

Guía de administración de NSX-T Data Center

Modificado el 6 mayo de 2022
VMware NSX-T Data Center 2.5

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 © 2022 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Acerca de administrar VMware NSX-T Data Center 13

1 Descripción general de NSX Manager 14

2 Puertas de enlace de nivel 0 17

Agregar una puerta de enlace de nivel 0 18

Crear una lista de prefijos IP 21

Crear una lista de comunidad 23

Configurar una ruta estática 24

Crear un mapa de rutas 24

Uso de expresiones regulares para hacer coincidir las listas de comunidades al agregar mapas de rutas 27

Configurar BGP 28

Configurar BFD 31

Configurar el reenvío de Capa 3 para IPv6 32

Crear perfiles de SLAAC y DAD para la asignación de direcciones IPv6 33

3 Puerta de enlace de nivel 1 35

Agregar una puerta de enlace de nivel 1 35

4 Segmentos 38

Perfiles de segmentos 38

Información sobre el perfil de segmentos de calidad de servicio 39

Información sobre el perfil de segmentos de detección de direcciones IP 42

Información sobre el perfil de segmentos de Spoofguard 44

Información sobre el perfil de segmento de seguridad del segmento 46

Información sobre el perfil de segmentos de detección de direcciones MAC 48

Agregar un segmento 50

5 Red privada virtual (VPN) 52

Información de VPN de IPSec 53

Usar una VPN de IPSec basada en directivas 54

Usar una VPN de IPSec basada en rutas 55

Comprender la VPN de capa 2 56

Agregar servicios de VPN 57

Agregar un servicio de VPN de IPSec 59

Agregar un servicio VPN de Capa 2 61

Agregar sesiones de VPN de IPSec 63

Agregar una sesión de IPSec basada en directivas	64
Agregar una sesión de IPSec basada en rutas	67
Información sobre las suites de cumplimiento admitidas	72
Fijación de MSS de TCP	72
Agregar sesiones de VPN de capa 2	73
Agregar una sesión del servidor VPN de capa 2	73
Agregar una sesión de cliente VPN de Capa 2	76
Descargar el archivo de configuración de VPN de capa 2 de lado remoto	77
Agregar endpoints locales	79
Agregar perfiles	80
Agregar perfiles de IKE	80
Agregar perfiles de IPSec	83
Agregar perfiles de DPD	86
Agregar una instancia de Edge autónoma como cliente VPN de Capa 2	87
Comprobar el estado realizado de una sesión de VPN de IPSec	90
Supervisar y solucionar problemas de sesiones de VPN	93
6 Traducción de direcciones de red	94
Configurar NAT en una puerta de enlace	94
7 Equilibrio de carga	97
Conceptos clave sobre el equilibrador de carga	98
Ajustar la escala de los recursos del equilibrador de carga	98
Funciones admitidas del equilibrador de carga	99
Topologías de equilibrador de carga	100
Configurar los componentes del equilibrador de carga	102
Agregar equilibradores de carga	102
Agregar un monitor activo	104
Agregar un monitor pasivo	108
Agregar un grupo de servidores	109
Configurar los componentes del servidor virtual	114
Grupos creados para grupos de servidores y servidores virtuales	139
8 Directivas de reenvío	140
Agregar o editar directivas de reenvío	141
9 Administración de direcciones IP (IP Address Management, IPAM)	143
Agregar una zona de DNS	143
Agregar un servicio de reenviador DNS	144
Agregar un servidor DHCP	145
Configurar un servidor de retransmisión DHCP para una puerta de enlace de nivel 0 o nivel 1	146

[Agregar un grupo de direcciones IP](#) 147

[Agregar un bloque de direcciones IP](#) 148

10 Seguridad 149

[Información general de la configuración de seguridad](#) 149

[Terminología de seguridad](#) 150

[Firewall de identidad](#) 150

[Flujo de trabajo del firewall de identidad](#) 151

[Perfil de contexto de Capa 7](#) 154

[Flujo de trabajo de reglas de firewall de Capa 7](#) 156

[Atributos](#) 157

[Firewall distribuido](#) 161

[Borradores de firewall](#) 162

[Agregar un firewall distribuido](#) 164

[Registros de paquetes de firewall distribuido](#) 169

[Seleccionar una estrategia de conectividad predeterminada](#) 171

[Administrar una lista de exclusión de firewall](#) 172

[Filtrar dominios específicos \(FQDN/URL\)](#) 172

[Ampliar las directivas de seguridad a las cargas de trabajo físicas](#) 174

[Conjuntos de direcciones compartidas](#) 181

[Seguridad de red de este a oeste: cadena de servicios de terceros](#) 181

[Conceptos clave de la protección de red de Este a Oeste](#) 182

[Requisitos de NSX-T Data Center para el tráfico de este a oeste](#) 183

[Tareas de alto nivel para la seguridad de red de Este a Oeste](#) 183

[Implementar un servicio de introspección de tráfico de este a oeste](#) 184

[Agregar un perfil de servicio](#) 186

[Agregar una cadena de servicios](#) 186

[Agregar reglas de redirección para el tráfico de este a oeste](#) 188

[Configurar un firewall de puerta de enlace](#) 190

[Agregar una regla y una directiva de firewall de puerta de enlace](#) 190

[Seguridad de red de norte a sur: inserción de servicio de terceros](#) 193

[Tareas de alto nivel para la seguridad de red de Norte a Sur](#) 193

[Implementar un servicio de introspección de tráfico de norte a sur](#) 194

[Configurar el redireccionamiento de tráfico](#) 196

[Agregar reglas de redireccionamiento para el tráfico de norte a sur](#) 197

[Supervisar el redireccionamiento de tráfico](#) 199

[Protección de endpoints](#) 199

[Protección de endpoints](#) 199

[Configurar la protección de endpoints](#) 204

[Administrar la protección de endpoints](#) 221

[Perfiles de seguridad](#) 235

- Crear un temporizador de sesión 235
- Protección contra inundación 237
- Configurar la seguridad de DNS 240
- Administrar prioridad grupo-perfil 241

11 Inventario 243

- Agregar un servicio 243
- Agregar un grupo 244
- Agregar un perfil de contexto 246

12 Supervisión 248

- Agregar un perfil de IPFIX para firewall 248
- Agregar un perfil de IPFIX para conmutador 249
- Agregar un recopilador IPFIX 251
- Agregar un perfil de creación de reflejo del puerto 251
- Protocolo de administración de red simple (SNMP) 252
- Utilizar vRealize Log Insight para supervisar el sistema 253
- Utilizar vRealize Operations Manager para supervisar el sistema 254
- Utilizar vRealize Network Insight Cloud para la supervisión del sistema 258
- Herramientas de supervisión avanzadas 273
 - Consultar información sobre la conexión de puertos 273
 - Traceflow 273
 - Supervisar las sesiones de creación de reflejo del puerto 276
 - Configurar filtros para un sesión de creación de reflejo del puerto 280
 - Configurar IPFIX 281
 - Supervisar la actividad de un puerto del conmutador lógico 451

13 Conmutadores lógicos 452

- Información sobre los modos de replicación del marco BUM 453
- Crear un conmutador lógico 455
- Conectar una VM a un conmutador lógico 456
 - Adjuntar una máquina virtual alojada en vCenter Server a un conmutador lógico NSX-T Data Center 457
 - Adjuntar una VM alojada en ESXi independiente a un conmutador lógico de NSX-T Data Center 458
 - Adjuntar una máquina virtual alojada en KVM a un conmutador lógico NSX-T Data Center 464
- Crear un puerto de conmutador lógico 465
- Probar la conectividad de Capa 2 466
- Crear un conmutador lógico VLAN para el vínculo superior de NSX Edge 469
- Perfiles de conmutación para conmutadores lógicos y puertos lógicos 471
 - Información sobre el perfil de conmutación de QoS 473

Información sobre el perfil de conmutación de creación de reflejo del puerto	475
Información sobre el perfil de conmutación de detección de direcciones IP	478
Información sobre SpoofGuard	481
Información sobre el perfil de conmutación de seguridad del conmutador	483
Información sobre el perfil de conmutación de gestión de direcciones MAC	485
Asociar un perfil personalizado a un conmutador lógico	487
Asociar un perfil personalizado a un puerto lógico	489
Pila de red mejorada	490
Asignar automáticamente núcleos lógicos de ENS	490
Configurar el enrutamiento entre VLAN invitadas	491
Puente de Capa 2	493
Crear un perfil de puente Edge	493
Configurar el puente basado en Edge	494
Crear un conmutador lógico respaldado por puentes de Capa 2	497

14 Enrutadores lógicos 500

Enrutador lógico de nivel 1	500
Crear un enrutador lógico de nivel 1	502
Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1	504
Agregar un puerto de VLAN en un enrutador lógico de nivel 0 o de nivel 1	505
Configurar anuncios de rutas en un enrutador lógico de nivel 1	505
Configurar una ruta estática de enrutador lógico de nivel 1	507
Crear un enrutador lógico de nivel 1 independiente	509
Enrutador lógico de nivel 0	511
Crear un enrutador lógico de nivel 0	513
Adjuntar nivel 0 y nivel 1	514
Conectar un enrutador lógico de nivel 0 a un conmutador lógico VLAN para el vínculo superior de NSX Edge	517
Agregar un puerto de bucle invertido al enrutador	520
Agregar un puerto de VLAN en un enrutador lógico de nivel 0 o de nivel 1	521
Configurar una ruta estática	521
Opciones de configuración de BGP	525
Configurar BFD en un enrutador lógico de nivel 0	531
Habilitar la redistribución de rutas en el enrutador lógico de nivel 0	532
Información sobre el enrutamiento ECMP	535
Crear una lista de prefijos IP	539
Crear una lista de comunidad	540
Crear un mapa de rutas	541
Configurar el temporizador de reenvíos	542

15 NAT avanzado 544

Traducción de direcciones de red	544
----------------------------------	-----

- NAT de nivel 1 546
- NAT de nivel 0 553
- NAT reflexiva 554

16 Agrupación de objetos avanzada 558

- Crear un conjunto de direcciones IP 558
- Crear un grupo de direcciones IP 559
- Crear un conjunto de direcciones MAC 559
- Crear un grupo NSGroup 560
- Configurar servicios y grupos de servicios 562
 - Crear un servicio NSService 563
- Administrar las etiquetas de una máquina virtual 563

17 DHCP avanzado 565

- DHCP 565
 - Crear un perfil de servidor DHCP 566
 - Crear un servidor DHCP 566
 - Adjuntar un servidor DHCP a un conmutador lógico 567
 - Desasociar un servidor DHCP de un conmutador lógico 567
 - Crear un perfil de retransmisión DHCP 568
 - Crear un servicio de retransmisión DHCP 568
 - Agregar un servicio de retransmisión de DHCP a un puerto de enrutador lógico 568
 - Eliminar una concesión de DHCP 569
- Servidores proxy de metadatos 569
 - Agregar un servidor proxy de metadatos 570
 - Asociar un servidor proxy de metadatos a un conmutador lógico 571
 - Desconectar un servidor proxy de metadatos de un conmutador lógico 571

18 Administración de direcciones IP avanzada 573

- Administrar los bloques de IP 573
- Administrar subredes para bloques de IP 574

