

Instalación de 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

Acerca de la Guía de instalación de vRealize Network Insight 5

1 Preparación de la instalación 6

Requisitos y recomendaciones del sistema 6

Privilegios 10

Puertos del sistema 10

Puertos de comunicación de red 19

Versiones y productos compatibles 21

2 Instalación de vRealize Network Insight 25

Flujo de trabajo de la instalación 25

Implementación del OVA de plataforma de vRealize Network Insight 27

Implementación mediante vSphere Web Client 27

Implementación mediante el cliente nativo de vSphere para Windows 29

Activación de la licencia 31

Generar un secreto compartido 31

Configuración del recopilador de Network Insight (OVA) 31

Implementación mediante vSphere Web Client 32

Implementar mediante el cliente nativo de vSphere para Windows 33

Configurar el recopilador de Network Insight (AMI) en AWS para VMware SD-WAN 35

Implementación de recopiladores adicionales en una configuración existente 37

3 Acceso a vRealize Network Insight mediante la licencia de evaluación 38

Adición de vCenter Server 38

Análisis de flujos de tráfico 40

Generación de un informe 40

4 Planificación para escalar verticalmente la implementación 41

Planificación para escalar verticalmente el clúster de plataforma 41

Planificación para escalar verticalmente el recopilador 42

Aumento del tamaño de brick de la configuración 44

5 Actualizar vRealize Network Insight 45

Actualización en línea 46

Actualización sin conexión con un solo clic 49

Actualización de CLI 52

6 Desinstalación de vRealize Network Insight 55

Eliminar la dirección IP del recopilador cuando NetFlow está habilitado en vCenter	56
Eliminar la dirección IP del recopilador cuando NetFlow está habilitado en NSX	56

Acerca de la Guía de instalación de vRealize Network Insight

La *Guía de instalación de vRealize Network Insight* está destinada a administradores o especialistas responsables de instalar vRealize Network Insight.

Público objetivo

Esta información está destinada a administradores o especialistas responsables de instalar vRealize Network Insight. La información está redactada para administradores de máquinas virtuales experimentados que están familiarizados con aplicaciones de gestión empresarial y operaciones de centros de datos.

Preparación de la instalación

1

Antes de instalar vRealize Network Insight, prepare el entorno de implementación para que cumpla con los requisitos del sistema.

Este capítulo incluye los siguientes temas:

- [Requisitos y recomendaciones del sistema](#)
- [Versiones y productos compatibles](#)

Requisitos y recomendaciones del sistema

Para obtener el mejor rendimiento posible, debe satisfacer las recomendaciones mínimas de la implementación.

Recomendaciones para la implementación de plataforma

Tabla 1-1. Especificaciones de tamaño de brick de plataforma

Tamaño de brick	Núcleos requeridos para CPU de 2,1 GHz	Núcleos requeridos para CPU de 2,3 GHz	Núcleos requeridos para CPU de 2,6 GHz	RAM	Disco
Mediano	10	9	8	32 GB	1 TB
Grande	15	14	12	48 GB	1 TB
Extragrande	20	18	16	64 GB	2 TB

Nota

- La reserva para la velocidad de CPU y la memoria RAM de cada nodo debe ser el 100 % del valor especificado anteriormente.
- Para que la configuración cumpla con todas las especificaciones, es posible que tenga que agregar recursos (RAM, disco, CPU). Consulte <https://kb.vmware.com/s/article/53550> y [Aumento del tamaño de brick de la configuración](#).

Tabla 1-2. Implementación sin clúster: capacidad máxima

Tamaño de brick	Número de máquinas virtuales (en miles)	Flujos por día (en millones)	Total de flujos (en millones)	Planificación de flujo (en millones)
Mediano	4.000	1.000.000	4.000.000	2.000.000
Grande	6.000	2.000.000	8.000.000	4.000.000

Tabla 1-3. Implementación sin clúster: capacidad máxima para VMware SD-WAN

Tamaño de brick	Número de instancias de Edge (en miles)	Flujos por día (en millones)	Total de flujos (en millones)
Mediano	2.000	1.000.000	4.000.000
Grande	2.000	2.000.000	8.000.000

Nota

- El número de máquinas virtuales incluye también las plantillas de vCenter.
- Total de flujos es el recuento máximo de flujos que el sistema puede almacenar para el período de conservación.
- Planificación de flujos es el total de flujos para los que el sistema puede realizar planes de seguridad.

Tabla 1-4. Implementación de clúster: capacidad máxima

Tamaño de brick	Tamaño de clúster	Número de máquinas virtuales (en miles)	Flujos por día (en millones)	Total de flujos (en millones)	Planificación de flujo (en millones)	Número de instancias de Edge para VMware SD-WAN (en miles)
Grande	3	10.000	2.000.000	8.000.000	4.000.000	4.000
Extragrande	3	18.000	6.000.000	24.000.000	4.000.000	6.000

Tabla 1-4. Implementación de clúster: capacidad máxima (continuación)

Tamaño de brick	Tamaño de clúster	Número de máquinas virtuales (en miles)	Flujos por día (en millones)	Total de flujos (en millones)	Planificación de flujo (en millones)	Número de instancias de Edge para VMware SD-WAN (en miles)
Extragrande	5	30.000	10.000.000	40.000.000	4.000.000	10.000
Extragrande	10	100.000	15.000.000	55.000.000	4.000.000	10.000

Nota

- El número de máquinas virtuales incluye también las plantillas de vCenter.
- Tamaño de clúster es la cantidad total de nodos en el clúster.
- Total de flujos es el recuento de flujos en el sistema para el período de conservación.
- La consulta para determinar el valor de Total de flujos es `count of flows in last 31 days` (suponiendo que el período de conservación es de 31 días).
- Planificación de flujos es el total de flujos para los que el sistema puede realizar planes de seguridad.

Recomendación para la implementación de recopilador

Tabla 1-5. Especificaciones de tamaño de brick de recopilador

Tamaño de brick	Núcleos necesarios para la CPU de 2,1 GHz	Núcleos necesarios para la CPU de 2,3 GHz	Núcleos necesarios para la CPU de 2,6 GHz	RAM	Disco
Mediano	5	5	4	12 GB	200 GB
Grande	10	9	8	16 GB	200 GB
Extragrande	10	9	8	24 GB	200 GB

Nota La reserva para la velocidad de CPU y la memoria RAM de cada nodo debe ser el 100 % del valor especificado anteriormente.

Tabla 1-6. Implementación de recopilador: capacidad máxima

Tamaño del recopilador	Número de máquinas virtuales (en miles)	Flujos por día (en millones)	Recuento de flujos en 4 días (en millones)	Número de instancias de Edge para VMware SD-WAN (en miles)
Mediano	4.000	2.500.000	3.250.000	4.000
Grande	10.000	5.000.000	6.500.000	6.000
Extragrande	20.000	10.000.000	13.000.000	10.000

Nota

- El número de máquinas virtuales incluye también las plantillas de vCenter.
- Para una implementación única con más de un recopilador, la limitación sobre el total de flujos entre recopiladores se basa en la capacidad de la plataforma.

Otros requisitos y consideraciones

- El sesgo temporal máximo entre los nodos de la plataforma debe ser inferior a 30 segundos.
- La disponibilidad del servicio NTP es fundamental para las operaciones del sistema. Asegúrese de no reiniciar el nodo de plataforma o el nodo de recopilador cuando el servicio NTP no esté disponible.
- Cuando los demás procesos en la plataforma utilizan por completo los recursos informáticos existentes, vRealize Network Insight se bloquea y no se recupera de forma automática. Si los servicios no se pueden recuperar, reinicie el nodo de plataforma.
- Si la latencia de red entre el nodo de la plataforma y el servidor de actualización es superior a 500 ms, es posible que se produzca un error en la actualización de vRealize Network Insight. Por tanto, la latencia de red debe ser inferior a 500 ms.
- La latencia de disco recomendada para obtener el mejor rendimiento es de hasta 5 ms. Si la latencia de disco supera los 5 ms, el rendimiento del sistema se degrada.
- El IOPS de disco recomendado es de 7.500.

Exploradores web compatibles

- Google Chrome: las dos versiones más recientes.
- Mozilla Firefox: las dos versiones más recientes.

Recomendaciones para admitir alta disponibilidad

Puede personalizar algunas opciones de vSphere HA para habilitar la alta disponibilidad de vSphere.

- **Error de host:** establézcala para que las máquinas virtuales se reinicien.

- **Aislamiento de host:** deshabilítela.
- **Invitado sin latido:** deshabilítela.

Privilegios

Privilegios necesarios en orígenes de datos

- Privilegios necesarios para configurar y utilizar IPFIX
 - Credenciales de vCenter Server con privilegios:
 - Conmutador distribuido: modificar
 - Grupo de dvPort: modificar
 - Las funciones predefinidas en vCenter Server deben tener los siguientes privilegios asignados en el nivel raíz, y que se deben propagar a las funciones secundarias:
 - System.Anonymous
 - System.Read
 - System.View
 - global.settings

Para obtener más información sobre las funciones de vCenter, consulte la sección Usar funciones para asignar privilegios en la guía *Seguridad de vSphere*.

- Privilegios necesarios en el proveedor de datos de NSX Manager
 - El proveedor de datos de NSX Manager requiere la función **Enterprise**.
 - Si la CLI Central está habilitada, se requieren las credenciales de `system admin` con el proveedor de datos de NSX Manager.
- Privilegios de usuario necesarios en conmutadores de Cisco para la recopilación de métricas
 - vRealize Network Insight es capaz de recopilar datos de métricas a través de SNMP, así como la configuración a través de SSH desde conmutadores de Cisco. La plataforma UCS de conmutadores de Cisco requiere el uso de SSH y API para la recopilación.

Tabla 1-7.

Tipo de datos	Privilegios de usuario
Datos de configuración	Solo lectura
Datos de métricas	SNMP de solo lectura
	SNMPv2 de solo lectura, Comunidad SNMP
	SNMPv3 de solo lectura

Puertos del sistema

A continuación se muestra la lista de puertos necesarios para la comunicación entrante de vRealize Network Insight:

Puertos de una configuración de clúster de plataformas

Tabla 1-8.

Origen	Destino	Puerto	Protocolo	Propósito	Confidencial	SSL	Autenticación
Cliente SSH	Plataforma	22	SSH	Acceso al host o a la CLI.	No	Sí	Usuario/contraseña o autenticación basada en clave SSH.
Web de cliente-Explorador y recopilador de vRNI	Plataforma	443	HTTPS	Acceso a la interfaz de usuario/API y comunicación con el recopilador de vRNI.	Sí	Sí	Canal SSL cifrado con certificado SHA2 basado en la clave RSA 2048b (o con un certificado personalizado configurado por el usuario). Los mensajes del recopilador a la plataforma de este canal se cifran también con HMAC.

