

Preguntas frecuentes sobre vRealize Network Insight

VMware vRealize Network Insight 5.2

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

<https://docs.vmware.com/es/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

- 1** Acerca de la guía de preguntas frecuentes de vRealize Network Insight 4
- 2** General 5
- 3** Instalación y configuración 8
- 4** Agregar o configurar orígenes de datos en vRealize Network Insight 15
- 5** Microsegmentación y flujos 18
- 6** Agrupar en clústeres 20
 - Agrupar en clústeres: general 20
 - Agrupar en clústeres: instalar y configurar 22
 - Agrupar en clústeres: escalar 24
 - Agrupar en clústeres: implementación 25
- 7** Administración y procesamiento de datos 28
- 8** IPFIX 30

Acerca de la guía de preguntas frecuentes de vRealize Network Insight

1

La guía de preguntas frecuentes de vRealize Network Insight ofrece al usuario preguntas frecuentes sobre vRealize Network Insight.

Público objetivo

Esta información está destinada a usuarios que trabajan con vRealize Network Insight.

¿Cómo se crea un paquete de soporte?

Consulte la sección sobre paquetes de soporte de la *Guía de referencia de la línea de comandos de vRealize Network Insight*.

¿Cómo se crea la función de administrador de solo lectura en Panorama de Palo Alto Networks para acceder a la API XML?

Para agregar una función de **administrador** para acceder a la API XML:

- 1 Seleccione **Panorama** → **Funciones de administrador**.
- 2 Haga clic en **Agregar** para agregar una nueva función de administrador y abrir el cuadro de diálogo Perfil de función de administrador.
- 3 En el cuadro de diálogo Perfil de función de administrador:
 - a Asigne un nombre a la función (por ejemplo, `api-only-admin`).
 - b Seleccione **Panorama** en **Función**.
 - c Deshabilite todas las entradas en la pestaña Interfaz de usuario web.
 - d Habilitar todas las entradas, excepto **Confirmar**, en la pestaña API XML.
 - e Haga clic en **Aceptar** para cerrar el cuadro de diálogo. Ahora la lista mostrará una nueva **Función de administrador**.
 - f Haga clic en **Confirmar** para confirmar los cambios en Panorama.
- 4 Asigne esta función de **Administrador** a una cuenta administrativa.

¿Cuándo se considera que un servicio es compartido?

Los siguientes puertos están configurados como compartidos:

Protocolo	Puerto
DNS	53
Bootpc	68
Kerberos	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269

Aparece un evento/error en el origen de datos que indica que cambió la información de identidad del origen de datos, como un certificado o la clave. ¿Qué significa?

vRealize Network Insight recibió un nuevo certificado de un origen de datos que no es el mismo que el almacenado en el producto. vRealize Network Insight acepta automáticamente el certificado presentado por los orígenes de datos. Durante el proceso, se obtiene un evento sobre los orígenes de datos donde se pueden descargar certificados antiguos y nuevos.

¿Cuál es el límite para importar registros de DNS en vRealize Network Insight?

Los límites para importar registros de DNS son los siguientes:

- Origen de datos de DNS de Infoblox: se pueden importar 900.000 registros desde un mismo origen de datos.
- Importación manual de registros de DNS: se pueden importar registros de DNS usando varios `.csv` o archivos de Bind empaquetados como un archivo zip. No hay ningún límite en cuanto a la cantidad de registros que se pueden importar, pero sí existen los siguientes límites de carga:
 - Número de archivos en un mismo archivo `.zip`: 25
 - Tamaño máximo de un solo archivo `.zip`: 10 MB.

¿Cuáles son los requisitos de recursos de vRealize Network Insight?

Consulte la guía de instalación de vRealize Network Insight para conocer los requisitos de recursos.

¿Qué sucede si se introduce una clave incorrecta durante la implementación del OVA del proxy de vRealize Network Insight?

La clave secreta no se valida durante la implementación del OVA del proxy de vRealize Network Insight. La implementación se completa incluso con una clave secreta incorrecta. Sin embargo, puede producirse un error en el emparejamiento y el proxy de vRealize Network Insight no se muestra como detectado en la interfaz de usuario de vRealize Network Insight.

Para corregir el secreto compartido, inicie sesión en la CLI del proxy de vRealize Network Insight y ejecute el comando `set-proxy-shared-secret` para definir la clave secreta correcta. Este comando reemplaza la clave anterior por la nueva, lo que permitirá que la plataforma de vRealize Network Insight detecte el proxy de vRealize Network Insight y se empareje con este.

¿Cómo se configura el DNS después de implementar el OVA del proxy de vRealize Network Insight?

Inicie sesión en la CLI del proxy de vRealize Network Insight y ejecute el comando `change-network-settings`. Este comando interactivo proporcionará al usuario una opción para agregar o modificar el DNS, tras lo cual el proxy de vRealize Network Insight se volverá a configurar con el nuevo DNS.

Si alguno de los parámetros de red no está configurado correctamente, use el comando `change-network-settings` para modificar los parámetros de configuración de red.

¿Cómo puede encontrarse la dirección IP de la máquina virtual de proxy de vRealize Network Insight en la interfaz de usuario?

Desplácese hasta la página Configuración y seleccione la opción de menú Infraestructura de vRealize Network Insight. Se muestra la dirección IP de las máquinas virtuales de la plataforma de vRealize Network Insight y del proxy de vRealize Network Insight.

¿Qué hay que hacer si el proxy de vRealize Network Insight no se detecta dentro de un plazo de 5 minutos después de la implementación del OVA del proxy de vRealize Network Insight?