19 Equilibrio de carga avanzado 575

- Conceptos clave sobre el equilibrador de carga 576
- Configurar componentes del equilibrador de carga 577
 - Crear un equilibrador de carga 577
 - Configurar un monitor de estado activo 578
 - Configurar los monitores de estado pasivos 582
 - Agregar un grupo de servidores para el equilibrio de carga 584
 - Configuración de los componentes de servidor virtual 587

20 Firewall avanzado 610

- Agregar o eliminar una regla de firewall de un enrutador lógico 610
- Configurar el firewall de un puerto de puente del conmutador lógico 611
- Secciones y reglas de firewall 612
 - Habilitar y deshabilitar el firewall distribuido 612
 - Agregar una sección de reglas de firewall 613
 - Eliminar una sección de reglas de firewall 614
 - Habilitar y deshabilitar reglas de sección 614
 - Habilitar y deshabilitar reglas de registro 615
 - Configurar una lista de exclusión en el firewall 615
- Acerca de las reglas de firewall 615
 - Agregar una regla de firewall 617
 - Eliminar una regla de firewall 620
 - Editar la regla de Distributed Firewall predeterminada 620
 - Cambiar el orden de una regla de firewall 621
 - Filtrar reglas de firewall 621

21 Operaciones y administración 623

- Ver los paneles de control de supervisión 624
- Ver el uso y la capacidad de las categorías de objetos 626
- Comprobar el estado de realización de un cambio de configuración 628
- Buscar objetos 632
- Filtrar por atributos de objeto 634
- Agregar un administrador de equipos 634
- Agregar una instancia de Active Directory 637
- Agregar un servidor LDAP 638
- Sincronizar Active Directory 639
- Administrar las cuentas de usuarios y el control de acceso basado en funciones 640
 - Administrar una contraseña de usuario 640
 - Restablecer las contraseñas de un dispositivo 641
 - Configuración de la directiva de autenticación 643
 - Obtener la huella digital del certificado desde un host de vIDM 644
 - Configurar la integración de VMware Identity Manager 644
 - Validar la funcionalidad de VMware Identity Manager 647
 - Sincronización de hora entre NSX Manager, vIDM y componentes relacionados 649
 - Control de acceso basado en funciones 650
 - Agregar una asignación de funciones o la identidad principal 662
- Restaurar y hacer copias de seguridad de NSX Manager 665
 - Configurar copias de seguridad 665
 - Eliminar las copias de seguridad antiguas 667
 - Lista de las copias de seguridad disponibles 668

Restaurar una copia de seguridad	668
Copia de seguridad y restauración durante la actualización	671
Quitar una extensión NSX-T Data Center de vCenter Server	672
Administrar el clúster de NSX Manager	672
Ver la configuración y el estado del clúster de NSX Manager	673
Apagar y encender el clúster de NSX Manager	676
Reiniciar una instancia de NSX Manager	676
Cambiar la dirección IP de NSX Manager	676
Cambiar el tamaño de un nodo de NSX Manager	678
Agregar y quitar un nodo de transporte de host ESXi en instancias de vCenter Server	679
Reemplazar un nodo de transporte de NSX Edge en un clúster de NSX Edge	680
Reemplazar un nodo de transporte de NSX Edge mediante la interfaz de usuario de NSX Manager	680
Reemplazar un nodo de transporte de NSX Edge mediante la API	681
Recuperar NSX-T cuando se pierde vCenter Server y no se puede recuperar	683
Implementación multisitio de NSX-T Data Center	684
Configurar dispositivos	692
Agregar una clave de licencia y generar un informe de uso de licencias	693
Configurar certificados	694
Importar un certificado	694
Crear un archivo de solicitud de firma del certificado	695
Importar un certificado de CA	697
Crear certificados de firma automática	697
Reemplazar el certificado de un nodo de NSX Manager o una IP virtual de clúster de NSX Manager	698
Importar una lista de revocación de certificados	699
Cómo configurar NSX Manager para recuperar una lista de revocación de certificados	700
Importar un certificado para una CSR	701
Almacenamiento de certificados públicos y claves privadas	701
Configuración basada en cumplimiento	701
Ver informe de estado de cumplimiento	702
Códigos de informe de estado de cumplimiento	703
Configurar el modo de cumplimiento global de FIPS para el equilibrador de carga	706
Recopilar paquetes de soporte	709
Mensajes de registro y códigos de error	710
Configurar registros remotos	712
Identificadores de mensajes de registro	719
Solucionar problemas de syslog	721
Configurar el registro serie en una máquina virtual de dispositivo	721
Programa de mejora de la experiencia de cliente	722
Editar la configuración del programa de mejora de la experiencia de cliente	722
Agregar etiquetas a un objeto	723

- Buscar la huella digital SSH de un servidor remoto 724
- Ver datos de aplicaciones que se ejecutan en máquinas virtuales 725
- Configurar un equilibrador de carga externo 726

22 Uso de NSX Cloud 727

- Un paseo rápido por Cloud Service Manager 727
 - Nubes 728
 - Sistema 732
- Detección de amenazas mediante la directiva de cuarentena de NSX Cloud 735
 - Directiva de cuarentena en Modo forzado de NSX 736
 - Directiva de cuarentena en Modo forzado de nube nativa 741
 - Incluir máquinas virtuales en la lista blanca 742
- Modo forzado de NSX 743
 - Sistemas operativos admitidos actualmente para máquinas virtuales de carga de trabajo 743
 - Incorporación de máquinas virtuales a Modo forzado de NSX 744
 - Administrar máquinas virtuales en Modo forzado de NSX 754
- Modo forzado de nube nativa 755
 - Administrar máquinas virtuales en Modo forzado de nube nativa 755
- Funciones de NSX-T Data Center admitidas por NSX Cloud 760
 - Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública 761
 - Uso de los servicios nativos de la nube 765
 - Inserción de servicios para la nube pública 767
 - Habilitar NAT en máquinas virtuales administradas por NSX 774
 - Habilitar el reenvío de syslog 775
 - Configurar una VPN en el modo forzado de NSX 775
- Preguntas frecuentes 781

23 Uso de NSX Intelligence 784

- Introducción a NSX Intelligence 784
 - Paseo por la página de inicio de NSX Intelligence 785
 - Familiarizarse con los elementos gráficos de NSX Intelligence 787
- Vistas y flujos de NSX Intelligence 789
 - Trabajar con la vista Grupos 790
 - Trabajar con la vista Máquinas virtuales 795
 - Trabajar con los flujos de tráfico 797
- Trabajar con las recomendaciones de NSX Intelligence 799
 - Información sobre las recomendaciones de NSX Intelligence 799
 - Generar una nueva recomendación de NSX Intelligence 800
 - Revisar y publicar una recomendación generada 802
- Copia de seguridad y restauración de NSX Intelligence 804
 - Configurar las copias de seguridad de NSX Intelligence 805

Realizar una copia de seguridad de NSX Intelligence	806
Restaurar copias de seguridad de NSX Intelligence	807
Resolución de problemas de NSX Intelligence	808
Comprobar el estado del dispositivo de NSX Intelligence	808
Recopilar paquetes de soporte de NSX Intelligence	813

Acerca de administrar VMware NSX-T Data Center

En la *Guía de administración de NSX-T Data Center* se proporciona información sobre la configuración y la administración de redes en VMware NSX-T™ Data Center, incluido cómo crear puertos y conmutadores lógicos, cómo configurar redes para enrutadores lógicos con niveles, NAT, firewalls, SpoofGuard, agrupaciones y DHCP. También se describe cómo configurar NSX Cloud.

Público objetivo

Esta información está dirigida a quien desee configurar NSX-T Data Center. La información está escrita para administradores de sistemas Windows o Linux con experiencia y que estén familiarizados con la tecnología de máquinas virtuales, las redes y las operaciones de seguridad.

Glosario de publicaciones técnicas de VMware

Publicaciones técnicas de VMware proporciona un glosario de términos que podrían resultarle desconocidos. Puede consultar la definición de los términos que se utilizan en la documentación técnica de VMware en <https://www.vmware.com/topics/glossary>.

Descripción general de NSX Manager

1

NSX Manager proporciona una interfaz de usuario basada en web en la que puede administrar el entorno de NSX-T. También aloja el servidor de API que procesa las llamadas de API.

La interfaz de usuario web de NSX Manager proporciona dos métodos para configurar recursos.

- Interfaz de directivas: pestañas **Redes**, **Seguridad**, **Inventario** y **Planificar y solucionar problemas**.
- Interfaz avanzada: pestaña **Opciones avanzadas de redes y seguridad**.

Cuándo utilizar la interfaz de directivas y la interfaz avanzada

Sea coherente respecto a la interfaz de usuario que utilice. Existen algunos motivos para usar una interfaz de usuario en lugar de la interfaz avanzada.

- Si va a implementar un nuevo entorno de con NSX-T Data Center 2.4 o una versión posterior, el uso de la nueva interfaz de usuario basada de directivas para crear y administrar su entorno es la mejor opción en la mayoría de las situaciones.
 - Algunas funciones no están disponibles en la interfaz de usuario basada en directivas. Si necesita estas funciones, utilice la interfaz de usuario avanzada para todas las configuraciones.
- Si va a actualizar a NSX-T Data Center 2.4 o una versión posterior, continúe para realizar cambios de configuración mediante la interfaz de usuario **Opciones avanzadas de redes y seguridad**.

Tabla 1-1. Cuándo utilizar la interfaz de directivas y la interfaz avanzada


Interfaz de directivas	Interfaz avanzada
La mayoría de las nuevas implementaciones deben utilizar la interfaz basada en directivas.	Las implementaciones que se crearon con la interfaz avanzada, por ejemplo, se actualizan desde versiones anteriores a la interfaz basada en directivas.
Implementaciones de NSX Cloud	Implementaciones que se integran con otros complementos. Por ejemplo, NSX Container Plug-in, OpenStack y otras plataformas de administración de la nube.

Tabla 1-1. Cuándo utilizar la interfaz de directivas y la interfaz avanzada (continuación)

Interfaz de directivas	Interfaz avanzada
<p>Funciones de redes disponibles solo en la interfaz de directivas:</p> <ul style="list-style-type: none"> ■ Servicios de DNS y zonas de DNS ■ VPN ■ Directivas de reenvío para NSX Cloud 	<p>Funciones de redes disponibles solo en la interfaz avanzada:</p> <ul style="list-style-type: none"> ■ Temporizador de reenvío ■ Rutas estáticas con BFD e interfaz como salto siguiente ■ Proxy de metadatos ■ Servidor DHCP adjunto a un segmento aislado y enlace estático
<p>Funciones de seguridad disponibles solo en la interfaz de directivas:</p> <ul style="list-style-type: none"> ■ Protección de endpoints ■ Introspección de red (inserción de servicios de este a oeste) ■ Perfiles de contexto <ul style="list-style-type: none"> ■ Aplicaciones de capa 7 ■ FQDN ■ Nuevo diseño de firewall distribuido y firewall de puerta de enlace <ul style="list-style-type: none"> ■ Categorías ■ Reglas de autoservicio ■ Borradores 	<p>Funciones de seguridad disponibles solo en la interfaz avanzada:</p> <ul style="list-style-type: none"> ■ Umbrales de CPU y de memoria ■ Firewall de puente ■ Reglas de firewall distribuido basadas en direcciones IP en el origen y el destino

Uso de la interfaz de directivas

Si decide utilizar la interfaz de directivas, utilícela para crear todos los objetos. No utilice la interfaz de opciones avanzadas para crear objetos.