Tabla 1-8. (continuación)

Origen	Destino	Puerto	Protocolo	Propósito	Confidencial	SSL	Autenticación
Plataforma	Plataforma	2181	HTTP	Comunicación entre servidores de Zookeeper en otros nodos (en caso de haber un clúster), almacenamiento de información de metadatos (datos de Znode).	No	No	
Plataforma	Plataforma	2888	HTTP	Se usa para conectarse al líder de Zookeeper.	No	No	
Plataforma	Plataforma	3000	HTTP	Se usa en las notificaciones de correo electrónico.	Sí	No	
Plataforma	Plataforma	3888	HTTP	Se usa para elegir el líder de Zookeeper.	Sí	No	
Plataforma	Plataforma	5432	jdbc	Almacenamiento de datos de configuración de máquinas virtuales y metadatos de infraestructura.	Sí	No	
Plataforma	Plataforma	8020	TCP/RPC	Comunicación entre otros nodos de nombre y nodos de datos.	Sí	No	

Tabla 1-8. (continuación)

Origen	Destino	Puerto	Protocolo	Propósito	Confidencia l	SSL	Autenticaci ón
Plataforma	Plataforma	8025	HTTP	Los administradores de nodos utilizan este puerto para conectarse al administrador de recursos.	No	No	
Plataforma	Plataforma	8030	HTTP	Lo usa el administrador de recursos para programar tareas.	No	No	
Plataforma	Plataforma	8032	HTTP	Dirección de la interfaz del administrador de aplicaciones en el administrador de recursos.	No	No	
Plataforma	Plataforma	8033	HTTP	Dirección de la interfaz de administración del administrador de recursos.	No	No	
Plataforma	Plataforma	8042	HTTP	Dirección de aplicación web del administrador de nodos.	No	No	
Plataforma	Plataforma	8080	HTTP	Atiende las solicitudes de interfaz de usuario.	Sí	No	

Tabla 1-8. (continuación)

Origen	Destino	Puerto	Protocolo	Propósito	Confidencial	SSL	Autenticación
Plataforma	Plataforma	8088	HTTP	Dirección HTTP de la aplicación web del administrador de recursos.	No	No	
Plataforma	Plataforma	8480	TCP/RPC	Servidor HTTP de JournalNode	No	No	
Plataforma	Plataforma	8485	TCP/RPC	Directorio de datos de ediciones compartidas de HDFS.	No	No	
Plataforma	Plataforma	9090	HTTP	Atiende las solicitudes del recopilador y envía comandos al recopilador.	Sí	Sí (protegido con nginx)	
Plataforma	Plataforma	9092	Binario sobre TCP	Puerto en el que otros agentes se comunican.	Sí	No	
Plataforma	Plataforma	9200-9300	HTTP	Atiende las solicitudes de búsqueda. ES usa un rango de puertos para escuchar; si 9200 está ocupado, utiliza el siguiente puerto disponible.	Sí	No	

Tabla 1-8. (continuación)

Origen	Destino	Puerto	Protocolo	Propósito	Confidencial	SSL	Autenticación
Plataforma	Plataforma	9300	HTTP	Atiende las solicitudes de búsqueda. ES usa un rango de puertos para escuchar; si 9200 está ocupado, utiliza el siguiente puerto disponible.	Sí	No	
Plataforma	Plataforma	30000:65535	TCP	Rango de puertos efímeros utilizados por varios procesos para establecer la conexión TCP con otros procesos.	No	No	
Plataforma	Plataforma	60000	IPC	Se utiliza para la comunicación entre los servidores principal y regional de HBASE	Sí	No	
Plataforma	Plataforma	60010	HTTP	Se usa para la interfaz de usuario web de HBASE.	No	No	

Tabla 1-8. (continuación)

Origen	Destino	Puerto	Protocolo	Propósito	Confidencia l	SSL	Autenticaci ón
Plataforma	Plataforma	60020	IPC	Comunicaci ón entre el servidor principal y el servidor regional de HBASE	Sí	No	
Plataforma	Plataforma	4500-4510	TCP	Comunicaci ón entre los servidores de base de datos de Foundation que se ejecutan en diferentes plataformas.	Sí	No	

Puertos de una configuración de plataforma única

Tabla 1-9.

Origen	Destino	Puerto	Protocolo	Propósito	Confidencialidad	SSL	Autenticación
Cliente SSH	Plataforma	22	SSH	Acceso al host o a la CLI.	No	Sí	Usuario/contraseña o autenticación basada en clave SSH.
Web de cliente-Explorador y recopilador de vRNI	Plataforma	443	HTTPS	Acceso a la interfaz de usuario/API y comunicación con el recopilador de vRNI.	Sí	Sí	Canal SSL cifrado con certificado SHA2 basado en la clave RSA 2048b (o con un certificado personalizado o configurado por el usuario). Los mensajes del recopilador a la plataforma de este canal se cifran también con HMAC.

Puertos del servidor de recopilador

Tabla 1-10.

Origen	Destino	Puerto	Protocolo	Propósito	Confidencialidad	SSL	Autenticación
Cliente SSH	Recopilador	22	SSH	Acceso al host o a la CLI.	No	Sí	Usuario/contraseña o autenticación basada en clave SSH.
Recopilador de vRNI	Plataforma	443	HTTPS	Canal de comunicación principal con plataforma	Sí	Sí	Canal SSL cifrado con certificado SHA2 basado en la clave RSA 2048b (o con un certificado personalizado configurado por el usuario). Los mensajes del recopilador a la plataforma de este canal se cifran también con HMAC.
Reenviador de flujos	Recopilador	UDP 2055	NetFlow/IPFIX	Los flujos procedentes del destino se envían a este puerto.	Sí	No	
Reenviador de flujos	Recopilador	UDP 6343	sFlow	Los flujos procedentes del destino se envían a este puerto.	Sí	No	

Tabla 1-10. (continuación)

Origen	Destino	Puerto	Protocolo	Propósito	Confidencialidad	SSL	Autenticación
Host ESXi	Recopilador	1991	TCP	Recopilar la medición de la latencia de la infraestructura virtual, por ejemplo: latencia entre vNIC a pNIC, VTEP a VTEP, TEP a TEP, etc.	No	No	
Dell OS10	Recopilador	50000	GRPC	Recibir información de telemetría de estadísticas del búfer desde dispositivos Dell OS10	No	No	

Puertos de comunicación de red

En la siguiente tabla, se enumeran los puertos y los protocolos que se utilizan para la comunicación de red en vRealize Network Insight.

También puede ver la lista de puertos en <https://ports.vmware.com/home/vRealize-Network-Insight>.

Tabla 1-11.

Propósito	De	Para	Puerto	Protocolo
Comunicación entre las máquinas virtuales de vRealize Network Insight	Recopilador	Plataforma Nota el puerto debe estar habilitado en todas las plataformas.	443	HTTPS
Servicios que requieren acceso a Internet	Plataforma y recopilador	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS
Comunicación de varios servicios configurados	Plataforma	Servidor LDAP	389, 636	LDAP y LDAPS
		Servidor SNMP	Configurable	SNMP

Tabla 1-11. (continuación)

Propósito	De	Para	Puerto	Protocolo
	Plataforma y recopilador	Servidor DNS	53	UDP
		Servidor Syslog	Configurable	
	Hosts ESXi	Recopilador	2055	TCP
	Hosts ESXi	Recopilador	1991	
Comunicación con AWS como origen de datos	Recopilador	AWS (*.amazonaws.com)	443	HTTPS
Comunicarse con el servicio de telemetría	Explorador	URL de telemetría (https://vcsa.vmware.com)	433	HTTPS
Comunicación con otros orígenes de datos dentro del centro de datos	Recopilador	Conmutadores de Arista	161 y 22	SNMP y SSH
		Azure	443	HTTPS
		Conmutadores de Brocade	161 y 22	SNMP y SSH
		Firewall de Check Point	443	HTTPS
		Cisco Nexus	161 y 22	SNMP y SSH
		Cisco UCS (sistema informático unificado)	161, 22 y 443	SNMP, SSH y HTTPS
		Conmutadores de Cisco Catalyst	161 y 22	SNMP y SSH
		Conmutadores ACI de Cisco	161	SNMP
		Controlador APIC de Cisco	161 y 443	HTTPS y SNMP
		Conmutadores de Dell	161 y 22	SNMP y SSH
		Dell OS10	50000	TCP
		VeloCloud	443, 2055	HTTPS
		HP	22	SSH
		Conmutadores de Juniper	161 y 22	SNMP y SSH
		Palo Alto Networks	443	HTTPS
		VMware vSphere	443	HTTPS

Tabla 1-11. (continuación)

Propósito	De	Para	Puerto	Protocolo
		VMware NSX-V (todos los componentes)	22 y 443	SSH y HTTPS
		NSX-T Manager	443	TCP
		Servidor de API de VMware PKS	8443 y 9021	TCP
		Servidor de API de Kubernetes	8443	TCP
		vRealize Log Insight	443	HTTPS
		Fortinet FortiManager	443	HTTPS

Versiones y productos compatibles

vRealize Network Insight admite varios productos y versiones.

Origen de datos	Versión/Modelo	Protocolo de conexión	Permisos/Privilegios
Amazon Web Services (solo licencia Enterprise)	No corresponde	HTTPS	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Conmutadores de Arista	7050TX, 7250QX, 7050QX-32S, 7280SE-72	SSH, SNMP	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Suscripción de Azure	No corresponde	HTTPS	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Conmutadores de Brocade	VDX 6740, VDX 6940, MLX, MLXe	SSH, SNMP	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Firewall de Check Point	Check Point R80, R80.10, R80.20 y R80.30	HTTPS, SSH	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Cisco ACI	3.2	HTTPS (a controladora APIC) SNMP (a controladora APIC y conmutadores ACI)	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Cisco ASA	Serie X con sistema operativo 9.4	SSH, SNMP	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Cisco Catalyst	3000, 3750, 4500, 6000, 6500	SSH, SNMP	Consulte la sección Agregar orígenes de datos en la guía de usuario.

Origen de datos	Versión/Modelo	Protocolo de conexión	Permisos/Privilegios
Cisco Nexus	3000, 5000, 6000, 7000, 9000	SSH, SNMP	Usuario de solo lectura Usuario de SNMP de solo lectura
Cisco UCS (sistema informático unificado)	Servidores blade serie B, servidores en rack serie C, chasis, interconexión de tejido	UCS Manager: HTTPS Tejido UCS: SSH, SNMP	Usuario de solo lectura Usuario de SNMP de solo lectura
Conmutadores de Dell	FORCE10 MXL 10, FORCE10 S6000, S4048, Z9100, S4810, PowerConnect 8024, Dell OS10	SSH, SNMP	Usuario de solo lectura Usuario de SNMP de solo lectura
Fortinet FortiManager	6.0.1	HTTPS	El usuario debe tener: <ul style="list-style-type: none"> ■ Al menos la función Usuario restringido con acceso a todos los ADOM y los paquetes de directivas. ■ Acceso rpc-permit read habilitado desde la interfaz de línea de comandos (Command Line Interface, CLI).
F5 BIG-IP	12.1.2 y posterior	HTTPS, SSH, SNMP	El usuario debe tener al menos la función de invitado. Además, TMSH debe estar habilitado y debe existir acceso a todas las particiones. F5 BIG-IP admite tanto el enrutamiento como el equilibrio de carga.
HP	HP Virtual Connect Manager 4.41, HP OneView 3.0	HP OneView 3.0: HTTPS HP Virtual Connect Manager 4.41: SSH	Usuario de solo lectura
Motor de nube Huawei	6800, 7800, 8800	SSH, SNMP	Usuario de solo lectura Usuario de SNMP de solo lectura
Infoblox	Infoblox NIOS 8.0, 8.1, 8.2	HTTPS	Usuario de solo lectura con acceso a la interfaz de API Permisos de solo lectura en los tipos de objeto DNS, del siguiente modo: <ul style="list-style-type: none"> ■ Tipo de permiso: DNS ■ Recursos: registros A, zonas DNS, vistas DNS
Conmutadores de Juniper	EX3300, QFX 51xx Series (JunOS 12 y 15, sin QFabric)	Netconf, SSH, SNMP	Usuario de solo lectura Usuario de SNMP de solo lectura
Kubernetes	<ul style="list-style-type: none"> ■ 1.12 en NSX-T 2.3.1 ■ 1.12 en NSX-T 2.3.2 ■ 1.13 en NSX-T 2.3.2 	HTTPS	El usuario debe tener la función de administrador de clústeres con permisos de lectura.