Inicie sesión en el proxy de vRealize Network Insight con `consoleuser` (consulte la guía de la interfaz de línea de comandos de vRealize Network Insight) y compruebe lo siguiente:

- Compruebe el estado de emparejamiento de la plataforma de vRealize Network Insight con el proxy de vRealize Network Insight mediante la CLI `show-connectivity-status`.
- Si el estado de emparejamiento muestra `Passed`, abra la interfaz de usuario de la plataforma en una nueva ventana del explorador e inicie sesión para comprobar el estado.
- Si el estado de emparejamiento muestra `Failed`, puede que la clave secreta compartida que se especificó durante la implementación del OVA del proxy de vRealize Network Insight sea incorrecta. Para solucionar este problema, use el comando `set-proxy-shared-secret` para establecer la clave secreta correcta. Este comando reemplaza la clave anterior por la nueva, lo que permite que la plataforma de vRealize Network Insight detecte el proxy de vRealize Network Insight.
- Si `show-connectivity-status` muestra la capacidad de la red para acceder a la plataforma de vRealize Network Insight como **Error**, compruebe si se puede acceder a la plataforma de vRealize Network Insight a partir de la máquina virtual de proxy de vRealize Network Insight mediante el comando `ping`.
- Si no se puede acceder, compruebe si NTP, DNS, la puerta de enlace o cualquier otro parámetro de red están configurados correctamente con el comando `show-config`.
- Si alguno de los parámetros de red no está configurado correctamente, use el comando `setup` para modificar los parámetros de configuración de red.

¿Qué hay que hacer si se olvidan las credenciales de inicio de sesión?

Si es el usuario local de la interfaz de usuario: póngase en contacto con el administrador de la interfaz de usuario de vRealize Network Insight para que restablezca las credenciales por usted.

Si es el administrador: en vRealize Network Insight 3.4, las credenciales de la interfaz de usuario se pueden cambiar mediante la CLI `modify-password`. Consulte la guía de la CLI para obtener más información. Si utiliza una versión de vRealize Network Insight anterior a la 3.4, póngase en contacto con el soporte técnico.

¿Cómo se cambia la contraseña de inicio de sesión?

Para cambiar la contraseña de inicio de sesión:

- 1 Vaya a **Administrador > Configuración** y, a continuación, haga clic en **Mi perfil** en el panel izquierdo.
- 2 En la página **Cambiar contraseña**, rellene la información necesaria y haga clic en **Guardar**.

¿Qué debe hacerse si aparece la pantalla de inicio de sesión antes de que se detecte la máquina virtual de proxy de vRealize Network Insight?

- Este comportamiento es normal cuando el explorador se actualiza o cuando la dirección URL se abre en una ventana nueva antes de detectar el proxy.
- Inicie sesión con las credenciales que estableció durante la activación de la licencia para el nombre de usuario `admin@local`.

¿vRealize Network Insight admite varias instancias de vCenter Server o NSX Manager?

Sí, vRealize Network Insight admite varias instancias de vCenter Server y NSX Manager.

¿Qué servicios de vRealize Network Insight deben tener acceso a Internet y por qué?

vRealize Network Insight admite la función de llamada doméstica remota, la cual debe poder acceder a Internet. La función o los servicios permiten al equipo de vRealize Network Insight comprender de mejor manera los entornos de los clientes, así como corregir o solucionar problemas de forma proactiva. Los siguientes servicios necesitan acceso a Internet:

- Servicio de actualización automática (`svc.ni.vmware.com:443`): vRealize Network Insight utiliza este servicio para ponerse en contacto con el host de actualización remota y extraer los paquetes de bits recién publicados a medida que estén disponibles. El usuario obtendrá una notificación en la interfaz de usuario cuando las actualizaciones estén disponibles. Este servicio está habilitado de forma predeterminada, pero puede deshabilitarlo en la interfaz de usuario o con el comando `online-upgrade` a través de la CLI.

- Servicio de telemetría de rendimiento (`svc.ni.vmware.com:443`): algunas métricas relacionadas con los servicios clave y el rendimiento de vRealize Network Insight se recopilan y se cargan de forma periódica para vRealize Network Insight. El equipo de soporte supervisa estas métricas e identifica las anomalías del entorno para que el equipo de soporte pueda actuar antes de que afecte a los servicios críticos. Este servicio está deshabilitado de forma predeterminada, pero puede habilitarlo o deshabilitarlo con el comando `telemetry` a través de la CLI. Puede obtener más información aquí: <https://kb.vmware.com/s/article/59242>
- Servicio de soporte (`support2.ni.vmware.com:443`): este servicio establece túneles seguros remotos al host de soporte de vRealize Network Insight, lo que permite al personal autorizado acceder de forma remota a las implementaciones y trabajar en ellas. Está deshabilitado de forma predeterminada, y se puede habilitar o deshabilitar a través de la interfaz de usuario o mediante el comando "support-tunnel" de la CLI.
- Servicio de registro (`reg.ni.vmware.com:443`): sirve para registrar el dispositivo en todos los servicios externos. Permitirá una comunicación de confianza entre los servicios mencionados anteriormente. Cuando el programa de instalación tiene acceso a Internet, el registro sucede automáticamente. En un entorno aislado, se puede realizar con el comando "offline-registration" de la CLI (consulte la guía de la CLI para obtener más información). Este servicio es necesario para habilitar el túnel de soporte.

Nota Si la plataforma de vRealize Network Insight está detrás de un proxy de Internet, incluya los siguientes puertos y nombres de dominio en la lista blanca:

Tabla 3-1.

Servicio	URL	Puerto
Servicio de actualización/Servicio de métricas	<code>svc.ni.vmware.com</code>	443
Servicio de soporte de túnel	<code>support2.ni.vmware.com</code>	443
Servicio de registro	<code>reg.ni.vmware.com</code>	443

¿Cómo se deshabilita el acceso a Internet desde el dispositivo?

Los siguientes servicios utilizan servicios de Internet o remotos seguros:

- Servicio de actualización automática
- Servicio de telemetría de rendimiento
- Servicio de soporte
- Servicio de registro

Para obtener información sobre cómo habilitar o deshabilitar estos servicios, consulte las preguntas frecuentes sobre [¿Qué servicios de vRealize Network Insight deben tener acceso a Internet y por qué?](#). vRealize Network Insight debe poder acceder a Internet si alguno de estos servicios está habilitado.

