

# Notas de la versión de NSX Container Plugin 2.4

VMware NSX Container Plugin 2.4 | 7 de marzo de 2019

Compruebe regularmente las adiciones y actualizaciones a este documento.

## Contenido de las notas de la versión

Las notas de la versión contienen los siguientes temas:

- [Novedades](#)
- [Requisitos de compatibilidad](#)
- [Problemas resueltos](#)
- [Problemas conocidos](#)

## Novedades

### Novedades

NSX Container Plugin (NCP) 2.4 tiene las siguientes características nuevas:

- El nombre de fundación del mosaico VMware-NSX-T ahora es opcional. Si no se especifica, se establece como el nombre de la implementación de PAS.
- La alta disponibilidad (HA) de NCP está habilitada de forma predeterminada en Kubernetes.
- NCP/nsx\_node\_agent se cerrará en caso de error de conexión de back-end.  
Se ha agregado la opción de configuración connect\_retry\_timeout. Se puede usar para configurar el tiempo en segundos para que NCP/nsx\_node\_agent recupere la conexión con NSX Manager, el adaptador del orquestador del contenedor o HyperBus antes de cerrarse.
- Compatibilidad con la afinidad de sesión para un servicio de tipo equilibrador de carga.  
Además de la opción de ConfigMap l4\_persistence, NCP admite ahora la configuración de SessionAffinity en la especificación de servicio para los servicios de tipo equilibrador de carga. Si l4\_persistence se establece en ninguno, la configuración de SessionAffinity en la especificación de servicio únicamente determinará el efecto de persistencia. De lo contrario, la afinidad de sesión está habilitada para todos los servicios de tipo equilibrador de carga, y el usuario puede utilizar la configuración de SessionAffinity en la especificación de servicio para controlar el tiempo de espera de la persistencia.
- Si se proporciona una dirección IP en la especificación de loadBalancerIP de un servicio de Kubernetes de tipo equilibrador de carga, el servicio estará expuesto de forma externa en esta dirección IP.
- Compatibilidad con el clúster de NSX Manager.

Nota: NCP omite las rutas de OpenShift con terminaciones de recifrado y acceso directo SSL.

## Requisitos de compatibilidad

Producto	Versión
Mosaico NCP/NSX-T para PAS	2.4
NSX-T	2.3, 2.3.1, 2.4

Kubernetes	1.12, 1.13
OpenShift	3.10, 3.11
Sistema operativo de máquina virtual de host de Kubernetes	Ubuntu 16.04, RHEL 7.5, 7.6, CentOS 7.4, 7.5
Sistema operativo de máquina virtual de host de OpenShift	RHEL 7.4, 7.5, 7.6, CentOS 7.4, 7.5
PAS (PCF)	OpsManager 2.3.x + PAS 2.3.x OpsManager 2.4.x (excepto 2.4.0) + PAS 2.4.x (excepto 2.4.0)

## Problemas conocidos

- Problema 2118515: En una configuración a gran escala, NCP tarda mucho tiempo en crear firewalls en NSX-T**  
 En una configuración a gran escala (por ejemplo, 250 nodos de Kubernetes, 5.000 pods y 2.500 directivas de red), NCP puede tardar unos minutos en crear las reglas y las secciones de firewall en NSX-T.  
  
 Solución alternativa: Ninguna. Después de crear las reglas y las secciones de firewall, el rendimiento debería volver a la normalidad.
- Problema 2125755: Un StatefulSet podría perder la conectividad de red al realizar actualizaciones de valores controlados y actualizaciones graduales por fases**  
 Si se creó un StatefulSet antes de actualizar NCP a la versión actual, el StatefulSet podría perder la conectividad de red al realizar actualizaciones de valores controlados y actualizaciones graduales por fases.  
  
 Solución alternativa: Crear el StatefulSet después de actualizar NCP a la versión actual.
- Problema 2131494: La entrada de Kubernetes de NGINX sigue funcionando después de cambiar la clase de entrada de NGINX a NSX**  
 Cuando se crea una entrada de Kubernetes de NGINX, NGINX crea reglas de reenvío de tráfico. Si cambia la clase de entrada a cualquier otro valor, NGINX no elimina las reglas y las sigue aplicando, incluso si elimina la entrada de Kubernetes después de cambiar la clase. Esta es una limitación de NGINX.  
  
 Solución alternativa: Para eliminar las reglas creadas por NGINX, elimine la entrada de Kubernetes cuando el valor de clase sea NGINX. A continuación, vuelva a crear la entrada de Kubernetes.
- Para un servicio de Kubernetes de tipo ClusterIP, no se admite la afinidad de sesión basada en IP de cliente**  
 NCP no es compatible con la afinidad de sesión basada en IP de cliente para un servicio de Kubernetes de tipo ClusterIP.  
  
 Solución alternativa: Ninguno
- Para un servicio de Kubernetes de tipo ClusterIP, no se admite la marca de modo horquilla**  
 NCP no es compatible con la marca de modo horquilla para un servicio de Kubernetes de tipo ClusterIP.  
  