Puede utilizar la interfaz avanzada para modificar los objetos que se crearon en la interfaz de directivas. La configuración de un objeto creado con directivas puede incluir un vínculo de **Configuración avanzada**. Este vínculo le dirige a la interfaz avanzada en la que puede ajustar la configuración. También puede ver los objetos creados por directivas directamente en la interfaz avanzada. Los ajustes administrados por directiva, pero que están visibles en la interfaz avanzada, muestra este icono: . No se pueden modificar desde la interfaz de usuario avanzada.

Dónde encontrar las interfaces de directivas y las interfaces avanzadas

Las interfaces basadas en directivas y las interfaces avanzadas aparecen en distintas partes de la interfaz de usuario de NSX Manager y utilizan diferentes URI de API.

Tabla 1-2. Interfaces de directivas e interfaces avanzadas

Interfaz de directivas	Interfaz avanzada
<ul style="list-style-type: none"> ■ Pestaña Redes ■ Pestaña Seguridad ■ Pestaña Inventario ■ Pestaña Planificar y solucionar problemas 	Pestaña Opciones avanzadas de redes y seguridad
URI de API que comienzan con <code>/policy/api</code>	URI de API que comienzan con <code>/api</code>

Nota La pestaña **Sistema** se utiliza para todos los entornos. Si modifica los nodos de Edge, los clústeres de Edge o las zonas de transporte, los cambios pueden tardar hasta 5 minutos en verse en la interfaz de usuario basada en directivas. Puede sincronizar inmediatamente mediante `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload`.

Para obtener más información sobre el uso de la API de directiva, consulte la [Guía de introducción de la API de directiva de NSX-T](#).

Nombres de los objetos creados en las interfaces de directiva y avanzada

Los objetos que cree tienen nombres diferentes según la interfaz que se utilizó para crearlos.

Tabla 1-3. Nombres de objetos

Objetos creados mediante la interfaz de directivas	Objetos creados mediante la interfaz avanzada
Segmento	Conmutador lógico
Puerta de enlace de nivel 1	Enrutador lógico de nivel 1
Puerta de enlace de nivel 0	Enrutador lógico de nivel 0
Grupo	Grupo de NS, conjuntos de direcciones IP, conjuntos de direcciones MAC
Directiva de seguridad	Sección de firewall
Regla	Regla de firewall
Firewall de puerta de enlace	Firewall de Edge

Puertas de enlace de nivel 0

2

Una puerta de enlace de nivel 0 ejecuta las funciones de un enrutador lógico de nivel 0. La puerta procesa el tráfico entre las redes lógicas y físicas.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

Un nodo de Edge solo es compatible con una puerta de enlace o un enrutador lógico de nivel 0. Al crear una puerta de enlace o un enrutador lógico de nivel 0, asegúrese de no crear un número de puertas de enlace o enrutadores lógicos de nivel 0 superior al número de nodos de Edge del clúster de NSX Edge.

Nota En la pestaña **Opciones avanzadas de redes y seguridad**, el término Enrutador lógico de nivel 0 se utiliza para hacer referencia a una puerta de enlace de nivel 0.

Este capítulo incluye los siguientes temas:

- [Agregar una puerta de enlace de nivel 0](#)
- [Crear una lista de prefijos IP](#)
- [Crear una lista de comunidad](#)
- [Configurar una ruta estática](#)
- [Crear un mapa de rutas](#)
- [Uso de expresiones regulares para hacer coincidir las listas de comunidades al agregar mapas de rutas](#)
- [Configurar BGP](#)
- [Configurar BFD](#)
- [Configurar el reenvío de Capa 3 para IPv6](#)
- [Crear perfiles de SLAAC y DAD para la asignación de direcciones IPv6](#)

Agregar una puerta de enlace de nivel 0

Una puerta de enlace de nivel 0 tiene conexiones de vínculo inferior con puertas de enlace de nivel 1, y conexiones de vínculo superior con redes físicas.

Puede configurar el modo de alta disponibilidad (High Availability, HA) de una puerta de enlace de nivel 0 en activo-activo o en activo-en espera. Los siguientes servicios solo se admiten en el modo activo-en espera:

- NAT
- Equilibrio de carga
- Firewall con estado
- VPN

Las puertas de enlace de nivel 0 y nivel 1 admiten las siguientes configuraciones de direccionamiento para todas las interfaces (vínculos superiores, puertos de servicio y vínculos inferiores) en las topologías de un solo nivel y de varios niveles:

- Solo IPv4
- Solo IPv6
- Pila dual: IPv4 e IPv6

Para usar direcciones IPv6 o de pila dual, habilite **IPv4 e IPv6** como el modo de redireccionamiento de capa 3 en **Redes > Configuración de red > Configuración de redes globales**.

Si configura la redistribución de rutas para la puerta de enlace de nivel 0, puede elegir entre dos grupos de orígenes: subredes de nivel 0 y subredes de nivel 1 anunciadas. Los orígenes del grupo de subredes de nivel 0 son:

Tipo de origen	Descripción
Interfaces y segmentos conectados	Incluyen subredes de interfaz externa, subredes de interfaz de servicio y subredes de segmentos conectadas a la puerta de enlace de nivel 0.
Rutas estáticas	Son rutas estáticas configuradas en la puerta de enlace de nivel 0.
IP de NAT	Son direcciones IP de NAT propiedad de la puerta de enlace de nivel 0 que se detectan a partir de reglas NAT configuradas en la puerta de enlace de nivel 0.
IP local de IPSec	Es la dirección IP del endpoint local de IPSEC que se usa para establecer sesiones de VPN.
IP del reenviador de DNS	Es la IP del agente de escucha para las consultas de DNS de clientes que también se utiliza como IP de origen para reenviar las consultas de DNS al servidor DNS upstream.

Los orígenes del grupo de subredes de nivel 1 anunciadas son:

Tipo de origen	Descripción
Interfaces y segmentos conectados	Estas incluyen subredes de segmentos conectadas a las subredes de la puerta de enlace de nivel 1 y de la interfaz de servicio configuradas en la puerta de enlace de nivel 1.
Rutas estáticas	Son rutas estáticas configuradas en la puerta de enlace de nivel 1.
IP de NAT	Son direcciones IP de NAT propiedad de la puerta de enlace de nivel 1 que se detectan a partir de reglas NAT configuradas en la puerta de enlace de nivel 1.
VIP de equilibrador de carga	Es la dirección IP del servidor virtual de equilibrio de carga.
IP de SNAT del equilibrador de carga	Es la dirección IP o el rango de direcciones IP que utiliza el equilibrador de carga para la NAT de origen.
IP del reenviador de DNS	Es la IP del agente de escucha para las consultas de DNS de clientes que también se utiliza como IP de origen para reenviar las consultas de DNS al servidor DNS upstream.
Endpoint local de IPSec	Es la dirección IP del endpoint local de IPSec.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Haga clic en **Agregar puerta de enlace de nivel 0**.
- 4 Introduzca un nombre para la puerta de enlace.
- 5 Seleccione un modo de HA.

El modo predeterminado es activo-activo. En el modo activo/activo, la carga del tráfico se equilibra en todos los miembros. En el modo activo/espera, un miembro activo elegido procesa todo el tráfico. Si el miembro activo no realiza este proceso, se elige otro nuevo miembro para que sea activo.

Importante Después de crear la puerta de enlace, no podrá cambiar el modo de HA.

- 6 Si el modo de alta disponibilidad es activo-en espera, seleccione un modo de conmutación por error.

Opción	Descripción
Preferente	Si se produce un error en el nodo preferente y se soluciona, reemplazará al nodo del mismo nivel y se convertirá en el nodo activo. El estado de este nodo cambiará a en espera.
No preferente	Si se produce un error en el nodo preferente y se soluciona, comprobará si el nodo del mismo nivel es el activo. Si es así, el nodo preferente no reemplazará al nodo del mismo nivel y será el nodo que esté en espera.

- 7 (opcional) Seleccione un clúster de NSX Edge.
- 8 (opcional) Agregue una o varias etiquetas.

9 (opcional) Haga clic en **Configuración adicional**.

- a En el campo **Subred de tránsito interna**, introduzca una subred.

Esta será la subred que se utilizará para la comunicación entre los componentes de esta puerta de enlace. La subred predeterminada es 169.254.0.0/28.

- b En el campo **Subredes de tránsito TO-T1**, introduzca una o varias subredes.

Estas subredes se utilizan para la comunicación entre esta puerta de enlace y todas las puertas de enlace de nivel 1 vinculadas a ella. Después de crear esta puerta de enlace y vincularle una puerta de enlace de nivel 1, verá la dirección IP real asignada al vínculo en el lado de la puerta de enlace de nivel 0 y en el lado de la puerta de enlace de nivel 1. La dirección se muestra en **Configuración adicional > Vínculos del enrutador** en la página de la puerta de enlace de nivel 0 y en la página de la puerta de enlace de nivel 1. La subred predeterminada es 100.64.0.0/16.

- c Seleccione un **Perfil ND** y un **Perfil DAD** para la configuración de direcciones IPv6.

Estos perfiles se utilizan para establecer la configuración automática de direcciones sin estado (SLAAC) y la detección de direcciones duplicadas (DAD) de las direcciones IPv6. Se creará el perfil predeterminado.

10 Haga clic en **Guardar**.

11 Para configurar la redistribución de rutas, haga clic en **Redistribución de rutas** y luego en **Establecer**.

Seleccione uno o varios de los orígenes:

- Subredes de nivel 0: **Rutas estáticas, IP de NAT, IP local de IPSec, IP del reenviador de DNS y Interfaces y segmentos conectados**.

En **Interfaces y segmentos conectados**, puede seleccionar una o varias de las siguientes opciones: **Subred de interfaz de servicio, Subred de interfaz externa, Subred de interfaz de bucle invertido y Segmento conectado**.

- Subredes de nivel 1 anunciadas: **IP del reenviador de DNS, Rutas estáticas, VIP de equilibrador de carga, IP de NAT, IP de SNAT del equilibrador de carga, Endpoint local de IPSec y Interfaces y segmentos conectados**.

En **Interfaces y segmentos conectados**, puede seleccionar **Subred de interfaz de servicio** o **Segmento conectado**.

12 Para configurar interfaces, haga clic en **Interfaces** y luego en **Establecer**.

- a Haga clic en **Agregar interfaz**.
- b Introduzca un nombre.
- c Seleccione un tipo.

Si el modo de HA es activo-en espera, las opciones son **Externa, Servicio y Bucle invertido**. Si el modo de HA es activo-activo, las opciones son **Externa y Bucle invertido**.

- d Introduzca una dirección IP en formato CIDR.
 - e Seleccione un segmento.
 - f Si el tipo de interfaz no es **Servicio**, seleccione un nodo de NSX Edge.
 - g (opcional) Si el tipo de interfaz no es **Bucle invertido**, introduzca un valor de MTU.
 - h (opcional) Agregue etiquetas y seleccione un perfil ND.
- 13** (opcional) Si el modo de HA es activo-en espera, haga clic en **Establecer** junto a **Agregar configuración de VIP de alta disponibilidad** para configurar la VIP de HA.

Con la VIP de HA configurada, la puerta de enlace de nivel 0 estará operativa aunque haya un vínculo superior inactivo. El enrutador físico interactúa solo con la VIP de alta disponibilidad. La VIP de alta disponibilidad está pensada para funcionar con enrutamiento estático y no con BGP.

- a Haga clic en **Agregar configuración de VIP de alta disponibilidad**.
 - b Introduzca una dirección IP y una máscara de subred.