¿Qué es el agregado de puertos y cuál es el mecanismo para llevarlo a cabo?

El agregado de puertos se incluye para poder agregar los flujos de puertos efímeros (como FTP dinámico, Oracle, MS-RPC, etc.). Esto ayuda a reducir la cantidad de flujos en el sistema y proporciona una vista agregada de un gran número de flujos relativos básicamente al mismo servicio.

El mecanismo para lograrlo es el siguiente:

- Durante los primeros tres días de observación de `destination_ip`, se agregarán puertos de destino a esa dirección IP concreta en depósitos de 10.000, y se empezará a crear un perfil de puerto para esa dirección IP (se crea un perfil de puerto por cada dirección IP de destino).
- Transcurridos esos tres días, y una vez creado el perfil, comenzaremos a agregar rangos de puertos donde la densidad de puertos sea alta (copiaremos el patrón de apertura de puertos efímeros). Los rangos en sí tendrán un tamaño dinámico (por ejemplo, 100, 1.000 o 10.000) y se crearán en función de la cantidad de puertos que se abran y lo comunes que sean en el rango de agregado en cuestión.

Nota Esta decisión tiene lugar de forma independiente para cada dirección IP del servidor.

- Esto permitirá marcar como sin agregado los flujos con una alta densidad de puertos cuando no haya ninguna actividad de apertura de puertos en masa. De igual modo, permitirá que pueda aplicarse agregado dinámico en caso de que dicha actividad exista.
- El perfil se actualiza continuamente según la caída de tiempo para tener en consideración los nuevos puertos que se abren o aquellos más antiguos que ya no se utilizan.

¿Cómo se cambia la dirección IP, la puerta de enlace o la máscara de red después de implementar el OVA de vRealize Network Insight?

Para cambiar la configuración de red del proxy o la plataforma de vRealize Network Insight, inicie sesión en la CLI y ejecute el comando `change-network-settings`. Este comando interactivo ofrecerá al usuario una opción para modificar la dirección IP, la puerta de enlace, la máscara de red, etc., tras lo cual el dispositivo de vRealize Network Insight vuelve a configurarse con los nuevos detalles.

Nota

- Esta tarea se debe realizar usando una sesión de consola de máquina virtual, ya que el dispositivo se reinicia al final.
- Si la dirección IP de la plataforma de vRNI se modifica y se empareja con proxies, ejecute este comando de la CLI en cada una de las máquinas virtuales de proxy:

```
vrni-proxy set-platform --ip-or-fqdn <New_Platform_IP>
```

¿Cómo se pasa de una licencia de evaluación a una licencia permanente?

Consulte la sección correspondiente a la adición y el cambio de licencias en la guía de usuario de vRealize Network Insight.

¿Cómo se caracterizan las licencias en vRealize Network Insight?

Tabla 3-2.

Nombre de la licencia	Tipo de licencia	Funciones
Enterprise	Completa/Producción: puede ser permanente o restringida a un límite de tiempo.	<p>Las siguientes funciones están habilitadas:</p> <ul style="list-style-type: none"> ■ AWS como proveedor de datos ■ Directivas de conservación de los datos adaptables ■ Origen de datos de DNS de Infoblox ■ Asignación de DNS y de IP físicas ■ Análisis
Avanzada	Completa/Producción: puede ser permanente o restringida a un límite de tiempo.	No corresponde

Nota TODAS las licencias se activan por socket de CPU y CCU (usuarios simultáneos). Las licencias de evaluación se pueden renovar o pasar a **Producción** con la clave actualizada en **Interfaz de usuario -> Configuración-> Acerca de**. Consulte la guía del usuario para obtener más información.

¿Cómo se hace una copia de seguridad de las máquinas virtuales en vRealize Network Insight?

Consulte *Prácticas recomendadas de VMware* para hacer copias de seguridad de las máquinas virtuales como VADP/API VDP de VMware. Se recomienda hacer una copia de seguridad antes de crear o expandir clústeres.

Agregar o configurar orígenes de datos en vRealize Network Insight

4

¿Qué hay que hacer si aparece un mensaje que indica que se agotó el tiempo de espera de la solicitud al agregar vCenter Server usando la dirección IP?

- Compruebe que se puede acceder a la dirección IP de vCenter Server desde la máquina virtual proxy de vRealize Network Insight.
- Inicie sesión en la CLI proxy de vRealize Network Insight y utilice el comando `ping` para confirmar que la dirección IP está accesible y `telnet` para confirmar que se puede acceder a vCenter Server en el puerto 443.
- Si se puede acceder a vCenter Server, intente realizar la operación de adición de nuevo.
- Si la dirección IP no está accesible, confirme que la puerta de enlace está configurada correctamente en la máquina virtual proxy de vRealize Network Insight con el comando `show-config`.
- Si la puerta de enlace es incorrecta, corríjala con el comando `setup`.

¿Qué hay que hacer si aparece un mensaje que indica que la dirección IP o el FQDN no son válidos al agregar vCenter Server?

- Compruebe que la dirección IP/FQDN de vCenter Server proporcionados son correctos.
- Compruebe que se puede acceder al FQDN desde la máquina virtual proxy de vRealize Network Insight con el comando `ping`.
- Si no se puede acceder, compruebe que el DNS está configurado correctamente en la máquina virtual proxy de vRealize Network Insight con los comandos `nslookup FQDN` y `show-config`.
- Si el DNS es incorrecto, corríjalo con el comando `setup`.

¿Qué privilegios requiere la plataforma de seguridad y operaciones de vRealize Network Insight?

vRealize Network Insight requiere credenciales de VMware vCenter Server con los siguientes privilegios:

- Conmutador distribuido: modificar
- Grupo de dvPort: modificar

¿Qué hay que hacer si aparece un error que indica que el usuario no tiene los privilegios necesarios al habilitar IPFIX en la página de origen de datos de vCenter Server?