Origen de datos	Versión/Modelo	Protocolo de conexión	Permisos/Privilegios
OpenShift	3.1.1	HTTPS	Consulte la sección Agregar orígenes de datos en la guía de usuario.
Palo Alto Networks	Panorama 7.0.x, 7.1, 8.x, 9.0	HTTPS	El usuario debe tener la función de administrador con acceso a la API XML. Para obtener más información, consulte la sección sobre Palo Alto Networks en la <i>Guía de usuario de vRealize Network Insight</i> .
ServiceNow	London	HTTPS	El usuario debe tener la función de administrador.
VMware SD-WAN	VeloCloud Orchestrator y Edge 3.3.1 y versiones posteriores	HTTPS	El usuario debe tener la función Cuenta con cualquiera de los siguientes permisos: <ul style="list-style-type: none"> ■ Superusuario ■ Administrador estándar ■ Soporte al cliente
VMC on AWS-vCenter	M8 y posterior Nota Solo se admiten SDDC de VMware Cloud on AWS basados en NSX-T.	HTTPS	El usuario debe tener el siguiente permiso: <ul style="list-style-type: none"> ■ Administrador de nube: para agregar un origen de datos y habilitar IPFIX.
VMC on AWS-NSX Manager	M8 y posterior Nota Solo se admiten SDDC de VMware Cloud on AWS basados en NSX-T.	HTTPS	El usuario debe tener cualquiera de los siguientes permisos: <ul style="list-style-type: none"> ■ Miembro de organización.Administrador: para agregar un origen de datos y habilitar IPFIX. ■ Miembro de organización.Administrador. Administrador de NSX Cloud: para agregar un origen de datos y habilitar IPFIX. ■ Miembro de organización.VMware Cloud on AWS (todas las funciones): para agregar un origen de datos y habilitar IPFIX. ■ Miembro de organización.Auditor de NSX Cloud: para agregar un origen de datos.
VMware Identity Manager	3.3 y posterior	HTTPS	El usuario debe tener la función de administrador.

Origen de datos	Versión/Modelo	Protocolo de conexión	Permisos/Privilegios
VMware PKS	Versiones compatibles		El usuario debe tener permisos de función de administrador de clústeres: <code>pks.clusters.admin</code> .
VMware NSX Manager (VMware NSX-V)	Versiones compatibles	SSH, HTTPS	Consulte la sección Recopilación de datos perimetrales en la <i>Guía de usuario de vRealize Network Insight</i> .
VMware NSX-T Manager	2.4. Para conocer más versiones admitidas, consulte Versiones compatibles .	HTTPS	Usuario de solo lectura
VMware vRealize Log Insight	Versiones compatibles	HTTPS	Usuario de API con permisos para instalar, configurar y administrar el paquete de contenido.
VMware vSphere	Versiones compatibles En IPFIX se necesita la versión del ESXi de VMware: <ul style="list-style-type: none"> ■ 5.5 Update 2 (compilación 2068190) y versiones posteriores ■ 6.0 Update 1b (compilación 3380124) y versiones posteriores ■ VMware VDS 5.5 y versiones posteriores <p>Nota VMware Tools debe estar instalado en todas las máquinas virtuales del centro de datos para identificar la máquina virtual en la ruta de acceso de la máquina virtual.</p>	HTTPS	Usuario de solo lectura Privilegios necesarios para configurar y utilizar IPFIX Credenciales de vCenter Server con privilegios: <code>Distributed Switch: Modify</code> <code>dvPort group: Modify</code> Las funciones predefinidas en vCenter Server deben tener los siguientes privilegios asignados en el nivel raíz, y que se deben propagar a las funciones secundarias: <code>System.Anonymous</code> <code>System.Read</code> <code>System.View</code> <code>global.settings</code>

Nota

- Los sistemas operativos compatibles con los dispositivos de Cisco ASA, ACI, Catalyst y Nexus son iOS o NX-OS, mientras que para Cisco UCS es la versión de UCSM.
- El sistema operativo admitido para Arista es Arista EOS.

Instalación de vRealize Network Insight

2

vRealize Network Insight se puede implementar mediante vSphere Web Client o mediante el cliente nativo de vSphere para Windows.

Nota Después de implementar correctamente el OVA de plataforma de vRealize Network Insight, confirme que la dirección IP estática facilitada está definida en vCenter Server.

Para automatizar la instalación, la configuración, la actualización, la revisión, la gestión de configuración, la corrección de diferencias y el estado desde un panel centralizado, puede utilizar vRealize Suite Lifecycle Manager. Si es un usuario nuevo, haga clic aquí para instalar [vRealize Suite Lifecycle Manager](#). Esto ofrece a los administradores de TI de la nube los recursos de administración necesarios para centrarse en las iniciativas vitales para la empresa, mientras se mejora la rentabilidad (time to value, TTV), la fiabilidad y la coherencia.

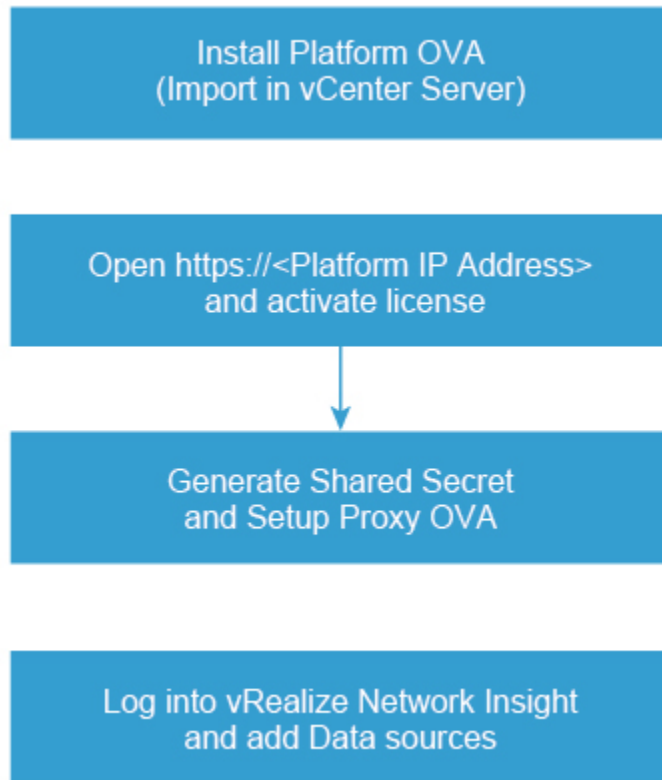
También puede instalar y actualizar vRealize Network Insight con vRealize Suite Lifecycle Manager. Para obtener más información, consulte la [Guía de instalación, actualización y administración de vRealize Suite Lifecycle Manager](#).

Este capítulo incluye los siguientes temas:

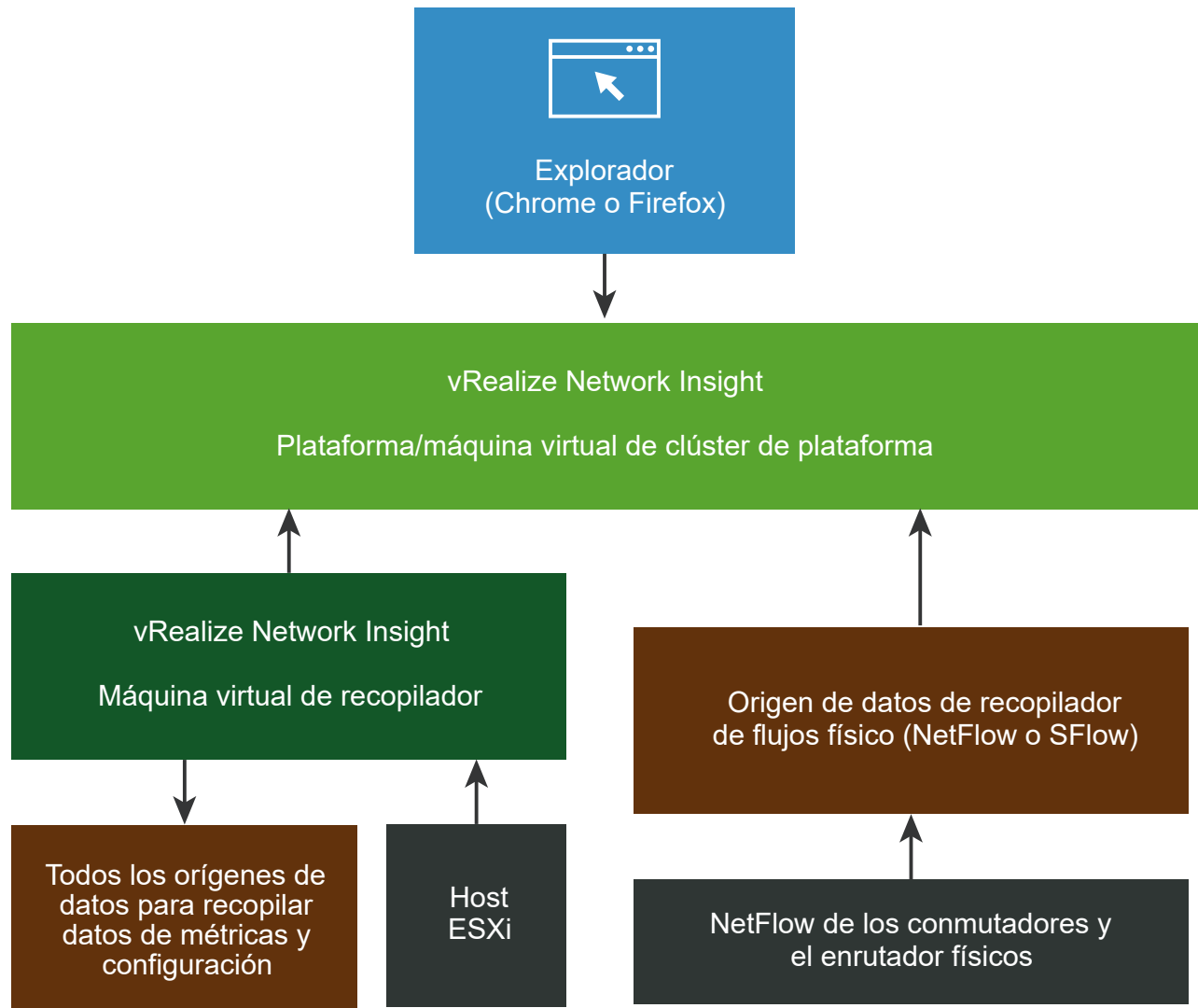
- [Flujo de trabajo de la instalación](#)
- [Implementación del OVA de plataforma de vRealize Network Insight](#)
- [Activación de la licencia](#)
- [Generar un secreto compartido](#)
- [Configuración del recopilador de Network Insight \(OVA\)](#)
- [Configurar el recopilador de Network Insight \(AMI\) en AWS para VMware SD-WAN](#)
- [Implementación de recopiladores adicionales en una configuración existente](#)

Flujo de trabajo de la instalación

Para instalar vRealize Network Insight, debe instalar el OVA de plataforma, activar la licencia, generar un secreto compartido y configurar el OVA del recopilador.