La subred VIP de HA debe ser la misma que la subred de la interfaz a la que está vinculada.
 - c Seleccione dos interfaces de dos nodos de Edge diferentes.
- 14** Haga clic en **Enrutamiento** para agregar listas de prefijos de IP, listas de comunidad, rutas estáticas y mapas de rutas.
- 15** Haga clic en **BGP** para configurar BGP.
- 16** Haga clic en **Configuración avanzada** para ir a la página **Opciones avanzadas de redes y seguridad > Enrutadores** para configurar los ajustes adicionales.
- a Para configurar el modo de reenvío de Capa 3, haga clic en la pestaña **Configuración global**.
 - b Haga clic en **Editar**.
 - c Seleccione **IPv4** o **IPv4 e IPv6**.

El valor predeterminado es IPv4 solo. No se admite el formato IPv6. Para habilitar IPv6, seleccione **IPv4 e IPv6**.
 - d Haga clic en **Guardar**.

Crear una lista de prefijos IP

Una lista de prefijos IP contiene una o varias direcciones IP que tienen asignados permisos de acceso para anunciar rutas. Las direcciones IP de esta lista se procesan de forma secuencial. Las listas de prefijos IP se incluyen a través de los filtros de vecino BGP o los mapas de rutas con dirección entrante o saliente.

Por ejemplo, puede agregar la dirección IP 192.168.100.3/27 a la lista de prefijos IP y no permitir que la ruta se redistribuya al enrutador ascendente. También puede agregar una dirección IP con los modificadores "igual o inferior a" (le) y "igual o superior a" (ge) para permitir o limitar la redistribución de rutas. Por ejemplo, los modificadores le 30 y ge 24 de 192.168.100.3/27 coinciden con las máscaras de subred iguales o superiores a 24 bits, e iguales o inferiores a 30 bits de largo.

Nota La acción predeterminada de una ruta es **Denegar**. Cuando cree una lista de prefijos para denegar o permitir rutas específicas, asegúrese de crear un prefijo de IP sin una dirección de red específica (seleccione **Cualquiera** en la lista desplegable) y elegir la acción **Permitir** si desea permitir otras rutas.

Requisitos previos

Compruebe que tenga una puerta de enlace de nivel 0 configurada. Consulte [Crear un enrutador lógico de nivel 0](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Enrutamiento**.
- 5 Haga clic en **Establecer** junto a **Lista de prefijos de IP**.
- 6 Haga clic en **Agregar lista de prefijos de IP**.
- 7 Introduzca un nombre para la lista de prefijos de IP.
- 8 Haga clic en **Establecer** para agregar los prefijos de IP.
- 9 Haga clic en **Agregar prefijo**.
 - a Introduzca una dirección IP en formato CIDR.
Por ejemplo, 192.168.100.3/27.
 - b (opcional) Establezca un rango de números de dirección IP en los modificadores **le** o **ge**.
Por ejemplo, establezca el valor 30 para el modificador **le** y el valor 24 para el modificador **ge**.
 - c Seleccione **Denegar** o **Permitir** en el menú desplegable.
 - d Haga clic en **Agregar**.
- 10 Repita el paso anterior para especificar prefijos adicionales.
- 11 Haga clic en **Guardar**.

Crear una lista de comunidad

Puede crear listas de comunidad de BGP para configurar mapas de rutas en función de estas.

Las listas de comunidad son listas de valores de atributos de comunidad definidas por el usuario. Estas listas se pueden utilizar para hacer coincidir o manipular el atributo de comunidades en los mensajes de actualización de BGP.

Se admiten tanto el atributo de comunidades de BGP (RFC 1997) como el atributo de las comunidades de gran tamaño (RFC 8092). El atributo de comunidades de BGP tiene un valor de 32 bits dividido en dos valores de 16 bits. El atributo de comunidades de gran tamaño de BGP tiene 3 componentes, cada uno con 4 octetos de longitud.

En mapas de ruta, podemos hacer coincidir o configurar el atributo de comunidades de BGP o de comunidades grandes. Con esta función, los operadores de red pueden implementar la directiva de red en función del atributo de comunidades de BGP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Enrutamiento**.
- 5 Haga clic en **Establecer** junto a **Lista de comunidad**.
- 6 Haga clic en **Agregar lista de comunidad**.
- 7 Escriba un nombre para la lista de comunidad.
- 8 Especifique una lista de comunidades. Para una comunidad normal, use el formato aa:nn (por ejemplo, 300:500). Para una comunidad grande, use el formato aa:bb:cc (por ejemplo, 11:22:33). Tenga en cuenta que la lista no puede contener comunidades normales y grandes. Debe incluir solo comunidades normales o solo comunidades grandes.

Además, puede seleccionar una o varias de las siguientes comunidades normales. Tenga en cuenta que no se pueden agregar si la lista contiene comunidades grandes.

- NO_EXPORT_SUBCONFED: no anuncia a pares EGBP.
- NO_ADVERTISE: no anuncia a ningún par.
- NO_EXPORT: no anuncia fuera de la confederación BGP.

- 9 Haga clic en **Guardar**.

Configurar una ruta estática

Puede configurar una ruta estática en la puerta de enlace de nivel 0 para redes externas. Tras configurar la ruta estática, no es necesario anunciar la ruta de nivel 0 a nivel 1, ya que las puertas de enlace de nivel 1 poseen de forma automática una ruta estática predeterminada hacia la puerta de enlace de nivel 0 a la que están conectadas.

Se admiten las rutas estáticas recursivas.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Enrutamiento**.
- 5 Haga clic en **Establecer** junto a **Rutas estáticas**.
- 6 Haga clic en **Agregar ruta estática**.
- 7 Introduzca un nombre y una dirección de red con el formato CIDR. Se admiten las rutas estáticas en función de IPv6. Los prefijos de IPv6 solo pueden tener un próximo salto de IPv6.
- 8 Haga clic en **Establecer próximos saltos** para agregar información de los próximos saltos.
- 9 Haga clic en **Agregar próximo salto**.
- 10 Introduzca una dirección IP.
- 11 Especifique la distancia administrativa.
- 12 Seleccione una interfaz de la lista desplegable.
- 13 Haga clic en el botón **Agregar**.

Pasos siguientes

Compruebe que la ruta estática está configurada correctamente. Consulte [Comprobar la ruta estática](#).

Crear un mapa de rutas

Un mapa de rutas es una secuencia de listas de prefijos IP, atributos de rutas BGP y una acción asociada. El enrutador analiza la secuencia para buscar una coincidencia de direcciones IP. Si hay alguna coincidencia, el enrutador realiza la acción y deja de analizar la secuencia.

Los mapas de rutas se pueden incluir en la redistribución de rutas y en el nivel de vecino BGP.

Requisitos previos

- Compruebe que se haya configurado una lista de prefijos de direcciones IP o una lista de comunidades. Consulte [Crear una lista de prefijos IP](#) o [Crear una lista de comunidad](#).
- Para obtener más información sobre cómo usar expresiones regulares para definir los criterios de coincidencia de mapa de ruta para las listas de comunidad, consulte [Uso de expresiones regulares para hacer coincidir las listas de comunidades al agregar mapas de rutas](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Enrutamiento**.
- 5 Haga clic en **Establecer** junto a **Mapas de rutas**.
- 6 Haga clic en **Agregar mapa de rutas**.
- 7 Introduzca un nombre y haga clic en **Establecer** para agregar criterios de coincidencia.
- 8 Haga clic en **Agregar criterios de coincidencia** para agregar uno o varios criterios de coincidencia.

9 Para cada criterio, seleccione **Prefijo de IP** o **Lista de comunidades** y haga clic en **Establecer** para especificar una o varias expresiones de coincidencia.

a Si seleccionó **Lista de comunidades**, especifique expresiones de coincidencia que definan cómo coinciden los miembros de las listas de comunidad. Para cada lista de comunidades, están disponibles las siguientes opciones de coincidencia:

- **HACER COINCIDIR CON CUALQUIERA:** realice la acción establecida en el mapa de rutas si coincide cualquiera de las comunidades de la lista de comunidades.
- **HACER COINCIDIR CON TODOS:** realice la acción establecida en el mapa de rutas si coinciden todas las comunidades de la lista de comunidades, independientemente del orden.
- **COINCIDENCIA EXACTA:** realice la acción establecida en el mapa de rutas si todas las comunidades de la lista de comunidades coinciden en el mismo orden.
- **COINCIDIR CON EXPRESIÓN REGULAR DE COMUNIDAD::** realice la acción establecida en el mapa de rutas si todas las comunidades regulares asociadas con el NRLI coinciden con la expresión regular.
- **COINCIDIR CON EXPRESIÓN REGULAR DE COMUNIDAD GRANDE:** realice la acción establecida en el mapa de rutas si todas las comunidades grandes asociadas con el NRLI coinciden con la expresión regular.

Debe utilizar el criterio de coincidencia **COINCIDIR CON EXPRESIÓN REGULAR DE COMUNIDAD** para hacer coincidir las rutas con las de las comunidades estándar, y **COINCIDIR CON EXPRESIÓN REGULAR DE COMUNIDAD GRANDE** para hacer coincidir las rutas con las comunidades grandes. Si desea permitir rutas que contengan la comunidad estándar o el valor de la comunidad grande, debe crear dos criterios de coincidencia. Si las expresiones de coincidencia se proporcionan en el mismo criterio de coincidencia, solo se permitirán las rutas que contengan las comunidades estándar y grandes.

Para cualquier criterio de coincidencia, las expresiones de coincidencia se aplican en una operación AND, lo que significa que todas las expresiones de coincidencia deben cumplirse para que se produzca una coincidencia. Si hay varios criterios de coincidencia, se aplican en una operación OR, lo que significa que se producirá una coincidencia si se cumple algún criterio de coincidencia.

10 Establezca atributos BGP.

Atributo BGP	Descripción
AS-path Prepend	Anteponga una ruta con uno o varios números de sistemas autónomos (autonomous system, AS) para que la ruta sea más larga y, por tanto, tenga menor preferencia.
MED	El atributo Discriminador de salida múltiple (Multi-Exit Discriminator, MED) indica a un par externo la ruta de preferencia a un AS.
Peso	Establece una ponderación que influye en la selección de las rutas. El rango es 0-65.535.

Atributo BGP	Descripción
Comunidad	<p>Especifique una lista de comunidades. Para una comunidad normal, use el formato aa:nn (por ejemplo, 300:500). Para una comunidad grande, use el formato aa:bb:cc (por ejemplo, 11:22:33). O utilice el menú desplegable para seleccionar uno de los siguientes atributos:</p> <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED: no anuncia a pares EBGp. ■ NO_ADVERTISE: no anuncia a ningún par. ■ NO_EXPORT: no anuncia fuera de la confederación BGP.
Preferencia local	Utilice este valor para elegir la ruta de acceso BGP externo saliente. Se prefiere la ruta de acceso con el valor más alto.

11 En la columna Acción, seleccione **Permitir** o **Denegar**.

Puede permitir o impedir que se anuncien las direcciones IP que coincidan con las listas de prefijos IP o las listas de la comunidades.

12 Haga clic en **Guardar**.

Uso de expresiones regulares para hacer coincidir las listas de comunidades al agregar mapas de rutas

Puede utilizar expresiones regulares para definir los criterios de coincidencia de mapas de ruta con las listas de comunidades. Las expresiones regulares de BGP se basan en las expresiones regulares de POSIX 1003.2.