Para poder habilitar IPFIX, vRealize Network Insight requiere credenciales de VMware vCenter Server con los siguientes privilegios:

- Conmutador distribuido: modificar
- Grupo de dvPort: modificar

Asegúrese de que el usuario de VMware vCenter Server proporcionado tiene permisos en la carpeta raíz de vCenter Server y en todas sus entidades secundarias (por ejemplo, en todas las carpetas y todos los centros de datos).

¿Con qué frecuencia se obtienen datos del entorno?

El proxy de vRealize Network Insight recupera datos del entorno cada 10 minutos.

¿Cuánto tiempo tardará en iniciarse el análisis de datos después de agregar la instancia de vCenter Server?

El análisis de datos comienza inmediatamente después de agregar una instancia de vCenter Server. La interfaz de usuario del producto mostrará una imagen parcial de los datos transcurridos unos minutos, lo que puede tardar dos horas en completarse.

Nota Los datos del tráfico de flujo cambian continuamente e incluyen al menos 24 horas de datos en el análisis.

¿Cómo se puede limpiar la configuración de IPFIX en vCenter Server si se eliminaron los OVA de vRealize Network Insight?

- En vSphere Web Client de VMware: vaya a **Inicio > Redes > VDS (nombre) > NetFlow**. Elimine la dirección IP de proxy de vRealize Network Insight de la configuración del recopilador.

- En el cliente de Windows de VMware vSphere: vaya a **Inicio > Inventario > Redes > VDS (nombre) > Editar**. Elimine la dirección IP de proxy de vRealize Network Insight de la configuración del recopilador en la pestaña NetFlow. Es necesario realizar este paso con cada VDS para el que IPFIX esté habilitado.

¿Cómo se puede limpiar la configuración de IPFIX en vRealize Network Insight?

En la interfaz de usuario de vRealize Network Insight, vaya a **Configuración > Orígenes de datos** y elimine la instancia de vCenter Server. Esto elimina la configuración de IPFIX realizada por vRealize Network Insight.

¿Cuánto tiempo tarda en mostrar las reglas de firewall correctas en la ruta de máquina virtual a máquina virtual después de agregar VMware NSX Manager en vRealize Network Insight?

Después de agregar VMware NSX Manager en vRealize Network Insight, puede tardar hasta 24 horas en calcular la relación de la máquina virtual con la regla de firewall.

¿Por qué no puedo ver la PNIC en la ruta de máquina virtual a máquina virtual después de agregar VMware vCenter en vRealize Network Insight?

Por lo general, vRealize Network Insight tarda alrededor de 2 horas en calcular la ruta de máquina virtual a máquina virtual después de agregar una instancia de VMware vCenter en vRealize Network Insight como origen de datos. Sin embargo, en algunas situaciones excepcionales, puede tardar unas 8 a 10 horas en mostrar la PNIC correctamente en la ruta de máquina virtual a máquina virtual después de agregar la instancia de VMware vCenter en vRealize Network Insight.

¿Qué son los números de pin de distribución de tráfico?

El porcentaje indica una descripción general de la distribución de tráfico basada en el análisis de flujo.

Tabla 5-1.

Tráfico	Descripción
Este-oeste (EO)	Tráfico de este a oeste como porcentaje del tráfico del grupo total.
Conmutado (porcentaje de EO)	Tráfico conmutado como porcentaje del tráfico de este a oeste.
Enrutado (porcentaje de EO)	Tráfico enrutado como porcentaje del tráfico de este a oeste.
Dentro del host (porcentaje de máquina virtual a máquina virtual)	Tráfico con origen y destino en el mismo host como porcentaje del tráfico de máquina virtual a máquina virtual.
Máquina virtual a máquina virtual (porcentaje de EO)	Tráfico de máquina virtual a máquina virtual como porcentaje del tráfico de este a oeste.
Internet	Tráfico de Internet como porcentaje del tráfico del grupo total.

¿Cómo se agregan puertos en los flujos?

El agregado de puertos se incluye para poder agregar los flujos de puertos efímeros (como FTP dinámico, Oracle, MS-RPC, etc.). Esto ayuda a reducir la cantidad de flujos en el sistema y proporciona una vista agregada de un gran número de flujos relativos básicamente al mismo servicio. El mecanismo para lograrlo es el siguiente:

- Durante los primeros tres días de observación de `destination_ip`, se agregarán puertos de destino a esa dirección IP en depósitos de 10.000, y se empezará a crear un perfil de puerto para esa dirección IP.

- Tras esos tres días (y después de crear un perfil que se puede utilizar con confianza), comenzaremos a agregar rangos de puertos en los que la densidad de puertos sea alta (en otras palabras, copiaremos el patrón de apertura de puertos efímeros). Los rangos en sí tendrán un tamaño dinámico (por ejemplo, 100, 1.000 o 10.000) y se crearán en función de la cantidad de puertos que se abran y lo comunes que sean en el rango de agregado en cuestión.
- Esto permitirá marcar como sin agregado los flujos con una alta densidad de puertos cuando no haya ninguna actividad de apertura de puertos en masa. De igual modo, permitirá que pueda aplicarse agregado dinámico en caso de que dicha actividad exista.
- El perfil se actualiza continuamente según la caída de tiempo para tener en consideración los nuevos puertos que se abren o aquellos más antiguos que ya no se utilizan.

¿Qué significa la dirección IP 240.240.240.240 en vRealize Network Insight?

240.240.240.240 es una dirección IP de marcador de posición en vRealize Network Insight. Esta dirección IP se utiliza si hay una gran cantidad de direcciones IP (más de 5.000) que llegan a una dirección IP en particular. Todas las direcciones IP de Internet entrantes (de la 5.001 en adelante) con la IP de marcador de posición, 240.240.240.240, se pueden reemplazar en ese endpoint de servicio.

