, el flujo (anterior) no se puede correlacionar con la configuración, ya que no existe desde la perspectiva del flujo. Dado que el flujo no se puede correlacionar normalmente, el valor predeterminado es IP-xxxx para su máquina virtual durante la búsqueda de flujo. Después de sincronizar la configuración, aparece el flujo real de la máquina virtual.

Solución alternativa: Modifique la ventana de tiempo para excluir el flujo que desea ver.

- **Problema 2370660:** NSX Intelligence muestra datos inconsistentes para máquinas virtuales específicas.

Es probable que esto se deba a que las máquinas virtuales tienen la misma dirección IP en el centro de datos. NSX Intelligence no admite esta función en NSX-T 2.5.

Solución alternativa: Ninguna. Evite asignar la misma dirección IP a dos máquinas virtuales en el centro de datos.

- **Problema 2372657:** la relación VM-GROUP y la correlación de flujo GROUP-GROUP se muestran de forma incorrecta temporalmente.

La relación VM-GROUP y la correlación de flujo GROUP-GROUP se muestran de forma incorrecta temporalmente si el dispositivo de NSX Intelligence se implementó mientras había flujos en curso en el centro de datos. En concreto, los siguientes elementos pueden mostrarse de forma incorrecta durante este período temporal:

- Las máquinas virtuales pertenecen de forma incorrecta al grupo Sin categorizar.
- Las máquinas virtuales pertenecen de forma incorrecta al grupo Desconocido.
- Los flujos correlacionados entre dos grupos pueden mostrarse de forma incorrecta.

Estos errores se corregirán automáticamente después de que el dispositivo NSX Intelligence se haya implementado durante más tiempo que el período de visualización seleccionado por el usuario.

Solución alternativa: Ninguna. Si el usuario sale del período de visualización durante el cual se implementó el dispositivo NSX Intelligence, el problema no se producirá.

- **Problema 2366630:** se puede producir un error en la operación de eliminación del nodo de transporte cuando se implementa el dispositivo de NSX Intelligence.

Si se elimina un nodo de transporte mientras se está implementando el dispositivo de NSX Intelligence, se puede producir un error en la eliminación debido a que NSX-INTELLIGENCE-GROUP NSGroup hace referencia al nodo de transporte. Para eliminar un nodo de transporte, es necesario usar la opción Forzar eliminación cuando se implementa el dispositivo de NSX Intelligence.

Solución alternativa: Use la opción Forzar eliminación para eliminar el nodo de transporte.

- **Problema 2357296:** es posible que algunos hosts de ESX no informen a NSX Intelligence en ciertas condiciones de escala y esfuerzo.

Es posible que la interfaz de NSX Intelligence no muestre los flujos de ciertas máquinas virtuales en determinados hosts y no proporcione recomendaciones de reglas de firewall para dichas máquinas virtuales. Como resultado, la seguridad del firewall podría verse comprometida en algunos hosts. Esto se observa en implementaciones con versiones de vSphere anteriores a las versiones 6.7U2 y 6.5U3. El problema se identifica como un fallo en la creación y eliminación del filtro de máquina virtual de hipervisor de ESX.

Solución alternativa: Actualice el host a la versión vSphere 6.7U2 y versiones posteriores o vSphere 6.5U3 y versiones posteriores.

- **Problema 2393142:** el inicio de sesión en NSX Manager con las credenciales de vIDM puede causar un error de usuario no autorizado 403.

Esto solo afecta a los usuarios que inician sesión como usuarios de vIDM, en oposición a usuarios locales, en NSX Manager. El inicio de sesión y la integración de vIDM no se admiten en NSX-T 2.5 al interactuar con el dispositivo de NSX Intelligence.

Solución alternativa: Para iniciar sesión como usuario local, agregue la IP o el FQDN de NSX Manager con la cadena 'login.jsp?local=true'.

- **Problema 2369802:** la copia de seguridad del dispositivo de NSX Intelligence excluye la copia de seguridad del almacén de datos de eventos.

Esta funcionalidad no se admite en NSX 2.5.

Solución alternativa: Ninguna.

- **Problema 2346545 (dispositivo de NSX Intelligence):** la sustitución de certificados afecta a la creación de informes sobre nuevos flujos.
Si el usuario reemplaza el certificado de identidad principal para el dispositivo de NSX Intelligence por un certificado autofirmado, el procesamiento de nuevos flujos se verá afectado y el dispositivo no mostrará la información actualizada a partir de entonces.

Solución alternativa: Ninguna.