A continuación se presenta un diagrama de implementación simplificado de vRealize Network Insight:



Implementación del OVA de plataforma de vRealize Network Insight

El OVA de plataforma de vRealize Network Insight se puede importar a su vCenter Server.

Nota No se admite la implementación del vRealize Network Insight OVA de plataforma en el SDDC de VMC.

Implementación mediante vSphere Web Client

vRealize Network Insight se puede implementar mediante vSphere Web Client.

Procedimiento

- 1 Haga clic con el botón secundario en el **Centro de datos** en el que desea instalar el dispositivo y seleccione **Implementar plantilla de OVF**.

- 2 Introduzca la URL para descargar e instalar el paquete de OVA, o bien desplácese para seleccionar la ubicación de origen del paquete de OVA.
- 3 Introduzca el nombre del OVA. Seleccione la carpeta de destino de la implementación.
- 4 Seleccione un host/clúster o un grupo de recursos en el que desea ejecutar la plantilla implementada.
- 5 Confirme los detalles de la plantilla de OVF.
- 6 Lea el contrato de licencia de usuario final y haga clic en **Aceptar**.
- 7 Seleccione una configuración de implementación. Haga clic en **Siguiente**.
- 8 Seleccione la ubicación en la que desea almacenar los archivos de la plantilla implementada. Seleccione **Aprovisionamiento fino** como el formato de disco virtual. Seleccione el almacén de datos o los clústeres de almacén de datos donde quiera almacenar los archivos. Haga clic en **Siguiente**.
- 9 Especifique la red que la máquina virtual implementada va a usar.

La red seleccionada debe permitir que el dispositivo acceda a Internet para obtener soporte y actualizaciones.
- 10 Para personalizar la plantilla para la implementación, deberá configurar el dispositivo manualmente mediante la consola de máquina virtual. Haga clic en **Siguiente**.
- 11 Confirme los detalles de configuración y haga clic en **Finalizar**.
- 12 [Aumento del tamaño de brick de la configuración](#) para que coincida con los requisitos y las recomendaciones del sistema.
- 13 Una vez que la plataforma esté instalada, inicie la máquina virtual y la consola.
- 14 Inicie sesión con la credencial de la consola que se muestra en pantalla y ejecute el comando `setup`.
- 15 Cree la contraseña para el usuario *support* y cambie la contraseña de *consoleuser*.

Nota

- La contraseña debe contener un mínimo de 6 caracteres. No se permiten comillas simples (').
 - Deberá cambiar las contraseñas de *support* y de *consoleuser* periódicamente para cumplir la directiva de su organización.
-

- 16 Introduzca los siguientes detalles para configurar la red:
 - a **Dirección IPv4** : segunda dirección IP estática reservada.
 - b **Máscara de red**: máscara de subred de la IP estática anterior.
 - c **Puerta de enlace predeterminada** : puerta de enlace predeterminada de la red.

- d **DNS:** servidor DNS del entorno.

Nota Si hay varios servidores DNS, asegúrese de que estén separados por un espacio.

- e **Lista de búsqueda de dominio:** el dominio que debe agregarse para las búsquedas de DNS

- f Introduzca `y` para guardar la configuración.

- 17 Introduzca el servidor NTP y asegúrese de que pueda acceder a él desde la máquina virtual. Los servicios no se iniciarán si la hora de NTP no está sincronizada.

Nota Si hay varios servidores NTP, asegúrese de que estén separados por comas.

- 18 (opcional) Para configurar el proxy web, introduzca `y`.

- 19 Se verifican todos los servicios.

- 20 Agregue espacio de disco adicional en función de los requisitos de configuración. Consulte <https://kb.vmware.com/s/article/53550>.

Implementación mediante el cliente nativo de vSphere para Windows

vRealize Network Insight se puede implementar mediante el cliente nativo de vSphere para Windows.

Nota vRealize Network Insight 5.2 es la última versión que admite la implementación OVA mediante el cliente nativo de vSphere para Windows. A partir de la versión 5.3, puede seguir usando vSphere Web Client para implementar el OVA de vRealize Network Insight.

Procedimiento

- 1 Haga clic en **Archivo > Implementar plantilla de OVF**.
- 2 Introduzca la URL para descargar e instalar el paquete de OVA desde Internet, o bien desplácese para seleccionar la ubicación de origen del paquete de OVA en el equipo.
- 3 Haga clic en **Siguiente** y confirme los detalles de la plantilla de OVF.
- 4 Lea el contrato de licencia para el usuario final y haga clic en **Aceptar**.
- 5 Proporcione un nombre y una ubicación para la plantilla implementada. Haga clic en **Siguiente**.
- 6 Seleccione la **Configuración de implementación**.
- 7 Seleccione una opción de **Host/Clúster** para ejecutar la plantilla implementada.
- 8 Seleccione una opción de **Grupo de recursos** para implementar esta plantilla.
- 9 Seleccione un almacenamiento de destino para los archivos de máquina virtual. Haga clic en **Siguiente**.
- 10 Especifique el formato en el que desea almacenar los discos virtuales. Seleccione **Aprovisionamiento fino** como el formato de disco virtual. Haga clic en **Siguiente**.

- 11 Especifique la red que debe utilizar la plantilla implementada. Asigne la red de OVA al inventario.
- 12 Personalice la plantilla para la implementación. Proporcione el secreto compartido que se generó en la página de incorporación. Tendrá que configurar manualmente el dispositivo mediante la consola de máquina virtual. Haga clic en **Siguiente**.
- 13 Compruebe todos los datos de configuración. Seleccione **Encender después de la implementación**. Haga clic en **Finalizar**.
- 14 [Aumento del tamaño de brick de la configuración](#) para cumplir con los [Requisitos y recomendaciones del sistema](#).
- 15 Una vez que está instalado el OVA del recopilador, inicie la máquina virtual y la consola.
- 16 Inicie sesión con la credencial de la consola que se muestra en pantalla y ejecute el comando `setup`.
- 17 Cree la contraseña para el usuario `support` y cambie la contraseña de `consoleuser`.

Nota

- La contraseña debe contener un mínimo de 6 caracteres. No se permiten comillas simples (').
 - Deberá cambiar las contraseñas de `support` y de `consoleuser` periódicamente para cumplir la directiva de su organización.
-

- 18 Introduzca los siguientes detalles para configurar la red:
 - a **Dirección IPv4** : segunda dirección IP estática reservada.
 - b **Máscara de red**: máscara de subred de la IP estática anterior.
 - c **Puerta de enlace predeterminada** : puerta de enlace predeterminada de la red.
 - d **DNS**: servidor DNS del entorno.

Nota Si hay varios servidores DNS, asegúrese de que estén separados por un espacio.

- e **Lista de búsqueda de dominio** : el dominio que se debe anexar para `dns lookup`.
 - f Introduzca `y` para guardar la configuración.
- 19 Introduzca el servidor NTP y asegúrese de que pueda acceder a él desde la máquina virtual. Los servicios no se iniciarán si la hora de NTP no está sincronizada.

Nota Si hay varios servidores NTP, asegúrese de que están separados por comas.

- 20 (opcional) Para configurar el proxy web, introduzca `y`.
- 21 Se verifican todos los servicios.
- 22 Agregue espacio de disco adicional en función de los requisitos de configuración. Consulte <https://kb.vmware.com/s/article/53550>.

Activación de la licencia

Después de instalar el OVA de plataforma de vRealize Network Insight, abra *https://<dirección IP de plataforma de vRealize Network Insight>* en el explorador web Chrome.

Procedimiento

- 1 Introduzca la clave de licencia que recibió en el correo electrónico de bienvenida.
- 2 Establezca la contraseña del nombre de usuario de administrador de interfaz de usuario (admin@local).

Nota La contraseña debe ser alfanumérica y tener entre 8 y 100 caracteres. No se permite el espacio entre caracteres.

- 3 Haga clic en **Activar**.
- 4 Agregue el recopilador de vRealize Network Insight después de activar la licencia.

Generar un secreto compartido

Puede generar e importar el dispositivo virtual de recopilador de vRealize Network Insight.

Genere un secreto compartido e importe el dispositivo virtual de recopilador de vRealize Network Insight:

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de vRealize Network Insight.
- 2 Expanda **Infraestructura y soporte** y haga clic en **Descripción general y actualizaciones**.
- 3 Desplácese hacia abajo y haga clic en **Agregar máquina virtual proxy**.

Aparece el cuadro de diálogo **Agregar un nuevo dispositivo virtual del recopilador de datos de Network Insight**.

- 4 Haga clic en **Copiar** para copiar el secreto compartido desde el cuadro de diálogo y, a continuación, haga clic en **Listo**.

Lo necesitará durante la implementación del OVA del recopilador de vRealize Network Insight.

Configuración del recopilador de Network Insight (OVA)

El recopilador de vRealize Network Insight se puede configurar importando el OVA a vCenter Server.

Siga los pasos que aparecen a continuación para importar el OVA del recopilador de vRealize Network Insight a su instancia de vCenter Server.

Implementación mediante vSphere Web Client

Es posible importar el archivo OVA del recopilador de vRealize Network Insight mediante vSphere Web Client.

Procedimiento

- 1 Haga clic con el botón secundario en el **Centro de datos** en el que desea instalar el dispositivo y seleccione **Implementar plantilla de OVF**.
- 2 Introduzca la URL para descargar e instalar el paquete OVA desde Internet o examine para seleccionar la ubicación de origen del archivo OVA en el equipo.
- 3 Proporcione un nombre y una ubicación para la plantilla implementada. Haga clic en **Siguiente**.
- 4 Seleccione el recurso (host o clúster) donde desea ejecutar la plantilla implementada. Haga clic en **Siguiente**.
- 5 Compruebe todos los detalles de la plantilla. Haga clic en **Siguiente**.
- 6 Lea el contrato de licencia para el usuario final y haga clic en **Aceptar**. Haga clic en **Siguiente**.
- 7 Seleccione una configuración de implementación. Haga clic en **Siguiente**.
- 8 Seleccione la ubicación en la que desea almacenar los archivos de la plantilla implementada. Especifique el formato en el que desea almacenar los discos virtuales. Seleccione **Aprovisionamiento fino** como el formato de disco virtual. Seleccione el almacén de datos donde desea instalar los archivos. Haga clic en **Siguiente**.
- 9 Especifique la red de destino para la red de origen. Haga clic en **Siguiente**.
- 10 Personalice la plantilla para la implementación. Proporcione el secreto compartido que se generó desde la interfaz de usuario. Tendrá que configurar manualmente el dispositivo mediante la consola de máquina virtual. Haga clic en **Siguiente**.
- 11 Compruebe todos los datos de configuración. Haga clic en **Finalizar**.
- 12 Una vez que está instalado el OVA del recopilador, inicie la máquina virtual y la consola.
- 13 Inicie sesión con la credencial de la consola que se muestra en pantalla y ejecute el comando `setup`.
- 14 Cree la contraseña para el usuario *support* y cambie la contraseña de *consoleuser*.