Esto sirve para limitar la cantidad de flujos en el sistema, ya que el servicio expuesto públicamente que registra cada cliente de Internet individualmente puede derivar en un gran número de flujos, lo que daría como resultado una mayor carga del sistema.

En todos los flujos que se sustituyeron por esta dirección IP de marcador de posición, todas las métricas se agregan en el flujo correspondiente con esta dirección IP, con lo cual no habrá pérdida de estadísticas en un nivel de agregado.

Todas las direcciones IP de destino de los flujos indicados en la vista de flujos se muestran como originadas en 240.240.240.240 y llegan a ellas un gran número de direcciones IP de Internet (más de 5.000).

Agrupar en clústeres

6

Este capítulo incluye los siguientes temas:

- [Agrupar en clústeres: general](#)
- [Agrupar en clústeres: instalar y configurar](#)
- [Agrupar en clústeres: escalar](#)
- [Agrupar en clústeres: implementación](#)

Agrupar en clústeres: general

¿Se puede agrupar en clústeres una máquina virtual proxy o de recopilador?

No. La agrupación en clústeres no es posible en las máquinas virtuales proxy o de recopilador.

¿Necesita vRealize Network Insight un equilibrador de carga, como vRealize Log Insight?

La agrupación en clústeres de vRealize Network Insight es una solución de escalado horizontal, no una de alta disponibilidad. Si se produce un error en el nodo principal o en la máquina virtual de plataforma principal, todo el servicio dejará de estar disponible.

¿Qué sucede si se interrumpe la conexión entre el proxy remoto y la plataforma?

En caso de que la conexión entre la máquina virtual proxy y la máquina virtual de plataforma esté inactiva, la máquina virtual proxy almacenará los datos de forma local (según el espacio de almacenamiento) y los enviará cuando vuelva a conectarse.

¿Se integra vRealize Log Insight con vRealize Network Insight?

Sí. vRealize Log Insight se integró con vRealize Network Insight 3.4. Las alertas se envían a syslog, que puede ser vRealize Log Insight.

¿Qué ocurre si un nodo se reinicia?

Si un nodo se reinicia, se une automáticamente al clúster y sigue estando operativo. Si se trata del nodo principal, se produce una pérdida completa del servicio durante el tiempo que esté inactivo.

¿Cómo se cambia la dirección IP de cualquier nodo de plataforma o de un recopilador en un clúster?

En un clúster, se puede cambiar la dirección IP de cualquier recopilador o nodo de plataforma mediante los comandos de la CLI.

Nota

- Póngase en contacto con el soporte de VMware antes de realizar esta operación.
 - El dispositivo se reinicia al final del proceso. Por lo tanto, debe realizar estos pasos en la consola de máquina virtual.
-
- Para cambiar la IP del recopilador, ejecute el comando `change-network-settings`.
 - Para cambiar la dirección IP de la plataforma:
 - a Ejecute el comando `change-network-settings`.
 - b Ejecute el comando `update-IP-change` en todas las demás plataformas para reflejar la nueva dirección IP.
 - c Ejecute el comando `show-connectivity-status` en un recopilador y busque **IP/URL de máquina virtual de plataforma** para identificar si está asociado a esta plataforma.
 - d Ejecute `vrni-proxy` para reflejar la nueva dirección IP de la plataforma en los recopiladores asociados.

Caso de uso 1: en un clúster de 3 nodos, solo se cambia la dirección IP de platform2. No hay ningún recopilador asociado a esta plataforma.

- 1 Ejecute `change-network-settings` en platform2.
- 2 Ejecute `update-IP-change` en platform1 y platform3 para indicar la nueva dirección IP de platform2.

Caso de uso 2: en un clúster de 3 nodos, se cambian las direcciones IP de platform1 y platform2. El recopilador A está asociado a platform2; los demás están asociados a platform3.

- 1 Ejecute `change-network-settings` en platform1.
- 2 Ejecute `change-network-settings` en platform2.
- 3 Ejecute `update-IP-change platform1-oldIP platform1-newIP` en platform2 y platform3.
- 4 Ejecute `update-IP-change platform2-oldIP platform2-newIP` en platform1 y platform3.
- 5 Ejecute `vrni-proxy set-platform --ip-or-fqdn platform2-newIP` en collectorA.

¿Cuánto espacio de disco se necesita en Platform1?

Platform1 requiere más espacio de disco en comparación con otros nodos del clúster, ya que algunos de los datos de configuración se almacenan solo en Platform1.

¿Qué sucede si alguno de los nodos se quedó sin espacio de disco?

La interfaz de usuario empieza a mostrar mensajes de error cuando el espacio de disco de cualquier nodo de la plataforma en particular alcanza un determinado umbral. Para agregar más espacio de disco al nodo de la plataforma, inicie sesión en vCenter.

¿Cuántas veces se replican los datos en el clúster?

El mecanismo de replicación de datos depende de los componentes presentes en el nodo de la plataforma.

Agrupar en clústeres: instalar y configurar

¿Todas las máquinas virtuales de la plataforma deben estar en el mismo segmento L2/L3?

No. Sin embargo, lo mejor es mantener todos los nodos de la plataforma en una red común con baja latencia entre los nodos. Esto se debe a que muchos de los componentes distribuidos replican datos entre los nodos, y una latencia elevada podría provocar problemas de estabilidad y de rendimiento en el sistema.

¿Se puede actualizar un clúster mediante la función de actualización en el producto?

Hasta la versión 3.7 no se admitían actualizaciones en línea de los clústeres. A partir de la versión 3.8 y posteriores, un clúster se puede actualizar mediante el método de actualización en línea.

¿Qué sucede si se produce un error durante el proceso de creación del clúster?

Se recomienda crear una instantánea de la plataforma principal y de los proxies antes de iniciar el proceso de creación del clúster. Si se produce un error, elimine los nodos de plataforma secundaria y recupere de las instantáneas la plataforma principal y las máquinas virtuales proxy.

¿Qué sucede con los datos y la configuración existentes cuando se expande la implementación de nodo único en un clúster?