- **Problema 2407198:** las máquinas virtuales aparecen incorrectamente en un grupo de máquinas virtuales sin categorizar en la postura de seguridad de NSX Intelligence.
Cuando los hosts ESXi se desconectan de vCenter, las máquinas virtuales de esos hosts se pueden mostrar en el grupo "Máquinas virtuales sin categorizar" aunque pertenezcan a otros grupos. Cuando los hosts ESXi se reconectaron con vCenter, las máquinas virtuales aparecerán en sus grupos correctos.

Solución alternativa: Vuelva a conectar los hosts a vCenter.

- **Problema 2410224:** después de completar el registro del dispositivo de NSX Intelligence, es posible que al actualizar la vista se obtenga el error 403 Prohibido.
Después de completar el registro del dispositivo NSX Intelligence, si hace clic en **Actualizar para ver**, es posible que el sistema devuelva un error 403 Prohibido. Esta es una condición temporal causada por el tiempo que necesita el dispositivo de NSX Intelligence para acceder a la interfaz.

Solución alternativa: Si recibe este error, espere unos minutos y vuelva a intentarlo.

- **Problema 2410096:** después de reiniciar el dispositivo NSX Intelligence, es posible que no se muestren los flujos recopilados en los últimos 10 minutos antes del reinicio.
Provocado por un problema de indexación.

Solución alternativa: Ninguna.

- **Problema 2436302:** después de sustituir el certificado de clúster de NSX-T Unified Appliance, no se puede acceder a NSX Intelligence a través de la API o la interfaz de NSX-T Manager.
En la interfaz de NSX-T Manager, acceda a la pestaña **Planificar y solucionar problemas** y, a continuación, haga clic en **Descubrir y realizar acción** o en **Recomendaciones**. La interfaz no se cargará y puede que devuelva un error como el siguiente: `No se pudo cargar la aplicación solicitada. Vuelva a intentarlo o póngase en contacto con el servicio de soporte técnico si el problema persiste.`

Solución alternativa: Consulte el [artículo 76223 de la base de conocimientos](#) para obtener más información y una solución alternativa.

Problemas conocidos de las operaciones y los servicios de supervisión

- **Problema 2401164:** las copias de seguridad aparecen de forma incorrecta como correctas, aunque se haya producido un error en el servidor SFTP.
Si caduca la contraseña del servidor SFTP utilizado para las copias de seguridad, NSX-T informa del error genérico "error desconocido de operación de copia de seguridad".

Solución alternativa: Compruebe que las credenciales para acceder al servidor SFTP estén actualizadas.

Problemas conocidos de actualización

- **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 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 2330417:** No se puede continuar con la actualización de los nodos de transporte que no están actualizados.
Al realizar la actualización, se marca como correcta aunque algunos nodos de transporte no se actualicen. Ubicación de registro: `/var/log/upgrade-coordinator/upgrade-coordinator.log`.

Solución alternativa: Reinicie el servicio coordinador de actualizaciones.

- **Problema 2348994:** error intermitente durante la actualización de NSX VIB en el nodo de transporte de ESXi 6.5 p03.
Se observó en algunas versiones de la 2.4.x a la 2.5. Cuando se actualizan los VIB de NSX en un nodo de transporte de ESXi 6.5 p03, a veces se produce un error en la operación de actualización y se muestra el siguiente error: "Excepción al invocar el SDK de VI: No se obtuvieron datos del proceso: LANG=en_US.UTF-8".

Solución alternativa: Actualice a ESXi 5 p04. También puede poner el host en modo de mantenimiento y reiniciarlo. Vuelva a intentar la actualización y salga del modo de mantenimiento.

- **Problema 2372653:** después de actualizar a la versión 2.5, el usuario no puede ubicar grupos basados en LogicalPort y LogicalSwitch en versiones anteriores de NSX-T.
Después de actualizar a la versión 2.5, los grupos basados en LogicalPort y LogicalSwitch creados a partir de la directiva en versiones anteriores de NSX-T no se encuentran en la interfaz del panel de control. Sin embargo, sí pueden encontrarse en la API. Esto se debe a un cambio de nombre provocado por el proceso de actualización. En la versión 2.5, los grupos basados en LogicalPort y LogicalSwitch aparecen como grupos basados en segmentos y en SegmentPort.

Solución alternativa: Use la API solo para acceder a estos grupos de directivas después de la actualización.

- **Problema 2408972:** durante la actualización, se produce un error en la vSphere Update Manager al corregir el último host.
Durante la actualización, se produce un error en la corrección de vSphere Update Manager del último host con cargas de trabajo de un conmutador lógico de NSX-T.

Solución alternativa: Migre manualmente todas las máquinas virtuales de la carga de trabajo de NSX-T a un host ya actualizado y, a continuación, vuelva a intentar la actualización del host con errores.