Nota

- La contraseña debe contener un mínimo de 6 caracteres. No se permiten comillas simples (').
 - Deberá cambiar las contraseñas de *support* y de *consoleuser* periódicamente para cumplir la directiva de su organización.
-

15 Introduzca los siguientes detalles para configurar la red:

- a **Dirección IPv4** : segunda dirección IP estática reservada.
- b **Máscara de red**: máscara de subred de la IP estática anterior.
- c **Puerta de enlace predeterminada** : puerta de enlace predeterminada de la red.
- d **DNS**: servidor DNS del entorno.

Nota Si hay varios servidores DNS, asegúrese de que estén separados por un espacio.

- e **Lista de búsqueda de dominio**: el dominio que debe agregarse para las búsquedas de DNS
- f Introduzca **y** para guardar la configuración.

16 Introduzca el servidor NTP y asegúrese de que pueda acceder a él desde la máquina virtual. Los servicios no se iniciarán si la hora de NTP no está sincronizada.

Nota Si hay varios servidores NTP, asegúrese de que están separados por comas.

17 (opcional) Para configurar el proxy web:

- a Introduzca **y**.
- b Proporcione los detalles del proxy web.

18 Se efectúa una comprobación para corroborar si se configuró la clave secreta compartida. El recopilador se empareja con la plataforma correspondiente. Esto puede tardar varios minutos.

19 Se verifican todos los servicios.

20 Haga clic en **Finalizar** una vez que se muestra el mensaje **Proxy detectado** en la página de incorporación. Se redirigirá a la página de inicio de sesión.

Implementar mediante el cliente nativo de vSphere para Windows

Puede importar el archivo OVA del recopilador de vRealize Network Insight mediante el cliente nativo de vSphere para Windows.

Nota vRealize Network Insight 5.2 es la última versión que admite la implementación OVA mediante el cliente nativo de vSphere para Windows. A partir de la versión 5.3, puede seguir usando vSphere Web Client para implementar el OVA de vRealize Network Insight.

Procedimiento

- 1 Haga clic en **Archivo > Implementar plantilla de OVF**.
- 2 Introduzca la URL para descargar e instalar el paquete de OVA desde Internet, o bien desplácese para seleccionar la ubicación de origen del paquete de OVA en el equipo.
- 3 Compruebe los detalles de la plantilla de OVF. Haga clic en **Siguiente**.
- 4 Lea el contrato de licencia para el usuario final y haga clic en **Aceptar**. Haga clic en **Siguiente**.

- 5 Proporcione un nombre y una ubicación para la plantilla implementada. Haga clic en **Siguiente**.
- 6 Seleccione una **Configuración de implementación**. Haga clic en **Siguiente**.
- 7 Seleccione una opción de **Host/Clúster** para ejecutar la plantilla implementada. Haga clic en **Siguiente**.
- 8 Seleccione una opción de **Grupo de recursos** para implementar esta plantilla. Haga clic en **Siguiente**.
- 9 Seleccione un almacenamiento de destino para los archivos de máquina virtual. Haga clic en **Siguiente**.
- 10 Especifique el formato en el que desea almacenar los discos virtuales. Seleccione **Aprovisionamiento fino** como formato de disco virtual. Haga clic en **Siguiente**.
- 11 Especifique la red que debe utilizar la plantilla implementada. Asigne la red de OVA al inventario.
- 12 Personalice la plantilla para la implementación. Proporcione el secreto compartido que se generó en la página de incorporación. Tendrá que configurar manualmente el dispositivo mediante la consola de máquina virtual. Haga clic en **Siguiente**.
- 13 Compruebe todos los datos de configuración. Seleccione **Encender después de la implementación**. Haga clic en **Finalizar**.
- 14 Una vez que está instalado el OVA del recopilador, inicie la máquina virtual y la consola.
- 15 Inicie sesión con las credenciales de la consola proporcionadas. Ejecute el comando `setup`.
- 16 Cree la contraseña para el inicio de sesión de `support`. Cambie la contraseña para `consoleuser`.
- 17 Introduzca los siguientes detalles para configurar la red:
 - a **Dirección IPv4** : segunda dirección IP estática reservada.
 - b **Máscara de red**: máscara de subred de la IP estática anterior.
 - c **Puerta de enlace predeterminada** : puerta de enlace predeterminada de la red.
 - d **DNS**: servidor DNS del entorno.

Nota Si hay varios servidores DNS, asegúrese de que estén separados por un espacio.

- e **Lista de búsqueda de dominio** : el dominio que se debe anexar para `dns lookup`.
 - f Introduzca `y` para guardar la configuración.
- 18 Introduzca el servidor NTP y asegúrese de que pueda acceder a él desde la máquina virtual. Los servicios no se iniciarán si la hora de NTP no está sincronizada.

Nota Si hay varios servidores NTP, asegúrese de que están separados por comas.

- 19 (opcional) Para configurar el proxy web:
 - a Introduzca `y`.
 - b Proporcione los detalles del proxy web.
- 20 Se efectúa una comprobación para corroborar si se configuró la clave secreta compartida. El recopilador se empareja con la plataforma correspondiente. Esto puede tardar varios minutos.
- 21 Se verifican todos los servicios.
- 22 Haga clic en **Finalizar** una vez que se muestra el mensaje **Proxy detectado** en la página de incorporación. Se redirigirá a la página de inicio de sesión.

Configurar el recopilador de Network Insight (AMI) en AWS para VMware SD-WAN

Puede configurar el recopilador de vRealize Network Insight para AWS importando Amazon Machine Image (AMI) en el entorno de AWS.

Si el entorno no cuenta con una instancia de vCenter Server y desea implementar el recopilador en un entorno de nube, puede implementar el recopilador en AWS.

Nota Actualmente, vRealize Network Insight admite la implementación de recopiladores en AWS únicamente mediante AMI para VMware SD-WAN.

El procedimiento y la tarea relacionados con las instancias de EC2 se documentan en <https://docs.aws.amazon.com/efs/index.html>.

Procedimiento

- 1 Inicie la instancia de EC2 mediante la AMI proporcionada por VMware en la consola de Amazon EC2. Para obtener más información sobre los procedimientos, consulte los temas acerca de la creación de recursos de EC2 y la inicialización de la instancia de EC2 en la documentación de *Amazon Elastic File System*.

Nota Cuando inicie la instancia de EC2 en AWS, debe seleccionar lo siguiente:

Opción	Acción
Tipo de instancia	m4.xlarge (BRICK MEDIANO)
Red	Seleccione una red y una subred adecuadas.
Almacenamiento	Almacenamiento predeterminado.
Etiquetas	En función de las políticas del cliente.
Grupo de seguridad	Permita el tráfico saliente a 0.0.0.0/0 para el puerto 443 (o para las reglas restringidas, permita tráfico saliente para FQDN del producto NI SaaS para el puerto 443).
Clave	Seleccione la clave adecuada (el inicio de sesión SSH está habilitado para AMI).

- 2 Cuando la instancia de EC2 se encuentre en estado de ejecución, inicie sesión en la instancia de EC2.
- 3 Inicie sesión con las credenciales de la consola proporcionadas. Ejecute el comando `setup`.
- 4 Cree la contraseña para el inicio de sesión de `support`. Cambie la contraseña para `consoleuser`.

Nota Después de cambiar la contraseña, las opciones de red se omitirán durante la configuración de la CLI.

La AMI de proxy no es compatible con lo siguiente:

- Cambio de IP
- IPv6
- Configuración de proxy web.

- 5 Introduzca el servidor NTP y asegúrese de que pueda acceder a él desde la máquina virtual. Los servicios no se iniciarán si la hora del NTP no está sincronizada.

Nota Si hay varios servidores NTP, asegúrese de que están separados por comas.

- 6 Se efectúa una comprobación para corroborar si se configuró la clave secreta compartida. El recopilador se empareja con la plataforma correspondiente. Este proceso puede tardar unos minutos.

7 Se verifican todos los servicios.

Pasos siguientes

Habilite la recopilación de flujos desde las instancias de Edge hasta el recopilador que implementó en AWS. Para habilitar la recopilación de flujos, haga lo siguiente:

- Configure el recopilador que implementó en AWS como un sitio no VeloCloud. Para obtener más información, póngase en contacto con el soporte de VMware.

Implementación de recopiladores adicionales en una configuración existente

Puede agregar un recopilador de vRealize Network Insight adicional a una configuración existente.

Procedimiento

- 1 Inicie sesión en la interfaz de usuario de vRealize Network Insight.
- 2 Expanda **Infraestructura y soporte** y haga clic en **Descripción general y actualizaciones**.
- 3 Desplácese hacia abajo y haga clic en **Agregar máquina virtual proxy**.

Aparece el cuadro de diálogo **Agregar un nuevo dispositivo virtual del recopilador de datos de Network Insight**.

- 4 Haga clic en **Copiar** para copiar el secreto compartido desde el cuadro de diálogo y, a continuación, haga clic en **Listo**.
- 5 Siga los pasos de la sección [Configuración del recopilador de Network Insight \(OVA\)](#) en el paso 3.

Acceso a vRealize Network Insight mediante la licencia de evaluación

3

vRealize Network Insight se inicia en el modo de evaluación de NSX cuando se utiliza la licencia de evaluación.

Puede agregar un origen de datos a vRealize Network Insight, analizar el flujo de tráfico y generar informes.

Nota Para cambiar al modo de producto completo, haga clic en la opción Cambiar a evaluación de producto completo situada en la esquina inferior derecha.

Este capítulo incluye los siguientes temas:

- [Adición de vCenter Server](#)
- [Análisis de flujos de tráfico](#)
- [Generación de un informe](#)

Adición de vCenter Server

Puede agregar instancias de vCenter Server como orígenes de datos a vRealize Network Insight.

Se pueden agregar varias instancias de vCenter Server a vRealize Network Insight para empezar a supervisar datos.

Requisitos previos

- Las funciones predefinidas en vCenter Server deben tener los siguientes privilegios asignados en el nivel raíz, y que se deben propagar a las funciones secundarias:
 - **System.Anonymous**
 - **System.Read**
 - **System.View**
 - **Global.Settings**
- Se requieren los siguientes privilegios de vCenter Server para configurar y utilizar IPFIX:
 - **Conmutador distribuido: operación de configuración de puertos y modificación**
 - **Grupo de dvPort: operación de directivas y modificación**

Para obtener más información sobre las funciones de vCenter, consulte la sección Usar funciones para asignar privilegios en la guía *Seguridad de vSphere*.