 Solución alternativa: Ninguno
- Problema 2193901: No se admiten varios PodSelectors ni NsSelectors para una única regla de directiva de red de Kubernetes**

Al aplicar varios selectores se permite solamente el tráfico entrante desde pods específicos.

Solución alternativa: En su lugar, utilice `matchLabels` con `matchExpressions` en un solo `PodSelector` o `NsSelector`.

- **Problema 2194646:** No se admite la actualización de las directivas de red cuando NCP está inactivo

Si actualiza una directiva de red cuando NCP está inactivo, el IPset de destino para la directiva de red será incorrecto cuando NCP vuelva a activarse.

Solución alternativa: Vuelva a crear la directiva de red cuando NCP esté activo.

- **Problema 2192489:** Después de deshabilitar 'BOSH DNS server' en la configuración de director de PAS, el servidor DNS de Bosh (169.254.0.2) sigue apareciendo en el archivo `resolve.conf` del contenedor

En un entorno de PAS que ejecute PAS 2.2, después de deshabilitar 'BOSH DNS server' en la configuración de director de PAS, el servidor DNS de Bosh (169.254.0.2) sigue apareciendo en el archivo `resolve.conf` del contenedor. Esto provoca que un comando de ping con un nombre de dominio completo tome mucho tiempo. Este problema no existe con PAS 2.1.

Solución alternativa: Ninguna. Este es un problema de PAS.

- **Problema 2194367:** El mosaico de NSX-T no admite en este momento segmentos de aislamiento de PAS que implementan sus propios enrutadores

El mosaico NSX-T no funciona con los segmentos de aislamiento de Pivotal Application Service (PAS) que implementan sus propias instancias de GoRouter y de enrutadores de TCP. Esto es porque NCP no puede obtener las direcciones IP de las máquinas virtuales del enrutador y crear reglas de firewall de NSX para permitir el tráfico de los enrutadores a los contenedores de aplicaciones de PAS.

Solución alternativa: Ninguna.

- **Problema 2199504:** El nombre para mostrar de los recursos de NSX-T creados por NCP se limita a 80 caracteres

Cuando NCP crea un recurso de NSX-T para un recurso en el entorno del contenedor, genera el nombre para mostrar del recurso de NSX-T al combinar el nombre del clúster, el espacio de nombres o el nombre de proyecto, y el nombre del recurso en el entorno del contenedor. Si el nombre para mostrar tiene más de 80 caracteres, este se trunca a 80 caracteres.

Solución alternativa: Ninguno

- **Problema 2199778:** Con NSX-T 2.2, la entrada, el servicio y los secretos con nombres que superan los 65 caracteres no son compatibles

Con NSX-T 2.2, cuando `use_native_loadbalancer` se establece como `True`, los nombres de las entradas, los secretos y los servicios a los que hacen referencia la entrada y los servicios del tipo de equilibrador de carga deben tener hasta 65 caracteres. De lo contrario, la entrada o el servicio no funcionarán correctamente.

Solución alternativa: Al configurar una entrada, un secreto o un servicio, especifique un nombre que sea de 65 caracteres o menos.

- **Problema 2065750:** Instalar el paquete de CNI de NSX-T falla con un conflicto de archivo

En un entorno de RHEL en el que se instaló Kubernetes, si instala el paquete de CNI de NSX-T mediante `yum localinstall` o `rpm -i`, aparece un error que indica un conflicto con un archivo del paquete de `kubernetes-cni`.

Solución alternativa: Instale el paquete de CNI de NSX-T con el comando `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm`.

- **Problema 2224218:** Después de eliminar un servicio o una aplicación, son necesarios dos

minutos para volver a liberar la IP de SNAT al grupo de direcciones IP

Si elimina un servicio o una aplicación, y vuelve a crearlos en menos de dos minutos, obtendrán una nueva IP de SNAT del grupo de direcciones IP.

Solución alternativa: Tras eliminar un servicio o una aplicación, espere dos minutos antes de volver a crearlos si desea volver a utilizar la misma dirección IP.

- **Problema 2218008: La configuración de clústeres de Kubernetes diferentes para que utilicen el mismo bloque de direcciones IP genera problemas de conectividad**

Si configura clústeres de Kubernetes diferentes para que utilicen el mismo bloque de direcciones IP, algunos pods no podrán comunicarse con otros pods ni con redes externas.

Solución alternativa: No configure clústeres de Kubernetes diferentes para que utilicen el mismo bloque de direcciones IP.

- **Problema 2263536: Un servicio de Kubernetes de tipo de nodo de puerto no reenvía el tráfico**

Con un servicio de tipo de nodo de puerto, un nodo de Kubernetes actúa como un enrutador que reenvía el tráfico de fuera del clúster a los pods. Al configurar dicho nodo, a veces las reglas en iptables no están configuradas correctamente para permitir el paso del tráfico.

Solución alternativa: Ejecute el siguiente comando para agregar una regla a iptables manualmente:

```
iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

Tenga en cuenta que esto solo funciona para un servicio de nodo de puerto con "externalTrafficPolicy: Cluster". No funciona para "externalTrafficPolicy: Local".