- **Problema 2400379:** la página Perfil de contexto muestra un mensaje de error de APP_ID no admitido.
La página Perfil de contexto muestra el siguiente mensaje de error: "Este perfil de contexto utiliza un APP_ID - [<APP_ID>] no admitido. Elimine este perfil de contexto manualmente después de asegurarse de que no se esté utilizando en ninguna regla." Esto se debe a la presencia posterior a la actualización de seis APP_ID obsoletos (AD_BKUP, SKIP, AD_NSP, SAP, SUNRPC, SVN) que ya no funcionan en la ruta de datos.

Solución alternativa: Después de asegurarse de que ya no se usan, elimine manualmente los seis perfiles de contexto de APP_ID.

- **Problema 2419246:** error en la actualización de Ubuntu KVM.
Se puede producir un error al actualizar los nodos de Ubuntu KVM debido a que el servicio nsx-vmapi no se está ejecutando. Sin embargo, el servicio nsx-vmapi depende de nsx-agent, pero nsx-agent aún no está configurado en este punto de la actualización. nsx-agent falla porque el componente vm-command-relay no se inicia correctamente.

Solución alternativa: Configure el componente nsx-agent, que no está instalado completamente. El siguiente comando vuelve a configurar todos los paquetes desempaquetados o configurados parcialmente:

```
dpkg --configure -a
```

También puede usar los siguientes comandos para volver a configurar solo nsx-agent y nsx-vmapi:

```
dpkg --configure nsx-agent
```

```
dpkg --configure nsx-vmapi
```

Problemas conocidos de la API

- **Problema 2260435:** Las reglas o directivas de redireccionamiento sin estado las crea de forma predeterminada la API, que no es compatible con las conexiones de este a oeste.
Las reglas o directivas de redireccionamiento sin estado las crea de forma predeterminada la API, que no es compatible con las conexiones de este a oeste. Como resultado, el tráfico no se redirecciona a los partners.

Solución alternativa: Al crear directivas de redireccionamiento mediante la API de la directiva, cree una sección con estado.

- **Problema 2200856:** el servicio cloud-service-manager no se reinicia correctamente.
El servicio cloud-service-manager restart puede fallar al reiniciarse si el usuario lo intenta sin esperar a que el servicio de API aparezca por primera vez.

Solución alternativa: Espere unos minutos y vuelva a intentarlo.

- **Problema 2378752:** la API permite la creación de varios mapas de enlace en segmentos o puertos.
Solo se observa en la API. Cuando el usuario crea varios mapas de enlace en un segmento o puerto, no se muestra ningún error. El problema aparece cuando el usuario intenta vincular varios perfiles en el segmento o puerto de forma simultánea.

Solución alternativa: En su lugar, utilice la interfaz de NSX Manager para realizar esta operación.

Problemas conocidos de NSX Cloud

- **2275232 - DHCP no funciona con las máquinas virtuales en la nube si Connectivity_strategy en 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.

- **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 2355113:** no se puede instalar NSX Tools en las máquinas virtuales de carga de trabajo RedHat y CentOS con redes aceleradas habilitadas en Microsoft Azure.
En Microsoft Azure, cuando se habilitan las redes aceleradas basadas en el sistema operativo RedHat (7.4 o versiones posteriores) o CentOS (7.4 o versiones posteriores) y con el agente NSX instalado, la interfaz de Ethernet no obtiene una dirección IP.

Solución alternativa: Después de arrancar la máquina virtual basada en RedHat o CentOS en Microsoft Azure, instale la última versión del controlador de Linux Integration Services disponible en <https://www.microsoft.com/en-us/download/details.aspx?id=55106> antes de instalar NSX Tools.

- **Problema 2391231:** es posible que se retrase la detección de cambios en las máquinas virtuales de Azure.
De forma intermitente, los cambios realizados en las máquinas virtuales de Azure en la nube se detectan con un ligero retraso. Eso podría afectar a la incorporación de las máquinas virtuales y a la creación de entidades lógicas para las máquinas virtuales en NSX-T. El retraso máximo observado fue de aproximadamente ocho minutos.

Solución alternativa: Ninguna. Una vez que pasa el período de retraso, el problema se corrige automáticamente.

- **Problema 2424818:** las estadísticas de DFW y Capa 2 no se actualizan en la interfaz de usuario de NSX Manager.
No todas las estadísticas producidas por el exportador lógico en las máquinas virtuales de carga de trabajo se reenvían a MP. Esto provoca un error al mostrar las estadísticas en la interfaz de usuario de la NSX Manager. Las estadísticas de DFW no se pueden ver en la interfaz de usuario de NSX Manager. El estado operativo de los puertos de conmutador lógicos se mostrará como inactivo y las estadísticas correspondientes no funcionarán. Esto solo es aplicable a las máquinas virtuales en la nube.

Solución alternativa: Ninguna. Las estadísticas se pueden ver a través de la CLI en las máquinas virtuales correspondientes.