Procedimiento

- 1 Haga clic en **Agregar vCenter**.
- 2 Haga clic en **Agregar nuevo origen** y personalice las opciones.

Opción	Acción
Máquina virtual de recopilador	Seleccione una máquina virtual de recopilador del menú desplegable.
Dirección IP/FQDN	Indique la dirección IP o el nombre de dominio completo de la instancia de vCenter Server.
Nombre de usuario	Introduzca el nombre de usuario con los siguientes privilegios: <ul style="list-style-type: none"> ■ Conmutador distribuido: modificar ■ Grupo de dvPort: modificar
Contraseña	Introduzca la contraseña del software de vRealize Network Insight para acceder al sistema vCenter Server.

- 3 Haga clic en **Validar**.

Si el número de máquinas virtuales detectadas supera la capacidad de la plataforma o de un nodo de recopiladores (o ambos), se produce un error en la validación. No se le permitirá agregar un origen de datos hasta que aumente el tamaño de brick de la plataforma o cree un clúster.

A continuación se presenta la capacidad especificada para cada tamaño de brick, tanto con flujos como sin ellos:

Tamaño de brick	Máquinas virtuales	Estado de flujos
Grande	6k	Habilitado
Grande	10k	Deshabilitado
Mediano	3k	Habilitado
Mediano	6k	Deshabilitado

- 4 Seleccione **Habilitar NetFlow (IPFIX)** en esta instancia de vCenter para habilitar IPFIX.

Para obtener más información sobre IPFIX, consulte la sección *Habilitar la configuración de IPFIX en VDS y DVPG* en la guía de usuario.

Nota Si habilita IPFIX en vCenter y en VMware NSX Manager, vRealize Network Insight detectará y eliminará automáticamente las redundancias de flujos deshabilitando IPFIX en algunos DVPG de la instancia de vCenter asociada.

- 5 Agregue orígenes de recopilación de datos avanzados al sistema vCenter Server.

- 6 Haga clic en **Enviar** para agregar el sistema vCenter Server. Los sistemas vCenter Server aparecerán en la página de inicio.

Análisis de flujos de tráfico

Puede usar vRealize Network Insight para analizar los flujos de su centro de datos.

Requisitos previos

Para poder iniciar el análisis de flujo, debe haber al menos dos horas de recopilación de datos.

Procedimiento

- 1 Especifique el ámbito del análisis. Por ejemplo, si está interesado en los flujos de todas las máquinas virtuales de un **clúster**, seleccione Clúster en el menú desplegable. También puede seleccionar todas las máquinas virtuales conectadas a una VLAN o VXLAN.
- 2 Seleccione el nombre de la entidad cuyos flujos quiera analizar.
- 3 Seleccione la duración y haga clic en **Analizar**.

Generación de un informe

Puede generar un informe de la evaluación de flujos.

Requisitos previos

Analice los flujos de tráfico en el centro de datos. Para elaborar informes completos, recopile datos correspondientes a un periodo de 24 horas antes de proceder al análisis.

Procedimiento

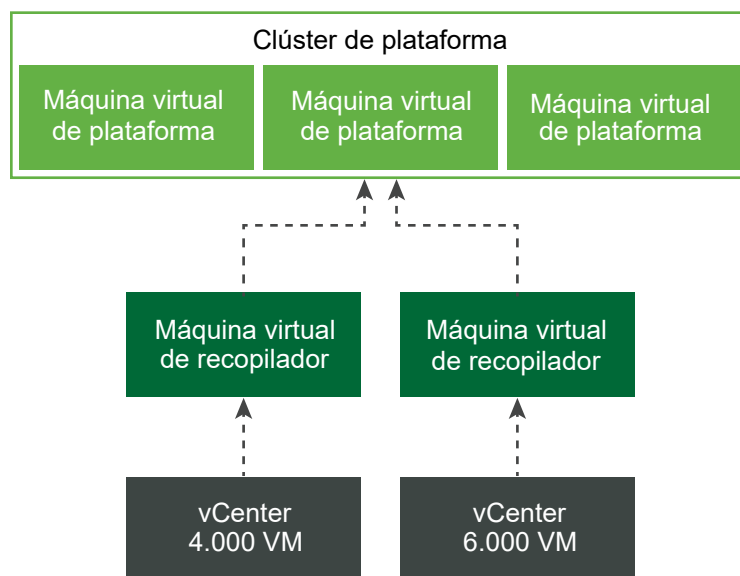
- 1 En el **modo de evaluación de NSX de prueba**, haga clic en **Generar informe** en la página Analizar flujos.
- 2 En la página **Microsegmentación** del **modo que no es de prueba**, haga clic en **Distribución de tráfico > Más opciones > Informe de evaluación**.

Planificación para escalar verticalmente la implementación

4

Si el número de máquinas virtuales o la cantidad de flujos activos en la configuración son elevados o se espera que crezcan, puede aumentar el tamaño de la plataforma o del recopilador.

Puede utilizar la siguiente arquitectura para comprender mejor la plataforma y la distribución de recopiladores:



Este capítulo incluye los siguientes temas:

- [Planificación para escalar verticalmente el clúster de plataforma](#)
- [Planificación para escalar verticalmente el recopilador](#)
- [Aumento del tamaño de brick de la configuración](#)

Planificación para escalar verticalmente el clúster de plataforma

El clúster de plataforma se puede escalar verticalmente para adaptarse a cargas cada vez mayores. En función de la carga, puede realizar un escalado vertical aumentando el tamaño del brick o creando o expandiendo un clúster de plataforma. Se pueden conectar tres bricks de

plataforma `LARGE` para formar un clúster de plataforma. Si una plataforma tiene un tamaño de brick `LARGE` o `EXTRA LARGE`, el escalado vertical se debe realizar creando un clúster de plataforma.

Para decidir el número y el tamaño de los bricks de plataforma, consulte [Requisitos y recomendaciones del sistema](#).

Nota El clúster de plataforma no admite configuraciones de alta disponibilidad. Todos los nodos de plataforma deben estar activos y en ejecución para que el clúster funcione a niveles de rendimiento óptimos.

Escenarios de escalado vertical del clúster de plataforma

- Escenario 1: una plataforma en la que se ejecutan 5.000 máquinas virtuales y 1,5 millones de flujos activos.

Convierta la plataforma de `MEDIUM` a `LARGE`. Consulte [Aumento del tamaño de brick de la configuración](#).

- Escenario 2: una plataforma en la que se ejecuta un solo nodo `LARGE` con 9.000 máquinas virtuales y 2 millones de flujos activos.

Agregue dos nodos de brick `LARGE` más para conseguir un clúster de bricks `LARGE` de tres nodos. Consulte la sección *Expandir clústeres* de la Guía de usuario de vRealize Network Insight.

- Escenario 3: una plataforma en la que se ejecuta un clúster de 3 nodos `LARGE` con 1 o más recopiladores, 15.000 máquinas virtuales y 4 millones de flujos activos.

Convierta los nodos de plataforma existentes de `LARGE` a `EXTRA-LARGE`. Consulte [Aumento del tamaño de brick de la configuración](#).

- Escenario 4: una plataforma en la que se ejecuta un clúster de 3 nodos `EXTRA-LARGE` con 1 o más recopiladores, 25.000 máquinas virtuales y 8 millones de flujos activos.

Agregue dos nodos de `EXTRA-LARGE` más para conseguir un clúster de cinco nodos `EXTRA-LARGE`. Consulte la sección *Expandir clústeres* de la Guía de usuario de vRealize Network Insight.

Planificación para escalar verticalmente el recopilador

La capacidad del recopilador se basa en el tamaño del brick. El origen de datos que se puede agregar a un recopilador depende de la capacidad de dicho recopilador (máquinas virtuales y flujos).

Consulte [Tabla 1-6. Implementación de recopilador: capacidad máxima](#). Cuando un recopilador tenga un tamaño de brick `LARGE`, se deberán agregar más recopiladores. Cada recopilador se puede escalar verticalmente a un tamaño `EXTRA-LARGE`.

Se pueden agregar varios orígenes de datos a un recopilador en función de la capacidad que ese recopilador admita. Sin embargo, no se puede agregar el mismo origen de datos a varios recopiladores.

Escenarios de escalado vertical de recopiladores

- Escenario 1: 2.000 máquinas virtuales en una instancia de vCenter.

Instale una máquina virtual de recopilador mediana. Agregue la instancia de vCenter a este recopilador. Consulte [Adición de vCenter Server](#).

- Escenario 2: 1.000 máquinas virtuales en vCenter1 y 2.000 máquinas virtuales en vCenter2 (todas se encuentran en un centro de datos).

Instale una máquina virtual de recopilador mediana. Agregue ambas instancias de vCenter a este recopilador. Consulte [Adición de vCenter Server](#).

- Escenario 3: 1.000 máquinas virtuales en vCenter1 (centro de datos 1) y 2.000 máquinas virtuales en vCenter2 (centro de datos 2)

Instale una máquina virtual de recopilador mediana en cada centro de datos. Agregue vCenter1 a una máquina virtual de recopilador en el mismo centro de datos y vCenter2, a una máquina virtual de recopilador en su centro de datos correspondiente. Consulte [Adición de vCenter Server](#).

- Escenario 4: el número de máquinas virtuales supera las 4.000, mientras que los flujos activos superan los 2,5 millones.

Convierta la máquina virtual de recopilador de `MEDIUM` a `LARGE`. Consulte [Aumento del tamaño de brick de la configuración](#).

- Escenario 5: 9.000 máquinas virtuales en vCenter1 sin flujos (centro de datos 1).

Instale una máquina virtual de recopilador grande. Agregue esta instancia de vCenter al recopilador. Consulte [Adición de vCenter Server](#).

- Escenario 6: el número de máquinas virtuales es igual o inferior a 10.000, pero los flujos activos superan los 5 millones.

Convierta la máquina virtual de recopilador de `LARGE` a `EXTRA-LARGE`. Consulte [Aumento del tamaño de brick de la configuración](#).

- Escenario 8: dos instancias de vCenter; vCenter1 tiene 10.000 máquinas virtuales y 9 millones de flujos activos, y vCenter2 tiene 10.000 máquinas virtuales y 4 millones de flujos activos.

Instale dos proxies, uno `EXTRA-LARGE` y otro `LARGE`. Agregue vCenter1 al proxy `EXTRA-LARGE` y vCenter2, al proxy `LARGE`.

- Escenario 9: una instancia de vCenter en la que se ejecutan 10.000 máquinas virtuales y 9 millones de flujos activos.

Instale un proxy `EXTRA-LARGE` y agregue la instancia de vCenter al proxy.

Aumento del tamaño de brick de la configuración

Para satisfacer sus requisitos, puede cambiar el tamaño del brick de la plataforma o del dispositivo del recopilador de **MEDIUM** a **LARGE** o de **LARGE** a **EXTRA-LARGE**.

Procedimiento

- ◆ Realice los pasos que sean relevantes según su configuración.