Las siguientes expresiones son un subconjunto de expresiones regulares de POSIX.

Expresión	Descripción
.	Coincide con cualquier carácter individual.
*	Coincide con 0 o más ocurrencias del patrón.
+	Coincide con 1 o más ocurrencias del patrón.
?	Coincide con 0 o 1 ocurrencias del patrón.
^	Coincide con el principio de la línea.
\$	Coincide con el final de la línea.
—	Este carácter tiene significados especiales en expresiones regulares de BGP. Coincide con un espacio, coma, como delimitadores de conjunto { and } y como delimitadores de la confederación (and). También coincide con el principio y el final de la línea. Por lo tanto, este carácter se puede utilizar para una coincidencia de límites de valores. Este carácter se evalúa técnicamente como (^ [,{}()])\$).

A continuación se incluyen algunos ejemplos de cómo usar expresiones regulares en los mapas de rutas:

Expresión	Descripción
^101	Coincide con las rutas que tienen un atributo de comunidad que empieza por 101.
^[0-9]+	Coincide con las rutas que tienen un atributo de comunidad que empieza por un número entre 0 y 9 e incluye una o varias instancias de ese número.

Expresión	Descripción
.*	Coincide con las rutas que incluyen cualquiera o ningún atributo de comunidad.
.+	Coincide con las rutas que tienen cualquier valor de comunidad.
^\$	Coincide con rutas que no tienen ningún valor de comunidad o tienen valores nulos.

Configurar BGP

Para habilitar el acceso entre las máquinas virtuales y el mundo exterior, puede configurar una conexión BGP externa o interna (eBGP o iBGP) entre la puerta de enlace de nivel 0 y el enrutador de la infraestructura física.

Al configurar BGP, debe configurar un número local de sistema autónomo (Autonomous System, AS) para la puerta de enlace de nivel 0. También debe configurar el número de AS remoto.

Los vecinos de EBGP deben estar conectados directamente y en la misma subred que el vínculo superior de nivel 0. Si no están en la misma subred, se deberá utilizar los saltos múltiples BGP.

BGPv6 se admite para saltos únicos o múltiples. Un vecino BGPv6 solo admite direcciones IPv6. La redistribución, la lista de prefijos y los mapas de rutas son compatibles con los prefijos IPv6.

Las puertas de enlace de nivel 0 en modo activo-activo admiten iBGP de SR interno (enrutador de servicio). Si la puerta de enlace 1 no puede comunicarse con un enrutador físico en dirección norte, el tráfico se redirige a la puerta de enlace 2 del clúster activo-activo. Si la puerta de enlace 2 se puede comunicar con el enrutador físico, el tráfico entre la puerta de enlace 1 y el enrutador físico no se verá afectado.

La implementación de ECMP en NSX Edge se basa en las 5 tuplas del número de protocolo, la dirección de origen y de destino, y el puerto de origen y de destino.

La función iBGP presenta las siguientes capacidades y restricciones:

- Se admite la redistribución, las listas de prefijos y los mapas de rutas.
- No se admiten los reflectores de ruta.
- No se admite la confederación BGP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.

4 Haga clic en **BGP**.

- a Introduzca el número del AS local.

En el modo activo-activo, ya aparece completado el valor de ASN predeterminado, que es 65.000. En el modo activo-en espera, no hay un valor de ASN predeterminado.

- b Haga clic en el botón de alternancia **BGP** para habilitar o deshabilitar BGP.

En el modo activo-activo, **BGP** está habilitado de forma predeterminada. En el modo activo-en espera, **BGP** está habilitado de forma predeterminada.

- c Si esta puerta de enlace está en el modo activo-activo, haga clic en el botón de alternancia **iBGP de SR interno** para habilitar o deshabilitar el iBGP de SR interno. Esta opción está habilitada de forma predeterminada.

Si la puerta de enlace está en modo activo-en espera, esta función no está disponible.

- d Haga clic en el botón de alternancia **ECMP** para habilitar o deshabilitar ECMP.

- e Haga clic en el botón de alternancia **Multipath Relax** para habilitar o deshabilitar el reparto de la carga entre varias rutas que solo se diferencian por los valores de atributo de ruta de AS, pero que tienen la misma longitud de ruta de AS.

Nota **ECMP** debe estar habilitado para **Multipath Relax** para que funcione.

- f En el campo **Reinicio estable**, seleccione **Deshabilitar**, **Solo aplicación auxiliar** o **Reinicio estable y aplicación auxiliar**.

De forma opcional, puede cambiar el **Temporizador de reinicio estable** y el **Temporizador obsoleto de reinicio estable**.

De forma predeterminada, el modo de reinicio estable se establece en **Solo aplicación auxiliar**. El modo de aplicación auxiliar resulta útil para eliminar y/o reducir la interrupción del tráfico asociada a las rutas obtenidas de un vecino capaz de realizar un reinicio estable. El vecino debe poder conservar su tabla de reenvío mientras se reinicia.

No se recomienda habilitar la función de reinicio estable en las puertas de enlace de nivel 0, ya que los pares de BGP de todas las puertas de enlace siempre están activos. En caso de conmutación por error, la capacidad de reinicio estable aumentará el tiempo que tarda un vecino remoto en seleccionar una puerta de enlace de nivel 0 alternativa. Esta acción retrasará la convergencia basada en BFD.

Nota: A menos que se anule por la configuración específica de un vecino, la configuración de nivel 0 se aplicará a todos los vecinos de BGP.

5 Configure la **Agregación de rutas** añadiendo prefijos de direcciones IP.

- a Haga clic en **Agregar prefijo**.
- b Introduzca un prefijo de dirección IP en formato CIDR.
- c Para la opción **Solo resumen**, seleccione **Sí** o **No**.

6 Haga clic en **Guardar**.

Debe guardar la configuración de BGP global para poder configurar vecinos BGP.

7 Configure los **Vecinos BGP**.

a Introduzca la dirección IP del vecino.

b Habilite o deshabilite **BFD**.

c Introduzca un valor para **Número de AS remoto**.

Para iBGP, introduzca el mismo número de AS que en el paso 4a. Para eBGP, introduzca el número de AS del enrutador físico.

d Configure el **Filtro de salida**.

e Configure el **Filtro de entrada**.

f Habilite o deshabilite la función **Allowas-in**.

De forma predeterminada, esta opción está deshabilitada. Con esta función habilitada, los vecinos BGP pueden recibir rutas con el mismo AS, por ejemplo, cuando hay dos ubicaciones conectadas entre sí mediante el mismo proveedor de servicios. Esta función se aplica a todas las familias de direcciones y no se puede aplicar a familias de direcciones específicas.

g En el campo **Direcciones de origen**, puede seleccionar una dirección de origen para establecer una sesión de emparejamiento con un vecino mediante esta dirección de origen específica. Si no selecciona ninguna, la puerta de enlace elegirá una automáticamente.

h En el campo **Familia de direcciones IP**, seleccione **IPv4**, **IPv6** o **Deshabilitado**.

i Introduzca un valor para **Límite máximo de saltos**.

- j En el campo **Reinicio estable**, también puede seleccionar **Deshabilitar**, **Solo aplicación auxiliar** o **Reinicio estable y aplicación auxiliar**.

Opción	Descripción
Ninguna opción seleccionada	El reinicio estable para este vecino seguirá la configuración de BGP de la puerta de enlace de nivel 0.
Deshabilitar	<ul style="list-style-type: none"> ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Deshabilitar, se deshabilitará el reinicio estable para este vecino. ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Solo aplicación auxiliar, se deshabilitará el reinicio estable para este vecino. ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Reinicio estable y aplicación auxiliar, se deshabilitará el reinicio estable para este vecino.
Solo aplicación auxiliar	<ul style="list-style-type: none"> ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Deshabilitar, el reinicio estable se configurará como Solo aplicación auxiliar para este vecino. ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Solo aplicación auxiliar, el reinicio estable se configurará como Solo aplicación auxiliar para este vecino. ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Reinicio estable y aplicación auxiliar, el reinicio estable se configurará como Solo aplicación auxiliar para este vecino.
Reinicio estable y aplicación auxiliar	<ul style="list-style-type: none"> ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Deshabilitar, el reinicio estable se configurará como Reinicio estable y aplicación auxiliar para este vecino. ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Solo aplicación auxiliar, el reinicio estable se configurará como Reinicio estable y aplicación auxiliar para este vecino. ■ Si la puerta de enlace de nivel 0 tiene BGP configurado como Reinicio estable y aplicación auxiliar, el reinicio estable se configurará como Reinicio estable y aplicación auxiliar para este vecino.

- k Haga clic en **Temporizadores y contraseña**.

- l Introduzca un valor para **Intervalo de BFD**.

La unidad es milisegundos. Para un nodo de Edge que se ejecuta en una máquina virtual, el valor mínimo es 1.000. Para un nodo de Edge sin sistema operativo, el valor mínimo es 300.

- m Introduzca un valor para **Multiplicador de BFD**.

- n Introduzca un valor para **Período de retención**.

- o Introduzca un valor para **Tiempo de conexión persistente**.

- p Escriba una contraseña.

Esto es necesario si se configura la autenticación MD5 entre pares de BGP.

- 8 Haga clic en **Guardar**.

Configurar BFD

El protocolo de detección de envío bidireccional (Bidirectional Forwarding Detection, BFD) puede detectar los errores de envío de rutas.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Configuración avanzada**.

Accederá a la página **Opciones avanzadas de redes y seguridad > Enrutadores**. La puerta de enlace aparecerá como uno de los enrutadores lógicos. Siga las instrucciones aquí: [Configurar BFD en un enrutador lógico de nivel 0](#)

Configurar el reenvío de Capa 3 para IPv6

El reenvío de Capa 3 para IPv4 está habilitado de forma predeterminada. También puede configurar el reenvío de Capa 3 para IPv6.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Editar una puerta de enlace de nivel 0. Para ello, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Configuración avanzada**.
Accederá a la página **Opciones avanzadas de redes y seguridad > Enrutadores**. La puerta de enlace aparecerá como uno de los enrutadores lógicos.
- 5 Haga clic en la pestaña **Configuración global**.
- 6 En el campo **Modo de reenvío de capa 3**, seleccione **IPv4 e IPv6**.
No se admite el formato IPv6.
- 7 Vuelva a editar la puerta de enlace. Para ello, desplácese hasta la pestaña **Redes**.
- 8 Desplácese hasta **Configuración adicional**.
 - a No hay direcciones IPv6 configurables para la **subred de tránsito interno**. El sistema utilizará automáticamente direcciones locales de vínculo IPv6.
 - b Introduzca una subred IPv6 para **Subredes de tránsito T0-T1**.
- 9 Desplácese hasta **Interfaces** y agregue una interfaz para IPv6.

Crear perfiles de SLAAC y DAD para la asignación de direcciones IPv6

Cuando se utilizan direcciones IPv6 en una interfaz de enrutador lógico, se puede configurar la configuración automática de direcciones sin estado (SLAAC) para la asignación de direcciones IP. SLAAC habilita el direccionamiento de un host en función de un prefijo de red anunciado desde un enrutador de red local a través de los anuncios de router. La detección de direcciones duplicadas (DAD) garantiza la exclusividad de las direcciones IP.