Todos los datos y la configuración se mantienen sin ningún cambio. Se podrá acceder a los datos después de la creación del clúster.

¿Se puede tener una máquina virtual de plataforma en regiones distintas?

No. Es indispensable que los nodos de la plataforma estén colocados en el mismo sitio. Los servidores proxy se pueden distribuir geográficamente.

¿Se puede alojar la plataforma en clústeres ampliados de vSAN (dos centros de datos...)?

Sí. Los clústeres de vSAN dentro del mismo centro de datos o en otros centros de datos seguirán manteniendo un cierto nivel de rendimiento de E/S como un almacenamiento local.

¿Se pueden alojar nodos de clúster en clústeres de vSAN distintos?

Sí. Los distintos nodos de un clúster de plataforma se pueden alojar en almacenes de datos subyacentes diferentes.

¿Es necesario hacer copias de seguridad de los nodos de plataforma?

Sí, las copias de seguridad se deben realizar con tecnologías de copia de seguridad o instantánea recomendadas de VMware.

¿Cómo se puede calcular el ancho de banda entre la máquina virtual proxy del clúster en una región y el clúster de máquina virtual de plataforma en otra región?

En algunas implementaciones de gran tamaño, vimos que oscila entre 1 y 20 Mbps. Existe una gran cantidad de deduplicación o compresión que tiene lugar en la máquina virtual proxy antes de que los datos se envíen a la máquina virtual de la plataforma.

¿Cuánto tráfico de red habrá en el nodo del clúster?

El tráfico suele depender del tamaño del clúster y del tipo de entorno del centro de datos.

Instalaciones con entre 30.000 y 50.000 máquinas virtuales:

- Entre clústeres: 50-400 Mbps aproximadamente.
- Entre el proxy y la plataforma: 100 Kbps-15 Mbps aproximadamente.

¿Cuál es la latencia máxima posible entre los nodos de un clúster?

Los nodos de la plataforma deben estar colocados en el mismo sitio. En estos casos, la latencia es mínima. Si los nodos de la plataforma se alojan en clústeres ampliados de vSAN (dos centros de datos), los clústeres de vSAN en los clústeres o entre ellos seguirán manteniendo un cierto nivel de rendimiento de E/S como un almacenamiento local. Las aplicaciones que se ejecutan en

centros de datos como vRealize Network Insight funcionan correctamente. Puede alojar nodos distintos de un clúster de plataforma en diferentes almacenes de datos subyacentes. Sin embargo, debe asegurarse de que todas las máquinas virtuales de plataforma de un clúster estén colocadas en el mismo sitio.

¿Cuál es la latencia máxima posible entre las máquinas virtuales proxy en una región y el clúster de máquina virtual de plataforma en otra región?

En una misma configuración puede haber proxies distribuidos geográficamente. Existe una conexión HTTPS entre la máquina virtual proxy y la máquina virtual de plataforma para tolerar latencias altas durante unos pocos segundos. vRealize Network Insight admite un máximo de 10 nodos en un clúster (30.000 máquinas virtuales con flujos o 50.000 sin flujos).

¿Cuál debería ser el tamaño de una máquina virtual proxy/de plataforma?

Use una configuración de bricks grandes; consulte la guía de instalación.

Agrupar en clústeres: escalar

¿Es posible ampliar un clúster ya creado?

Sí. Se admite la ampliación de un clúster de hasta 10 nodos.

¿Qué sucede si una máquina virtual de plataforma no principal deja de estar disponible?

Los servicios internos tienen una resistencia limitada a errores de nodo no principal. En general, Network Insight pierde alimentación de los recursos informáticos ante errores de nodo.

¿Qué tipo de equilibrio de carga se admite?

La asignación de proxy a una plataforma se solucionó. Cuando los datos de cualquier máquina virtual proxy lleguen a una máquina virtual de plataforma, se equilibrará la carga de su procesamiento internamente entre todas las máquinas virtuales de la plataforma.

Si se crea un clúster de plataforma, ¿aumentará el uso del ancho de banda?

Las máquinas virtuales proxy o de recopilador siguen en contacto únicamente con la máquina virtual principal o de la plataforma. El requisito de ancho de banda para la comunicación de agrupación en clústeres de máquinas virtuales de plataforma es mínimo. Por tanto, no existe un aumento significativo del uso de ancho de banda.

¿Cuál es la frecuencia de transmisión de datos entre la máquina virtual proxy y la máquina virtual de la plataforma?

La máquina virtual proxy envía datos deduplicados o comprimidos continuamente a la máquina virtual de la plataforma.

¿Se realiza algún tipo de optimización de los datos en la máquina virtual proxy?

En la máquina virtual proxy se producen varios pasos de deduplicaciones, compresiones, reducciones o procesamientos por lotes. Cuando la conexión entre la máquina virtual de la plataforma y la máquina virtual proxy está inactiva, esta última almacena los datos de forma local (según el espacio de disco) y los envía cuando la conexión se restaure.

¿Se realiza algún tipo de optimización del ancho de banda de red?

Sí. En la máquina virtual proxy se producen varios pasos de deduplicaciones, compresiones, reducciones o procesamientos por lotes.

¿Es posible agrupar en los servidores proxy?

No. No es posible agrupar en clústeres en los servidores proxy.

¿Cómo envía vCenter el tráfico al servidor proxy?

Los vCenter no envían tráfico al servidor proxy. Los servidores proxy en realidad se conectan a la instancia de vCenter designada para recuperar la información.

Al implementar un clúster, ¿cómo envía vCenter el tráfico a los distintos servidores proxy?

En realidad, los proxies se conectan a vCenter para recuperar la información. El servidor proxy correspondiente se conectará a la instancia de vCenter designada para recuperar la información. En los servidores proxy no es posible agrupar en clústeres.

Agrupar en clústeres: implementación

¿Cómo se puede acceder a la interfaz de usuario después de escalar horizontalmente el clúster?