Opción	Descripción
Para una plataforma de un solo nodo o un OVA independiente nuevo	<ul style="list-style-type: none"> a Inicie sesión en vCenter. b Apague la máquina virtual de plataforma. c Aumente los valores de disco, RAM, vCPU total y reserva correspondiente de la máquina virtual para igualarlos al tamaño de brick de destino. Para obtener más información, consulte la página Requisitos y recomendaciones del sistema. d Reinicie la máquina virtual de plataforma.
Para una plataforma de clústeres	<ul style="list-style-type: none"> a Inicie sesión en vCenter. b Apague la máquina virtual de plataforma en orden cronológico inverso; por ejemplo, apague del nodo 3 al nodo 1. c Aumente los valores de disco, RAM, vCPU total y reserva correspondiente. Para obtener más información, consulte los Requisitos y recomendaciones del sistema. d Reinicie las máquinas virtuales de plataforma en orden cronológico. por ejemplo, reinicie del nodo 1 al nodo 3.
Para un recopilador	<ul style="list-style-type: none"> a Inicie sesión en vCenter. b Apague la máquina virtual de recopilador. c Aumente los valores de disco, RAM, vCPU total y reserva correspondiente de la máquina virtual para igualarlos al tamaño de brick de destino. Para obtener más información, consulte la página Requisitos y recomendaciones del sistema. d Reinicie la máquina virtual de recopilador.

Actualizar vRealize Network Insight

5

Puede actualizar su entorno actual de vRealize Network Insight a la versión más reciente.

Los siguientes son puntos importantes que se deben tener en cuenta antes de la actualización:

- Después de la actualización, vRealize Network Insight tarda entre 12 y 24 horas en procesar los datos que estaban en la canalización durante la operación de actualización y mostrarlos en la interfaz de usuario.
- vRealize Network Insight no admite que el producto se revierta ni se cambie a una versión anterior. Debe realizar una copia de seguridad antes de proceder con la actualización. Para obtener más información sobre el proceso de copia de seguridad y restauración, consulte el artículo de la base de conocimientos <https://kb.vmware.com/s/article/55829>.
- En un entorno de clúster, solo debe realizar la operación de actualización en el nodo de Platform1.
- Después de actualizar a vRealize Network Insight 5.1, es posible que se cambien algunos de los identificadores de reglas de firewall por los identificadores nuevos que devuelve la API de VMware Cloud on AWS 1.9. Tenga en cuenta lo siguiente si existe cualquiera de las reglas de firewall de VMware Cloud on AWS 1.8 asociadas a los flujos:
 - Las reglas de firewall de VMware Cloud on AWS 1.9 correctas o correspondientes se asociarán inmediatamente después de la actualización para todos los flujos activos.
 - Las reglas de firewall harían referencia a reglas que no existen para los flujos cuyos períodos de inactividad sean superiores a 24 horas antes de la actualización de la versión 1.8 a la versión 1.9.

Nota Si surgen problemas como errores de carga o errores de interfaz de usuario al realizar la actualización centralizada, póngase en contacto con el soporte de VMware.

Migrar a la base de datos de Foundation

Para distribuir datos de configuración entre almacenes de datos del clúster, vRealize Network Insight 5.1 reemplaza PostgreSQL por la base de datos de Foundation para almacenar los datos de configuración. Esto permite a vRealize Network Insight hacer lo siguiente:

- Reducir la carga en el nodo de Platform1.
- Evitar un punto único de error.

- Mejorar la resistencia.
- Mejorar el rendimiento.
- Compartir el disco uniformemente entre los nodos del clúster.

El proceso de migración realiza lo siguiente de forma automática:

- Cierra todos los servicios.
- Inicia la migración entre las tablas de PostgreSQL a las de la base de datos de Foundation.
- Muestra la información de progreso de migración dinámica en la interfaz de usuario de Platform1.

El tiempo de migración para mover datos desde PostgreSQL a la base de datos de Foundation depende de la velocidad del disco y del número de nodos (un mayor número de nodos proporcionan una mayor capacidad de escritura de la base de datos de Foundation).

El tiempo que se tarda en completar el proceso de migración depende del tamaño de la base de datos.

Tamaño de la configuración	Tamaño de los datos	Número de nodos	Tiempo típico de migración
Pequeño	De 20 GB a 40 GB	1 nodo	De 1 a 2 horas
Mediano	De 60 GB a 100 GB	3 nodos	De 7 a 10 horas
Configuraciones de una nube de gran tamaño	500 GB	Clúster de 10 nodos	De 15 a 20 horas
XL (Megatron)	1 TB	Clúster de 10 nodos	De 35 a 40 horas

Tenga en cuenta que la migración se realiza como parte del proceso de actualización de vRealize Network Insight. Por lo tanto, es posible que el tiempo de actualización sea mayor, lo cual se mostrará en la pantalla durante el proceso.

vRealize Network Insight ofrece los diferentes modos de actualización.

Este capítulo incluye los siguientes temas:

- [Actualización en línea](#)
- [Actualización sin conexión con un solo clic](#)
- [Actualización de CLI](#)

Actualización en línea

Siempre que haya disponible una nueva versión de vRealize Network Insight, recibirá una notificación.

Requisitos previos

- Puede que se produzcan errores en los pasos de actualización si no hay suficiente espacio en el directorio `/tmp`. Compruebe que cumple los siguientes requisitos de espacio de disco del servidor de plataforma y recopilador:
 - `/tmp`: 6 GB
 - `/home`: 2 GB
- Compruebe que cumple los siguientes requisitos de espacio de disco del servidor de plataforma:
 - `/`: 6 GB (solo para el nodo Platform1)
 - `/var`: 40 GB
- Compruebe que cumple con el requisito de ancho de banda mínimo de 500 KB/s para descargar el paquete de actualización del servidor. La página **Instalación y soporte** genera un error si el ancho de banda de descarga no es suficiente.
- Asegúrese de que todos los nodos estén conectados. Si algún nodo está inactivo, no podrá activar la actualización.
- Cree las instantáneas de las máquinas virtuales.
- Tenga en cuenta los siguientes valores que se comprobarán después de la migración:
 - Recuento de máquinas virtuales
 - Máquina virtual en la que el recuento de instantáneas sea superior a 0
 - Recuento de reglas de firewall
 - Recuento de grupos de seguridad
 - Recuento de firewalls de NSX

Procedimiento

- 1 Cuando haya una actualización disponible, aparecerá la notificación de mensaje **Actualización disponible**.

Nota

- Si la notificación de actualización no está disponible, compruebe que las máquinas virtuales del recopilador y de la plataforma de vRealize Network Insight tienen conectividad con `svc.ni.vmware.com` en el puerto 443 y con `reg.ni.vmware.com` en el puerto 443. Para ello, ejecute el comando `show-connectivity-status`. Si esta conectividad requiere `http proxy`, configúrelo en cada máquina virtual con el comando `set-web-proxy`. Asegúrese de que el resultado refleja el estado de conectividad de actualización como `Passed`.
 - Tramite un ticket de soporte e indique la etiqueta de servicio de la interfaz de usuario del producto. La etiqueta de servicio se muestra en **Configuración > Acerca de**.
 - Inicie sesión en el dispositivo y ejecute el comando `show-connectivity-status`. Proporcione una captura de pantalla del resultado del comando de cada máquina virtual de recopilador y de plataforma de vRealize Network Insight.
-

- 2 En la notificación de mensaje `Actualización disponible`, haga clic en **Ver detalles** para consultar los detalles de la actualización.

Aparecerá la pantalla Actualización de vRealize Network Insight.

- 3 Lea las instrucciones que aparecen en **Antes de continuar** y haga clic en **Continuar**.
- 4 Espere a que se completen las comprobaciones previas, las cuales verifican lo siguiente:
 - El espacio de disco, incluido el espacio necesario para la migración.
 - La versión.
 - El estado de la sincronización de NTP.
 - El ancho de banda.

En la configuración, puede ver el tiempo aproximado que se necesita para completar el proceso de actualización (incluida la duración de la migración).

- 5 Haga clic en **Instalar ahora**.

- 6 Cuando comience el proceso de actualización, la pantalla Actualización de vRealize Network Insight reflejará el estado del proceso de actualización.

Nota

- Si un nodo se vuelve inactivo, el proceso de actualización no continúa. La actualización no se reanuda hasta que el nodo vuelve a estar activo.
- Platform1 se convierte en el servidor de actualización. Si Platform1 está sin conexión, no se actualiza ningún otro nodo.
- Una vez actualizadas las plataformas, puede reanudar las operaciones normales de vRealize Network Insight aunque la actualización del recopilador se realice en paralelo. Hasta que el proceso de actualización finalice por completo, se mostrará el mensaje `Node Version Mismatch detected` en la página Instalación y soporte.

- Tras actualizar los servicios, Nginx se reinicia para mostrar el proceso de migración. Por tanto, es posible que no pueda acceder a la interfaz de usuario durante un breve período de tiempo (de uno a dos minutos).
- vRealize Network Insight inicia la migración de datos a la base de datos de Foundation. En la pantalla Estado de migración de datos, verá lo siguiente:
 - El estado general.
 - El tiempo transcurrido.
 - El estado de cada tabla.
 - La cantidad de registros migrados.

Si encuentra problemas, puede utilizar la opción **Exportar registros de migración** y compartir los registros con el equipo de soporte de VMware.

- Los datos de PostgreSQL en los recopiladores también se migran a la base de datos de Foundation como parte del proceso de actualización. Sin embargo, el estado de migración del recopilador no se muestra en la interfaz de usuario.

- 7 Una vez que se complete el proceso de actualización, verá el mensaje de confirmación.

Se actualizan todos los nodos de recopiladores y plataformas.

Pasos siguientes

- Inicie sesión en vRealize Network Insight y realice las tareas.
- Después de dos o tres días, elimine las instantáneas para ahorrar espacio de disco.

Actualización sin conexión con un solo clic

vRealize Network Insight admite la actualización sin conexión con un solo clic para el producto de la versión 3.7 y versiones posteriores.

Requisitos previos

- Puede que se produzcan errores en los pasos de actualización si no hay suficiente espacio en el directorio `/tmp`. Compruebe que cumple los siguientes requisitos de espacio de disco del servidor de plataforma y compilador:
 - `/tmp`: 6 GB
 - `/home`: 2 GB
- Compruebe que cumple los siguientes requisitos de espacio de disco del servidor de plataforma:
 - `/`: 12 GB (solo para el nodo Platform1)
 - `/var`: 40 GB

Nota Es posible que se produzcan errores en la carga del paquete y en los pasos de actualización posteriores si no hay espacio suficiente en el directorio `/tmp`.