Requisitos previos

Desplácese hasta **Opciones avanzadas de redes y seguridad > Enrutadores > Configuración global** y seleccione **IPv4 e IPv6** como **Modo de reenvío de capa 3**

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 0**.
- 3 Para editar una puerta de enlace de nivel 0, haga clic en el icono de menú (tres puntos) y seleccione **Editar**.
- 4 Haga clic en **Configuración adicional**.
- 5 Para crear un **Perfil ND** (perfil SLAAC), haga clic en el icono de menú (tres puntos) y seleccione **Crear nuevo**.
 - a Introduzca un nombre para el perfil.
 - b Seleccione un modo:
 - **Deshabilitado**: Los mensajes de anuncio de enrutador están deshabilitados.
 - **SLAAC con DNS a través de RA**: La dirección y la información de DNS se generan con el mensaje de anuncio de enrutador.
 - **SLAAC con DNS a través de DHCP**: La dirección se genera con el mensaje de anuncio de enrutador y el servidor DHCP genera la información de DNS.
 - **DHCP con dirección y DNS a través de DHCP**: El servidor DHCP genera la dirección y la información de DNS.
 - **SLAAC con dirección y DNS a través de DHCP**: El servidor DHCP genera la dirección y la información de DNS. Esta opción solo es compatible con NSX Edge y no con los hosts de KVM ni ESXi.
 - c Introduzca el tiempo accesible y el intervalo de retransmisión para el mensaje de anuncio del enrutador.
 - d Introduzca el nombre de dominio y especifique una duración para el nombre de dominio. Introduzca estos valores solo para las **SLAAC con DNS a través de RA**.

- e Introduzca un servidor DNS y especifique una duración para el servidor DNS. Introduzca estos valores solo para las **SLAAC con DNS a través de RA**.
 - f Introduzca los valores del anuncio de enrutador:
 - **Intervalo de RA:** Intervalo de tiempo entre la transmisión de mensajes de anuncio de enrutador consecutivos.
 - **Límite de saltos :** La duración de las rutas anunciadas.
 - **Vigencia del enrutador:** La duración del enrutador.
 - **Vigencia del prefijo:** La duración del prefijo en segundos.
 - **Tiempo de preferencia del prefijo:** La hora en la que se prefiere una dirección válida.
- 6 Para crear un **Perfil DAD**, haga clic en el icono de menú (tres puntos) y seleccione **Crear nuevo**.
- a Introduzca un nombre para el perfil.
 - b Seleccione un modo:
 - **Débil:** Se recibe una notificación de dirección duplicada, pero no se realiza ninguna acción cuando se detecta una dirección duplicada.
 - **Estricto:** Se recibe una notificación de dirección duplicada y ya no se utiliza la dirección duplicada.
 - c Introduzca el **Tiempo de espera (en segundos)** que especifica el intervalo de tiempo entre los paquetes de NS.
 - d Introduzca el **Recuento de reintentos de NS**, que especifica el número de paquetes de NS para detectar direcciones duplicadas a intervalos definidos por el **Tiempo de espera (en segundos)**

Puerta de enlace de nivel 1

3

Una puerta de enlace de nivel 1 realiza las funciones de un enrutador lógico de nivel 1. Tiene conexiones de vínculo inferior a segmentos y conexiones de vínculo superior a puertas de enlace de nivel 0.

Nota En la pestaña **Opciones avanzadas de redes y seguridad**, el término "enrutador lógico de nivel 1" se utiliza para hacer referencia a una puerta de enlace de nivel 1.

Puede configurar los anuncios de rutas y las rutas estáticas en una puerta de enlace de nivel 1. Se admiten las rutas estáticas recursivas.

Este capítulo incluye los siguientes temas:

- [Agregar una puerta de enlace de nivel 1](#)

Agregar una puerta de enlace de nivel 1

Por lo general, una puerta de enlace de nivel 1 está conectada a una puerta de enlace de nivel 0 en la dirección norte y a los segmentos en la dirección sur.

Las puertas de enlace de nivel 0 y nivel 1 admiten las siguientes configuraciones de direccionamiento para todas las interfaces (vínculos superiores, puertos de servicio y vínculos inferiores) en las topologías de un solo nivel y de varios niveles:

- Solo IPv4
- Solo IPv6
- Pila dual: IPv4 e IPv6

Para usar direcciones IPv6 o de pila dual, habilite **IPv4 e IPv6** como el modo de redireccionamiento de capa 3 en **Redes > Configuración de red > Configuración de redes globales**.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Puertas de enlace de nivel 1**.
- 3 Haga clic en **Agregar puerta de enlace de nivel 1**.

- 4 Introduzca un nombre para la puerta de enlace.
- 5 (opcional) Seleccione una puerta de enlace de nivel 0 para conectarse a esta puerta de enlace de nivel 1 y crear así una topología de varios niveles.
- 6 Seleccione un modo de conmutación por error.

Opción	Descripción
Preferente	Si se produce un error en el nodo de NSX Edge preferente y el nodo se recupera, reemplazará al nodo del mismo nivel y se convertirá en el nodo activo. El estado de este nodo cambiará a en espera.
No preferente	Si se produce un error en el nodo sw NSX Edge preferente y el nodo se recupera, comprobará si el nodo del mismo nivel es el activo. Si es así, el nodo preferente no reemplazará al nodo del mismo nivel y será el nodo que esté en espera. Esta es la opción predeterminada.

- 7 (opcional) Si quiere que la puerta de enlace de nivel 1 aloje servicios con estado (como NAT, equilibrador de carga o firewall), seleccione un clúster de NSX Edge.

Si se selecciona un clúster de NSX Edge, siempre se creará un enrutador de servicio (incluso si no se configuran los servicios con estado), lo que afecta al patrón de tráfico de norte a sur.

- 8 (opcional) Seleccione un nodo de NSX Edge.
- 9 (opcional) Haga clic en el botón de alternancia **Habilitar reubicación en espera** para habilitar o deshabilitar la reubicación en espera.

La reubicación en espera significa que si se produce un error en el nodo de Edge en el que se ejecuta el enrutador lógico activo o en espera, se creará un nuevo enrutador lógico en espera en otro nodo de Edge para mantener la alta disponibilidad. Si el nodo de Edge en el que se produce el error ejecuta el enrutador lógico activo, el enrutador lógico en espera original se convertirá en el enrutador lógico activo y se creará un nuevo enrutador lógico en espera. Si el nodo de Edge en el que se produce el error ejecuta el enrutador lógico en espera, el nuevo enrutador lógico en espera lo reemplazará.

- 10 Haga clic en **Guardar**.
- 11 (opcional) Haga clic en **Anuncio de rutas**.

Seleccione una o varias de las siguientes opciones:

- **Todas las rutas estáticas**
- **Todas las IP de NAT**
- **Todas las rutas del reenviador de DNS**
- **Todas las rutas VIP de equilibrador de carga**
- **Todos los segmentos y los puertos de servicio**
- **Todas las rutas IP de SNAT de equilibrador de carga**
- **Todos los endpoints locales de IPSec**

En el campo **Establecer reglas de anuncio de rutas**, haga clic en **Establecer** para agregar reglas de anuncio de rutas.

12 (opcional) Haga clic en **Interfaces de servicio** y en **Establecer** para configurar conexiones a los segmentos. Se requiere en algunas topologías, como segmentos respaldados por VLAN o equilibrio de carga de un solo brazo.

- a Haga clic en **Agregar interfaz**.
- b Introduzca un nombre y una dirección IP en formato CIDR.
- c Seleccione un segmento.
- d En el campo **MTU**, introduzca un valor entre 64 y 9000.
- e En el campo **Perfil ND**, seleccione un perfil.
- f Haga clic en **Guardar**.

13 (opcional) Haga clic en **Rutas estáticas** y en **Establecer** para configurar rutas estáticas.

- a Haga clic en **Agregar ruta estática**.
- b Introduzca un nombre y una dirección de red con el formato CIDR o el formato CIDR para IPv6.
- c Haga clic en **Establecer próximos saltos** para agregar información de los próximos saltos.
- d Haga clic en **Guardar**.

Segmentos

4

Un segmento realiza las funciones de un conmutador lógico.

Nota En la pestaña **Opciones avanzadas de redes y seguridad**, el término "conmutador lógico de términos" se utiliza para hacer referencia a un segmento.

Este capítulo incluye los siguientes temas:

- [Perfiles de segmentos](#)
- [Agregar un segmento](#)

Perfiles de segmentos

Los perfiles de segmentos incluyen detalles de configuración de redes de capa 2 para segmentos y puertos de segmentos. NSX Manager admite varios tipos de perfiles de segmentos.

Estos son los tipos de perfiles de segmentos disponibles:

- Calidad del servicio (Quality of Service, QoS)
- Detección de IP
- SpoofGuard
- Seguridad de segmentos
- Administración de MAC

Nota No puede editar ni eliminar los perfiles de segmentos predeterminados. Si necesita ajustes alternativos a los que se encuentran en el perfil de segmentos predeterminado, puede crear un perfil de segmentos personalizado. De forma predeterminada, todos los perfiles de segmentos personalizados, excepto el perfil de segmentos de seguridad, heredan la configuración del perfil de segmentos predeterminado correspondiente. Por ejemplo, un perfil de segmentos de detección de IP personalizado tendrá la misma configuración que el perfil de segmentos de detección de IP predeterminado.

Cada perfil de segmentos predeterminado o personalizado tiene un identificador único. Este identificador se utiliza para asociar el perfil de segmentos a un segmento o a un puerto de segmentos.

Los segmentos o los puertos de segmentos solo se pueden asociar a un perfil de segmentos de cada tipo. No puede tener, por ejemplo, dos perfiles de segmentos de calidad de servicio asociados a un segmento o puerto de segmentos.

Si no asocia un perfil de segmentos al crear un segmento, NSX Manager asociará el perfil de segmentos definido por el sistema predeterminado correspondiente. Los puertos de segmentos secundarios heredan el perfil de segmentos definido por el sistema predeterminado del segmento principal.

Cuando se crea o se actualiza un segmento o un puerto de segmentos, se puede elegir asociar un perfil de segmentos predeterminado o uno personalizado. Cuando el perfil de segmentos se asocia o se disocia de un segmento, se aplica el perfil de segmentos a los puertos de segmentos secundarios en función de los siguientes criterios.

- Si el segmento principal tiene un perfil asociado a él, el puerto de segmentos secundario hereda el perfil de segmentos del principal.
- Si el segmento principal no tiene un perfil de segmentos asociado a él, el perfil de segmentos predeterminado se asigna al segmento y el puerto de segmentos hereda dicho perfil de segmentos predeterminado.
- Si asocia explícitamente un perfil personalizado a un segmento, este perfil personalizado anula el perfil de segmentos existente.

Nota Si asoció un perfil de segmentos personalizado a un segmento, pero quiere conservar el perfil de segmentos predeterminado para uno de los puertos de segmentos secundarios, debe realizar una copia del perfil de segmentos predeterminado y asociarlo al puerto de segmentos específico.

No puede eliminar un perfil de segmentos personalizado si está asociado a un segmento o a un puerto de segmentos. Puede averiguar si hay asociado algún segmento o puerto de segmentos al perfil de segmentos personalizado accediendo a la sección Asignado a de la vista Resumen y haciendo clic en los segmentos y puertos de segmentos enumerados.

Información sobre el perfil de segmentos de calidad de servicio

QoS proporciona un rendimiento de red dedicado y de gran calidad para el tráfico preferido que necesita un gran ancho de banda. Para ello, el mecanismo de QoS prioriza ancho de banda suficiente, controla la latencia y la vibración, y disminuye la pérdida de datos de los paquetes preferidos incluso cuando se produce una congestión de red. Este nivel del servicio de red se proporciona mediante los recursos de red existentes de manera eficiente.