El acceso a la interfaz de usuario solo está restringido a Platform1.

¿Qué es Platform1 y por qué debo recordar este nodo?

El nodo de plataforma desde el que se inicia el proceso de creación de clústeres se considera **Platform1**. El acceso a la interfaz de usuario solo debe realizarse desde este nodo de los n nodos del clúster.

¿Cómo se recuperan datos de los otros nodos de un clúster si el acceso a la interfaz de usuario está restringido solo a Platform1?

Los datos del centro de datos se distribuyen en todos los nodos de un clúster. Cuando la capa de interfaz de usuario solicita datos en Platform1, el nodo de Platform1 obtiene los datos almacenados en todos los nodos y envía una respuesta a la interfaz de usuario.

¿Se puede utilizar un nodo de plataforma que esté implementado en otro centro de datos para crear clústeres?

Todos los nodos de un clúster intercambian datos entre ellos. Por lo tanto, para evitar problemas de latencia, se recomienda utilizar los nodos de plataforma implementados en el mismo centro de datos para crear un clúster.

¿Qué sucede con los datos de la plataforma existente al escalar horizontalmente el nodo de la plataforma?

Los datos de un nodo de plataforma existente se conservan y distribuyen en todos los nodos de un clúster.

¿Es importante el número de máquinas virtuales proxy para determinar cuántos bricks de plataforma se necesitan?

No. Solo el número total de máquinas virtuales en todas las instancias de vCenter y el estado de los flujos (habilitado o deshabilitado) influyen en la cantidad de bricks necesarios. Consulte la tabla de modelos de bricks en la *Guía de instalación de vRealize Network Insight*.

¿El número de instancias de vCenter o la cantidad de dispositivos físicos (como, por ejemplo, enrutadores) o cualquier otro tipo de origen de datos tienen impacto en la cantidad de bricks de plataforma que se necesitan?

No. Solo el número total de máquinas virtuales en todas las instancias de vCenter y el estado de los flujos (habilitado o deshabilitado) influyen en la cantidad de bricks necesarios. Consulte la tabla de modelos de bricks en la *Guía de instalación de vRealize Network Insight*.

¿Admite vRNI clústeres de plataforma distribuidos entre dos centros de datos por motivos relacionados con la alta disponibilidad?

No. El clúster de plataforma no admite la división entre centros de datos. Todas las máquinas virtuales del clúster de la plataforma deben estar en el mismo sitio. Actualmente, los clústeres de plataforma no admiten alta disponibilidad, lo cual está previsto en el plan. Los clientes pueden utilizar SRM para alta disponibilidad en la recuperación ante desastres en dos sitios.

¿Admite vRNI una sola instancia de vCenter con más de 6.000 máquinas virtuales y flujos habilitados?

Hasta la versión 3.5, los proxies de vRNI no admiten la recopilación de datos de una sola instancia de vCenter de gran tamaño con más de 6.000 máquinas virtuales con flujos, lo cual está previsto en el plan.

¿Cuánto espacio de disco se necesita en Platform1?

Platform1 requiere más espacio de disco en comparación con otros nodos del clúster, ya que algunos de los datos de configuración se almacenan solo en Platform1.

¿Qué sucede si alguno de los nodos se quedó sin espacio de disco?

La interfaz de usuario empieza a mostrar mensajes de error cuando el espacio de disco de cualquier nodo de la plataforma en particular alcanza un determinado umbral. Para agregar más espacio de disco al nodo de la plataforma, inicie sesión en vCenter.

¿Cuántas veces se replican los datos en el clúster?

El mecanismo de replicación de datos depende de los componentes presentes en el nodo de la plataforma.

¿Cómo funcionan los clústeres?

- Todos los proxies de una implementación se conectan a una plataforma (Platform1). La conectividad entre la plataforma y el proxy se realiza a través de HTTPS en el puerto 443. Por lo tanto, solo el puerto 443 es visible para los proxies desde Platform1.
- Al recibir las solicitudes del proxy, Platform1 equilibra la carga de las solicitudes en otros nodos de la plataforma en el clúster mediante técnicas de round robin.
- El nodo de la plataforma normaliza los datos y los coloca en la cola de mensajes para que el motor de cálculo los procese.
- El motor de cálculo distribuye los datos entre todos los nodos del clúster usando un mecanismo de replicación de datos. De este modo, no se perderán datos si alguno de los nodos (excepto Platform1) deja de funcionar en el clúster.
- Algunos de los datos de configuración se almacenan expresamente en el nodo de Platform1 que no se replica. Este es el motivo por el que no se admite la solución de alta disponibilidad.

Administración y procesamiento de datos

7

¿Cómo se comporta la canalización de procesamiento de datos en condiciones límite, como cuando se interrumpe la comunicación entre el servidor proxy y la plataforma?

- ¿Cuál es el período de retención predeterminado?

30 días, aunque puede aumentarse desde la interfaz de usuario con licencia Enterprise. Nota: cuando se aumente, procure seguir las directrices del disco.

- ¿Cómo se tratan los datos en el proxy?

Todos los datos en el proxy, incluidos los datos de flujo, se convierten en un mensaje autodescriptivo (Self Describing Message, SDM) antes de enviarlos a la plataforma. Esto abarca todos los datos de configuración, inventario y métricas de cualquier origen de datos. Si no se puede acceder a la plataforma o la carga del SDM en la cola de Kafka genera errores, los datos se escribirán en el disco, en la máquina virtual proxy (en /var/BLOB_STORE).

- ¿Cuándo se empezarán a purgar los datos en el proxy?

Datos que no son de flujo: existe una asignación de 10 GB de espacio para almacenar SDM en el disco (BLOB_STORE). Cuando el almacenamiento llega a su límite, el recopilador comienza a eliminar los SDM más antiguos y agrega nuevos SDM al disco. La rapidez con la que se llegue a este límite depende del tamaño de los datos recopilados de todos los orígenes de datos.