- Para evitar que se agote el tiempo de espera de la sesión de la interfaz de usuario, desplácese hasta **Configuración > Configuración del sistema > Tiempo de espera de sesión de usuario** y aumente el valor de **Tiempo de espera de sesión de usuario** a por lo menos 2 horas. Después de cambiar la duración del tiempo de espera de la sesión, debe volver a iniciar sesión en el sistema.
- Asegúrese de que todos los nodos estén conectados. Si algún nodo está inactivo, no podrá activar la actualización.
- Cree las instantáneas de las máquinas virtuales.
- Tenga en cuenta los siguientes valores que se comprobarán después de la migración:
 - Recuento de máquinas virtuales
 - Máquina virtual en la que el recuento de instantáneas sea superior a 0
 - Recuento de reglas de firewall
 - Recuento de grupos de seguridad
 - Recuento de firewalls de NSX

Procedimiento

- 1 Descargue el archivo de paquete de actualización necesario de [My VMware](#) y guarde el paquete de actualización en el disco local.
- 2 Asegúrese de que el valor de `MD5SUM` del paquete descargado coincide con el valor de `MD5SUM` especificado en el sitio web de VMware.
- 3 En la página **Instalación y soporte**, en **Versión de software**, seleccione **Haga clic aquí**.

- 4 Haga clic en **Examinar** para seleccionar el archivo y, a continuación, haga clic en **Cargar**.

Cuando la carga se complete, vRealize Network Insight mostrará el mensaje de notificación `Carga de paquetes completada durante 2-3 minutos`, y el procesamiento del paquete se producirá en segundo plano.

Nota

- Hasta que se produzca la carga del paquete, asegúrese de que no se cierre la sesión. Si la sesión finaliza, debe reiniciar el proceso de carga.
 - Después de cargar el paquete, no actualice la página hasta que aparezca la notificación de mensaje `Actualización disponible`.
-

- 5 En la notificación de mensaje `Actualización disponible`, haga clic en **Ver detalles**.

Aparecerá la pantalla Actualización de vRealize Network Insight.

- 6 Lea la instrucción **Antes de continuar** y haga clic en **Continuar**.

- 7 Espere a que se completen las comprobaciones previas, las cuales verifican lo siguiente:

- El espacio de disco, incluido el espacio necesario para la migración.
- La versión.
- El estado de la sincronización de NTP.
- El paquete.

- 8 Haga clic en **Instalar ahora**.

En la configuración, puede ver el tiempo aproximado que se necesita para completar el proceso de actualización.

- 9 Cuando comience el proceso de actualización, la pantalla Actualización de vRealize Network Insight reflejará el estado del proceso de actualización.

Nota

- Si un nodo se vuelve inactivo, el proceso de actualización no continúa. La actualización no se reanuda hasta que el nodo vuelve a estar activo.
 - Platform1 se convierte en el servidor de actualización. Si Platform1 está sin conexión, no se actualiza ningún otro nodo.
 - Una vez actualizadas las plataformas, puede reanudar las operaciones normales de vRealize Network Insight aunque la actualización del recopilador se realice en paralelo. Hasta que el proceso de actualización finalice por completo, se mostrará el mensaje `Node Version Mismatch detected` en la página Instalación y soporte.
-
- Tras actualizar los servicios, Nginx se reinicia para mostrar el proceso de migración. Por tanto, es posible que no pueda acceder a la interfaz de usuario durante un breve período de tiempo (de uno a dos minutos).

- vRealize Network Insight inicia la migración de datos a la base de datos de Foundation. En la pantalla Estado de migración de datos, verá lo siguiente:
 - El estado general.
 - El tiempo transcurrido.
 - El estado de cada tabla.
 - La cantidad de registros migrados.

Si encuentra problemas, puede utilizar la opción **Exportar registros de migración** y compartir los registros con el equipo de soporte de VMware.

- Los datos de PostgreSQL en los recopiladores también se migran a la base de datos de Foundation como parte del proceso de actualización. Sin embargo, el estado de migración del recopilador no se muestra en la interfaz de usuario.

10 Una vez que se complete el proceso de actualización, verá el mensaje de confirmación.

Se actualizan todos los nodos de recopiladores y plataformas.

Pasos siguientes

- Inicie sesión en vRealize Network Insight y realice las tareas.
- Después de dos o tres días, elimine las instantáneas para ahorrar espacio de disco.

Actualización de CLI

Considere actualizar la CLI solo si la actualización en línea o la actualización sin conexión con un solo clic no funcionan. Las máquinas virtuales de plataforma se deben actualizar antes que las máquinas virtuales de recopilador. Sin embargo, debe ponerse en contacto con el soporte de VMware antes de iniciar la actualización sin conexión mediante la CLI.

En un entorno de clúster, la operación de actualización solo debe realizarse desde el nodo Platform1 (P1); los demás nodos de plataforma del clúster se actualizan automáticamente. Sin embargo, debe actualizar cada recopilador de forma individual.

Requisitos previos

- Puede que se produzcan errores en los pasos de actualización si no hay suficiente espacio en el directorio `/tmp`. Compruebe que cumple los siguientes requisitos de espacio de disco del servidor de plataforma y recopilador:
 - `/tmp`: 6 GB
 - `/home`: 2 GB
 - `/var`: 40 GB
- Asegúrese de que todos los nodos estén conectados. Si algún nodo está inactivo, no podrá activar la actualización.
- Cree las instantáneas de las máquinas virtuales.

- Tenga en cuenta los siguientes valores que se comprobarán después de la migración:
 - Recuento de máquinas virtuales
 - Máquina virtual en la que el recuento de instantáneas sea superior a 0
 - Recuento de reglas de firewall
 - Recuento de grupos de seguridad
 - Recuento de firewalls de NSX

Procedimiento

- 1 Descargue el archivo de paquete de actualización necesario de [My VMware](#).
- 2 Asegúrese de que el valor de MD5SUM del paquete descargado coincide con el valor de MD5SUM especificado en el sitio web de VMware.
- 3 Copie el paquete de actualización en la máquina virtual de la plataforma 1 de vRealize Network Insight y en todas las máquinas virtuales del recopilador.

- Para copiar el archivo de la máquina virtual de Linux a la máquina virtual de vRealize Network Insight, ejecute el comando `scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/.`
- Para copiar el archivo de la máquina virtual de Windows a la máquina virtual de vRealize Network Insight, ejecute el comando `pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/.`

Nota Use la utilidad `pscp` de <https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe>.

- 4 Inicie sesión en la plataforma 1 de vRealize Network Insight a través de la CLI mediante `consoleuser` y ejecute los siguientes comandos:
 - `package-installer copy --host localhost --user consoleuser --path /home/consoleuser/<filename>.upgrade.bundle`
 - `package-installer upgrade --name <filename>.upgrade.bundle`

Nota Primero debe actualizar la plataforma y, a continuación, iniciar la actualización del recopilador.

- 5 Vuelva a ejecutar el comando `package-installer upgrade` después de que se reinicie el programa de instalación como parte de la actualización del sistema operativo.

Importante Si se produce un error de tiempo de espera agotado de la sesión de SSH, deberá consultar `/var/log/arkin/centralized_upgrade.log` para determinar si el reinicio ya ocurrió. Si el reinicio es correcto, debe volver a ejecutar el comando `package-installer upgrade`.

- 6 Inicie sesión en cada nodo de recopilador mediante la CLI y realice la actualización mediante los mismos comandos que se utilizaron para la actualización de la plataforma.

Nota Puede actualizar todos los recopiladores de forma simultánea.

- 7 Compruebe la versión actualizada con el comando `show-version`.

Desinstalación de vRealize Network Insight

6

vRealize Network Insight se desinstala a través de vSphere Web Client.

Procedimiento

1 Si puede acceder al portal web de vRealize Network Insight, haga lo siguiente:

- a Inicie sesión en el portal web de vRealize Network Insight.
- b Vaya a **Configuración > Cuentas y orígenes de datos**.
- c Apague y elimine todos los orígenes de datos.

Si el origen de datos de vCenter se elimina, también lo hará la configuración de IPFIX (si se definió) en VDS. De manera similar, si se elimina el origen de datos de NSX Manager, se eliminará también la configuración de IPFIX del monitor de flujos de NSX.

2 Si no puede acceder al portal web de vRealize Network Insight, haga lo siguiente:

- a Si NetFlow (IPFIX) está habilitado en vCenter, elimine la dirección IP del recopilador de vRealize Network Insight de la configuración de IPFIX de VDS/DVPG. Consulte [Eliminar la dirección IP del recopilador cuando NetFlow está habilitado en vCenter](#).
- b Si IPFIX está habilitado en NSX, elimine la configuración de supervisión de flujos de dirección IP del recopilador de vRealize Network Insight. Consulte [Eliminar la dirección IP del recopilador cuando NetFlow está habilitado en NSX](#).
- c Si NetFlow está configurado en conmutadores físicos para enviar NetFlow al recopilador de NetFlow de vRealize Network Insight, modifique la configuración en los conmutadores para que dejen de enviar esa información de NetFlow.

3 Si se crearon reglas de enrutamiento o de firewall específicas para permitir o enrutar el tráfico hacia las máquinas virtuales de vRealize Network Insight y desde estas, elimínelas.

4 Por motivos de seguridad, limpie las credenciales de acceso utilizadas para configurar orígenes de datos en vRealize Network Insight.

5 Apague y elimine las máquinas virtuales de plataforma y todos los recopiladores de vRealize Network Insight.

Eliminar la dirección IP del recopilador cuando NetFlow está habilitado en vCenter

Si NetFlow (IPFIX) está habilitado en vCenter, utilice este procedimiento para eliminar la dirección IP del recopilador de vRealize Network Insight de la configuración de IPFIX del servidor dedicado virtual (VDS)/grupo de puertos virtuales distribuidos (DVPG).

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Vaya a **Inicio > Redes**.
- 3 En el panel izquierdo, seleccione el **VDS** y haga clic en **Configurar > Editar**.
- 4 En el campo **Dirección IP del recopilador**, elimine los detalles de dirección IP del recopilador de vRealize Network Insight.
- 5 En el campo **Puerto del recopilador**, elimine los detalles del puerto.
- 6 Haga clic en **Aceptar**.
Debe esperar unos dos minutos antes de continuar con el siguiente paso.
- 7 Seleccione el DVPG de este VDS y haga clic en **Configurar > Directivas > Editar**.
- 8 En el campo **NetFlow**, seleccione **Deshabilitar** en el menú desplegable.
- 9 Compruebe la configuración y haga clic en **Aplicar**.

Pasos siguientes

Vuelva a realizar los pasos para cada VDS y sus correspondientes DVPG para los que IPFIX está habilitado, y eliminar así la dirección IP del recopilador de vRealize Network Insight.

Eliminar la dirección IP del recopilador cuando NetFlow está habilitado en NSX

Si NetFlow (IPFIX) está habilitado en NSX, utilice este procedimiento para eliminar la configuración de supervisión del flujo de direcciones IP del recopilador de vRealize Network Insight (vRealize Network Insight).

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Inicio > Redes y seguridad > Herramientas > Supervisión de flujo > Configuración**.
- 3 En **Estado de la colección de flujos global**, haga clic en **Deshabilitar**.
- 4 Para deshabilitar la conexión del flujo, haga clic en **IPFIX**.
- 5 En la pestaña **IPFIX**, seleccione la **Dirección IP del recopilador** y haga clic en **Eliminar**.

- 6 Si no hay más direcciones IP a la izquierda, haga clic en **Editar** y desactive la casilla de verificación **Habilitar configuración de IPFIX**.
- 7 Haga clic en **Guardar**.