Esta versión permite moldear y marcar el tráfico específicamente, así como admite CoS y DSCP. La clase de servicio (Class of Service, CoS) de Capa 2 le permite especificar la prioridad de los paquetes de datos cuando el tráfico se almacena en búfer en el segmento debido a una congestión. El punto de código de servicios diferenciados (DSCP) de Capa 3 detecta los paquetes en función de sus valores DSCP. CoS siempre se aplica al paquete de datos independientemente del modo de confianza.

NSX-T Data Center confía en la configuración DSCP aplicada por una máquina virtual o en la modificación y configuración del valor DSCP en el nivel del segmento. En cada caso, el valor DSCP se propaga al encabezado de IP externa de los marcos encapsulados. Esto permite que la red física externa priorice el tráfico en función de la configuración DSCP del encabezado externo. Cuando DSCP está en el modo de confianza, el valor DSCP se copia del encabezado interno. En este modo, el valor DSCP no se conserva para el encabezado interno.

Nota La configuración DSCP solo funciona en el tráfico de túnel. Esta configuración no se aplica al tráfico del mismo hipervisor.

Puede utilizar el perfil de conmutación de QoS para configurar los valores del ancho de banda de entrada y de salida para establecer la frecuencia del límite de transmisión. La frecuencia del ancho de banda máximo se utiliza para soportar el tráfico de ráfaga que tiene permitido un conmutador lógico para evitar la congestión en los vínculos de red ascendente. Esta configuración no garantiza el ancho de banda, pero permite limitar el uso del ancho de banda de la red. El ancho de banda real que observará se determina en función de la velocidad de vínculo del puerto o de los valores en el perfil de conmutación, el valor que sea menor.

La configuración del perfil de conmutación de calidad de servicio se aplica al segmento y la hereda el puerto de segmento secundario.

Crear un perfil de segmentos para calidad de servicio

Puede definir el valor DSCP y configurar las opciones de entrada y salida para crear un perfil de conmutación de calidad de servicio personalizado.

Requisitos previos

- Familiarícese con el concepto de perfil de conmutación de calidad de servicio. Consulte [Información sobre el perfil de conmutación de QoS](#).
- Identifique el tráfico de red que desea priorizar.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Segmentos > Perfiles de segmentos**.
- 3 Haga clic en **Agregar perfil de segmento** y seleccione **Calidad de servicio**.

4 Complete los detalles del perfil de conmutación de calidad de servicio.

Opción	Descripción
Nombre	Escriba un nombre para el perfil.
Modo	<p>Seleccione la opción de Modo De confianza o No de confianza en el menú desplegable.</p> <p>Si selecciona el modo Confianza, el valor DSCP del encabezado interno se aplica al encabezado de IP externa en el tráfico IP/IPv6. Para tráfico que no sea IP/IPv6, el encabezado de IP externa toma el valor predeterminado. El modo Confianza no es compatible con un puerto lógico basado en superposiciones. El valor predeterminado es 0.</p> <p>El modo no de confianza no es compatible con puertos lógicos basados en superposiciones o VLAN. Para un puerto lógico basado en superposiciones, el valor DSCP del encabezado IP saliente se establece con el valor configurado al margen del tipo de paquete interno para el puerto lógico. Para el puerto lógico basado en VLAN, el valor DSCP del paquete IP/IPv6 se establece con el valor configurado. El rango de valores DSCP para el modo no de confianza se encuentra entre 0 y 63.</p> <p>Nota La configuración DSCP solo funciona en el tráfico de túnel. Esta configuración no se aplica al tráfico del mismo hipervisor.</p>
Prioridad	<p>Establezca el valor de la prioridad de la clase de servicio.</p> <p>Los valores de prioridad van desde 0 a 63, donde 0 se corresponde con la prioridad más importante.</p>
Clase de servicio	<p>Establezca el valor de la clase de servicio.</p> <p>La clase de servicio es compatible con puertos lógicos basados en VLAN. La clase de servicio agrupa tipos similares de tráfico en la red y cada tipo de tráfico se trata como una clase con su propio nivel de prioridad de servicio. El tráfico con menor prioridad se ralentiza o, en algunos casos, se descarta para proporcionar mejor rendimiento al tráfico con mayor prioridad. La clase de servicio también puede configurarse para el ID de VLAN con paquete cero. El rango de valores de clase de servicio se encuentra entre 0 y 7, siendo 0 el servicio de mejor esfuerzo.</p>
Entrada	<p>Establezca valores personalizados para el tráfico de red saliente de la máquina virtual a la red lógica.</p> <p>Puede utilizar el ancho medio de banda para reducir la congestión de red. El valor máximo de ancho de banda se utiliza para soportar tráfico a ráfagas, y el tamaño de las ráfagas se basa en la duración con el ancho de banda máximo. La duración de la ráfaga se establece en la opción Tamaño de ráfaga. No se puede garantizar el ancho de banda. Sin embargo, puede configurar los valores de tamaño medio, máximo y de ráfaga para limitar el ancho de banda de red.</p> <p>Por ejemplo, si el ancho de banda medio es de 30 Mbps, el ancho de banda máximo es de 60 Mbps y la duración permitida es 0,1 segundos, el tamaño de ráfaga será $60 * 1000000 * 0,1/8 = 750000$ bytes.</p> <p>El valor predeterminado 0 deshabilita el límite del tráfico de entrada.</p>

Opción	Descripción
Difusión de entrada	<p>Establezca valores personalizados para el tráfico de red saliente de la máquina virtual a la red lógica en base a la difusión.</p> <p>Por ejemplo, si establece el ancho de banda medio de un conmutador lógico en 3000 Kbps, el ancho de banda máximo es 6000 Kbps y la duración permitida es 0,1 segundos, el tamaño de ráfaga será $6000 * 1000 * 0,10/8 = 75000$ bytes.</p> <p>El valor predeterminado 0 deshabilita el límite del tráfico de difusión de entrada.</p>
Saliente	<p>Establezca valores personalizados para el tráfico de red entrante de la red lógica a la máquina virtual.</p> <p>El valor predeterminado 0 deshabilita el límite del tráfico de salida.</p>

Si no están configuradas las opciones de entrada, difusión de entrada y salida, los valores predeterminados se utilizan.

- Haga clic en **Guardar**.

Información sobre el perfil de segmentos de detección de direcciones IP

La detección de IP utiliza la intromisión de DHCP y DHCPv6, la intromisión de protocolo de resolución de direcciones (Address Resolution Protocol, ARP), la intromisión de detección de vecinos (Neighbor Discovery, ND) y VM Tools para aprender las direcciones IP y MAC.

Nota Los métodos de detección de IP para IPv6 están deshabilitados en el perfil de segmentos de detección de IP predeterminado. Para habilitar la detección de direcciones IP de IPv6 para segmentos, debe crear un perfil de detección de IP con las opciones de IPv6 habilitadas y asociar el perfil a los segmentos. Además, asegúrese de que el firewall distribuido permita los paquetes de detección de vecinos IPv6 entre todas las cargas de trabajo (permitidas de forma predeterminada).

Las direcciones IP y MAC detectadas se utilizan para lograr la supresión de ARP/ND, lo que minimiza el tráfico entre las máquinas virtuales conectadas al mismo segmento. Las direcciones también las utilizan SpoofGuard y los componentes de firewall distribuido (DFW). DFW utiliza los enlaces de direcciones para determinar la dirección IP de los objetos en las reglas de firewall.

La intromisión de DHCP/DHCPv6 inspecciona los paquetes de DHCP/DHCPv6 que se intercambian entre el servidor y el cliente de DHCP/DHCPv6 para aprender las direcciones IP y MAC.

La intromisión de ARP inspecciona los paquetes de ARP y de ARP innecesario (Gratuitous ARP, GARP) salientes de una máquina virtual para aprender las direcciones IP y MAC.

VM Tools es el software que se ejecuta en las máquinas virtuales alojadas en ESXi y que puede proporcionar información de configuración de las máquinas virtuales, como las direcciones MAC, IP o IPv6. Este método de detección de direcciones IP está disponible para máquinas virtuales que se ejecutan solo en hosts ESXi.

La intromisión de ND es el equivalente IPv6 de la intromisión de ARP. Examina los mensajes de solicitud de equipos vecinos (NS) y de anuncio de equipos vecinos (NA) para aprender las direcciones IP y MAC.

Con la detección de direcciones duplicadas se comprueba si una dirección IP recién detectada ya figura en la lista de enlaces aplicada de otro puerto. Esta comprobación se realiza para los puertos en el mismo segmento. Si se detecta una dirección duplicada, la dirección recién detectada se agrega a la lista descubierta, pero no se agrega a la lista de enlaces aplicada. Todas las direcciones IP duplicadas tienen una marca de tiempo de detección asociada. Si se quita la dirección IP que se encuentra en la lista de enlaces, ya sea porque se agrega a la lista de enlaces ignorados o porque se deshabilita la intromisión, la dirección IP duplicada con la marca de tiempo más antigua se moverá a la lista de enlaces. La información de la dirección duplicada está disponible a través de una llamada de API.

De forma predeterminada, los métodos de detección intromisión de ARP y de ND funcionan en un modo denominado Confianza desde el primer uso (Trust On First Use, TOFU). En el modo TOFU, cuando se detecta una dirección y se agrega a la lista de enlaces realizados, ese enlace permanece en la lista de realizados para siempre. TOFU se aplica a los primeros enlaces 'n' únicos <IP, MAC, VLAN> detectados mediante la intromisión ARP/ND, donde 'n' es el límite de enlace que puede configurar. Puede deshabilitar TOFU para la intromisión de ARP/ND. Los métodos seguirán funcionando en el modo de confianza en cada uso (TOEU). En el modo TOEU, cuando se detecta una dirección, se agrega a la lista de enlaces aplicados y, cuando se elimina o caduca, se elimina de la lista de enlaces aplicados. La intromisión de DHCP y VM Tools siempre funciona en el modo TOEU.

Nota TOFU no es igual que SpoofGuard y no bloquea el tráfico de la misma forma. Para obtener más información, consulte [Información sobre el perfil de segmentos de Spoofguard](#).

Para las máquinas virtuales Linux, el problema de flujo de ARP puede provocar que la intromisión de ARP obtenga información incorrecta. Puede evitar el problema con un filtro ARP. Para obtener más información, consulte <http://linux-ip.net/html/ether-arp.html#ether-arp-flux>.

Para cada puerto, NSX Manager mantiene una lista de enlaces ignorados, que contiene las direcciones IP que no se pueden enlazar al puerto. Si accede a **Redes y seguridad > Conmutación > Puertos** y selecciona un puerto, puede agregar enlaces detectados a la lista de enlaces omitidos. También puede eliminar un enlace detectado o aplicado existente copiándolos en **Enlaces omitidos**.

Crear un perfil de segmentos de detección de IP

NSX-T Data Center tiene varios perfiles de conmutación de detección de IP predeterminados. También puede crear otros perfiles adicionales.

Requisitos previos

Familiarícese con los conceptos del perfil de conmutación de detección de IP. Consulte [Información sobre el perfil de conmutación de detección de direcciones IP](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Segmentos > Perfiles de segmentos**.
- 3 Haga clic en **Agregar perfil de segmento** y seleccione **Detección de IP**.
- 4 Especifique los detalles del perfil de conmutación de detección de IP.