Datos de flujo: existe una asignación de 15 GB de espacio para almacenar flujos sin procesar (en /var/flows/vds/nfcapd). En cuanto este espacio se consuma, el procesador de flujos comienza a eliminar los archivos de flujo más antiguos. Con una velocidad de flujos sin procesar entrantes de alrededor de 2 M/min, la rotación se iniciarían después de unas 10 horas.

- ¿Cuál es la lógica de la purga?

Los SDM más antiguos se eliminan primero.

- ¿Cuándo dejarán de procesarse los nuevos datos en el proxy?

Nunca, siempre y cuando los servicios funcionen correctamente.

- Suponiendo que la plataforma y el proxy están desconectados y que no se cumple ninguna condición de purga, ¿se reconciliarán todos los datos en la plataforma al restablecerse la conexión?

Todos los datos almacenados en el disco se enviarán a la plataforma. Deberían reconciliarse completamente, excepto si existen condiciones de pérdida de datos en la plataforma (encontrará más información a continuación).

- ¿Cuáles son las condiciones en las que se pueden perder datos en la plataforma?

La plataforma comienza a quitar los SDM que lleven más de 6 horas en la cola de Kafka (o 18, si se trata de un clúster de 3 nodos). Otra posibilidad es que la cola esté saturada. Esto puede ocurrir cuando hay un retraso de compilación en el sistema y la velocidad de los datos entrantes es alta.

- ¿En qué orden se envían los SDM, de más reciente a más antiguo o al revés?

Primero se envían los SDM más antiguos. Existe un problema conocido hasta la versión 3.9 que hará que se pierdan algunos datos. Póngase en contacto con GSS para obtener más información.

- ¿Los datos se almacenan en el disco en el proxy y, después, se envían a la plataforma cuando no hay ningún problema de comunicación?

Si no hay ningún problema de comunicación, los SDM no se almacenan en el disco, sino que se envían a la plataforma desde la propia memoria. Solo se almacenarán en el disco cuando el proxy reciba que hubo un problema al enviar un SDM.

- En caso de que haya algún problema, ¿cómo sabe el proxy cuál fue el último archivo de flujo que se procesó?

El procesador de flujos deja un marcador en la base de datos en la que se procesó el archivo nfcapd por última vez.

- ¿Cuál es el tamaño máximo de SDM que se puede procesar sin problemas? ¿Cómo puede estar el usuario al tanto en caso de infringirlo?

Existe un límite de 15 MB en el tamaño del SDM. A partir de la versión 3.9, cada vez que la plataforma quita un SDM grande, se genera un evento.

¿Qué es IPFIX?

IPFIX es un protocolo IETF para exportar información de flujos. Un flujo se define como un conjunto de paquetes transmitidos en una franja horaria específica que comparten los valores de cinco tuplas: dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino y protocolo. La información de flujo puede incluir propiedades como marcas de tiempo, recuento de bytes/paquetes, interfaces de entrada/salida, marcas de TCP, identificador de VXLAN, información de flujo encapsulado, etc. Esto suele denominarse NetFlow. Sin embargo, IPFIX es el protocolo IETF estándar.

¿Qué información de flujo exporta el VDS?

Es posible configurar un VDS en el entorno de vSphere para exportar información de flujo mediante IPFIX. Habilite la supervisión del flujo en todos los grupos de puertos asociados al VDS. Cuando los paquetes llegan a un puerto X de un VDS y salen de un puerto Y, se emite el registro de flujos correspondiente si la supervisión de flujo está habilitada en el puerto Y. La dirección de cada registro de flujo está establecida en "Salida".

¿Cómo usa IPFIX vRealize Network Insight?

vRealize Network Insight usa IPFIX de VDS de VMware para recopilar datos de tráfico de red. Cada sesión tiene dos rutas. Por ejemplo, "Sesión A↔C" tiene paquetes en sentido A→C y paquetes en sentido C→A. Para analizar la información completa de una sesión, se requieren datos de IPFIX sobre los paquetes en ambas direcciones. Consulte el siguiente diagrama, donde VM-A se conecta a DVPG-A y se comunica con VM-C. Aquí, DVPG-A solo proporcionará datos sobre los paquetes C→A y DVPG con vínculo superior proporcionará datos sobre los paquetes A→C. Para obtener la información completa del tráfico de A, IPFIX debe estar habilitado en DVPG-A y DVPG con enlace ascendente.

¿Cómo se solucionan los problemas de recopilación de flujos de vRealize Network Insight?

- 1 Asegúrese de que el VDS específico y sus DVPG y propiedades de vínculo superior tienen la supervisión de NetFlow establecida como **Habilitado**, y que la dirección IP del recopilador es la del recopilador de vRealize Network Insight.
- 2 Un firewall (NSX, virtual o físico) está quitando paquetes de NetFlow de IPFIX. Asegúrese de que los paquetes de NetFlow destinados al puerto 2055 de UDP en la dirección IP del recopilador de vRealize Network Insight tienen permiso para atravesar cualquier firewall que pueda estar presente en la ruta entre el host ESXi y el recopilador de vRealize Network Insight.
- 3 El host ESXi dejó de enviar paquetes de NetFlow de IPFIX. El host ESXi deja de enviar paquetes de NetFlow después de un tiempo si no se puede acceder al puerto 2055 de UDP. Esto puede ocurrir debido a que el firewall esté quitando los paquetes.
- 4 El host ESXi no puede acceder al recopilador de vRealize Network Insight debido a un problema de enrutamiento de red. Asegúrese de que hay una ruta adecuada entre el host ESXi y el recopilador de vRealize Network Insight.

¿Qué artículos de la base de conocimientos de VMware se deben tener en cuenta en relación con IPFIX?

VMware ESXi 6.0 Update 1: [2135956](#).

¿Cuándo se considera que un servicio es compartido?

Protocolo	Puerto
DNS	53
Bootpc	68
Kerberos	88
Pop3	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587

Protocolo	Puerto
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269