Opción	Descripción
Nombre	Introduzca un nombre.
Intromisión de ARP	Para un entorno IPv4. Aplica si las máquinas virtuales tienen direcciones IP estáticas.
Límite de enlace de ARP	El número máximo de direcciones IP IPv4 que se pueden enlazar a un puerto. El mínimo permitido es 1 (el valor predeterminado) y el máximo es 256.
Tiempo de espera del límite de enlace de ND de ARP	El valor de tiempo de espera, en minutos, para direcciones IP en la tabla de enlace de ARP/ND si TOFU está deshabilitado. Si se agota el tiempo de espera de una dirección, la reemplazará una nueva dirección detectada.
Intromisión de DHCP	Para un entorno IPv4. Aplica si las máquinas virtuales tienen direcciones IPv4.
Intromisión de DHCP V6	Para un entorno IPv6. Aplica si las máquinas virtuales tienen direcciones IPv6.
VM Tools	Disponible solo para las máquinas virtuales alojadas en ESXi.
VM Tools para IPv6	Disponible solo para las máquinas virtuales alojadas en ESXi.
Intromisión de detección de vecinos	Para un entorno IPv6. Aplica si las máquinas virtuales tienen direcciones IP estáticas.
Límite de enlace de detección de vecinos	El número máximo de direcciones IPv6 que se pueden enlazar a un puerto.
Confiar en el primer uso	Aplicable a intromisión de ND y ARP.
Detección de direcciones IP duplicadas	Para todos los métodos de intromisión y los entornos IPv4 e IPv6.

- 5 Haga clic en **Guardar**.

Información sobre el perfil de segmentos de Spoofguard

SpoofGuard ayuda a evitar un ataque malicioso denominado "suplantación de páginas web" o "suplantación de identidad". Una directiva SpoofGuard bloquea el tráfico que se determina que se va a suplantar.

SpoofGuard es una herramienta diseñada para evitar que las máquinas virtuales de su entorno envíen tráfico con una dirección IP desde la que no está permitido finalizar el tráfico. En el caso de que la dirección IP de una máquina virtual no coincida con la dirección IP en el enlace de direcciones de segmento y de puerto lógico correspondiente de Spoofguard, la vNIC de la máquina virtual no podrá acceder a la red por completo. Spoofguard se puede configurar en el nivel del puerto o del segmento. Hay varias razones por las que podría utilizar SpoofGuard en su entorno:

- Evitar que una máquina virtual no autorizada suplante la dirección IP de una máquina virtual existente.
- Garantizar que las direcciones IP de las máquinas virtuales no se puedan modificar sin intervención. En algunos entornos, es preferible que las máquinas virtuales no puedan modificar sus direcciones IP sin cambiar correctamente la revisión de control. Para ello, SpoofGuard garantiza que el propietario de la máquina virtual no pueda modificar la dirección IP y seguir trabajando sin impedimentos.
- Garantizar que las reglas de Distributed Firewall (DFW) no se omitan involuntariamente (o deliberadamente). En el caso de las reglas de DFW que se creen con conjuntos de direcciones IP como orígenes o destinos, siempre cabe la posibilidad de que una máquina virtual pueda tener su dirección IP falsificada en el encabezado del paquete y, por tanto, se omitan las reglas en cuestión.

La configuración de SpoofGuard de NSX-T Data Center incluye lo siguiente:

- SpoofGuard de direcciones MAC: autentica la dirección MAC del paquete.
- SpoofGuard de direcciones IP: autentica las direcciones IP y MAC del paquete.
- Inspección del protocolo de resolución de direcciones dinámicas (ARP), es decir, la validación de SpoofGuard de descubrimiento cercano (ND) y de SpoofGuard del protocolo de resolución de direcciones gratuito (GARP) y del ARP contradice la asignación del origen de direcciones IP-MAC, el origen de direcciones MAC y el origen de direcciones IP en la carga de ARP/GARP/ND.

En el nivel del puerto, la lista blanca de MAC/VLAN/IP permitidas se proporciona a través de la propiedad de enlaces de direcciones del puerto. Cuando la máquina virtual envía tráfico, se descarta si su IP/MAC/VLAN no coincide con las propiedades de IP/MAC/VLAN del puerto. SpoofGuard del nivel del puerto se ocupa de la autenticación del tráfico (por ejemplo, la consistencia del tráfico con la configuración VIF).

En el nivel del segmento, la lista blanca de MAC/VLAN/IP permitidas se proporciona a través de la propiedad de enlaces de direcciones del segmento. Suele ser una subred o un rango de IP permitidos del segmento, mientras que la instancia de Spoofguard del nivel del segmento se ocupa de la autorización del tráfico.

Spoofguard del nivel del segmento y del nivel del puerto debe permitir el tráfico antes de que se permita en el segmento. Puede controlar la habilitación o la deshabilitación de Spoofguard del nivel del segmento o del puerto con el perfil de segmento de Spoofguard.

Crear un perfil de segmentos para Spoofguard

Al configurar Spoofguard, si la dirección IP de la máquina virtual cambia, el tráfico de la máquina virtual puede bloquearse hasta que los correspondientes enlaces de direcciones de puerto/segmento configurados se actualicen con la nueva dirección IP.

Habilite Spoofguard para los grupos de puertos que incluyan invitados. Si se habilita en cada adaptador de red, Spoofguard inspecciona los paquetes para la dirección MAC preestablecida y su correspondiente dirección IP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Segmentos > Perfiles de segmentos**.
- 3 Haga clic en **Agregar perfil de segmento** y seleccione **Spoofguard**.
- 4 Introduzca un nombre.
- 5 Para habilitar el nivel del puerto Spoofguard, establezca **Enlaces de puertos** en **Habilitado**.
- 6 Haga clic en **Guardar**.

Información sobre el perfil de segmento de seguridad del segmento

La seguridad del segmento ofrece seguridad de Capa 2 y de Capa 3 sin estado. Para ello, comprueba el tráfico que entra al segmento y descarta los paquetes no autorizados que se envían desde máquinas virtuales comparando la dirección IP, la dirección MAC y los protocolos con un conjunto de direcciones y protocolos permitidos. Puede utilizar la seguridad del segmento para proteger la integridad del segmento mediante el filtrado de los ataques maliciosos que proceden de la máquina virtual de la red.

Tenga en cuenta que el perfil de seguridad del segmento predeterminado tiene habilitado los ajustes de DHCP `Server Block` y `Server Block - IPv6`. Esto significa que un segmento que utiliza el perfil de seguridad de segmentos predeterminado bloqueará el tráfico de un servidor DHCP a un cliente DHCP. Si desea un segmento que permita el tráfico del servidor DHCP, deberá crear un perfil de seguridad de segmento personalizado para el segmento.

Crear un perfil de segmento de seguridad de segmentos

Es posible crear un perfil de segmento de seguridad del segmento personalizado con direcciones MAC de destino de la lista permitida BPDU y configurar el límite de frecuencia.

Requisitos previos

Familiarícese con el concepto de perfil de segmento de seguridad del segmento. Consulte [Información sobre el perfil de conmutación de seguridad del conmutador](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Segmentos > Perfiles de segmentos**.
- 3 Haga clic en **Agregar perfil de segmento** y seleccione **Seguridad de segmentos**.
- 4 Complete los detalles del perfil de seguridad del segmento.

Opción	Descripción
Nombre	Escriba un nombre para el perfil.
Filtro de BPDU	<p>Alterne el botón Filtro BPDU para habilitar el filtro BPDU. Deshabilitado de forma predeterminada.</p> <p>Al habilitar el filtro BPDU, todo el tráfico a la dirección MAC de destino BPDU se bloquea. El filtro BPDU habilitado también deshabilita STP en los puertos de conmutadores lógicos, ya que dichos puertos no deberían formar parte de STP.</p>
Lista de permitidos de filtro de BPDU	Haga clic en la dirección MAC de destino de la lista de direcciones MAC de destino BPDU para permitir el tráfico al destino seleccionado. Debe habilitar el Filtro de BPDU para poder seleccionar un elemento de esta lista.
Filtro de DHCP	<p>Alterne el botón Bloqueo de servidores y Bloqueo de clientes para habilitar el filtro DHCP. Ambas opciones están deshabilitadas de forma predeterminada.</p> <p>La opción Bloqueo de servidores bloquea el tráfico de un servidor DHCP a un cliente DHCP. Tenga en cuenta que esto no bloquea el tráfico de un servidor DHCP a un agente de retransmisión DHCP.</p> <p>La opción Bloqueo de clientes de DHCP evita que una máquina virtual adquiera una dirección IP de DHCP bloqueando las solicitudes de DHCP.</p>
Filtro DHCPv6	<p>Active el botón Bloquear de servidores: IPv6 y Bloquear de clientes: IPv6 para habilitar el filtro DHCP. Ambas opciones están deshabilitadas de forma predeterminada.</p> <p>La opción Bloquear servidor DHCPv6 bloquea el tráfico que procede de un servidor DHCPv6 y se dirige a un cliente DHCPv6. Tenga en cuenta que esto no bloquea el tráfico de un servidor DHCP a un agente de retransmisión DHCP. Se filtran los paquetes cuyo número de puerto UDP de origen es 547.</p> <p>La opción Bloquear cliente DHCPv6 evita que una máquina virtual adquiera una dirección IP de DHCP al bloquear las solicitudes de DHCP. Se filtran los paquetes cuyo número de puerto UDP de origen es 546.</p>
Bloquear tráfico que no usa IP	<p>Alterne el botón Bloquear tráfico que no usa IP para permitir solo el tráfico de IPv4, IPv6, ARP y BPDU.</p> <p>Se bloqueará el resto de tráfico que no use IP. El tráfico IPv4, IPv6, ARP, GARP y BPDU permitido se basa en otro conjunto de directivas de la configuración de los enlaces de dirección y Spoofguard.</p> <p>De forma predeterminada, esta opción se deshabilita para permitir que el tráfico que no usa IP se gestione como tráfico estándar.</p>

Opción	Descripción
Protección de RA	Alterne el botón Protección de RA para filtrar los anuncios de entrada del enrutador IPv6. Se filtran los 134 paquetes del tipo ICMPv6. Esta opción está habilitada de forma predeterminada.
Límites de velocidad	<p>Establezca un límite de transmisión para el tráfico de difusión y multidifusión. Esta opción está habilitada de forma predeterminada.</p> <p>Los límites de transmisión se pueden utilizar para proteger el conmutador lógico o las máquinas virtuales de eventos como las tormentas de difusión.</p> <p>Para evitar problemas de conectividad, el valor mínimo de límite de frecuencia debe ser ≥ 10 pps.</p>

5 Haga clic en **Guardar**.

Información sobre el perfil de segmentos de detección de direcciones MAC

El perfil de segmentos de gestión de direcciones MAC admite dos funciones: el cambio de direcciones MAC y el aprendizaje de estas direcciones.

La función para cambiar de dirección MAC permite que una máquina virtual cambie su dirección MAC. Una máquina virtual conectada a un puerto puede ejecutar un comando administrativo para cambiar la dirección MAC de su vNIC y seguir enviando y recibiendo el tráfico en dicha vNIC. Esta función solo es compatible con ESXi y no con KVM. Esta propiedad está deshabilitada de forma predeterminada.

El aprendizaje de direcciones MAC proporciona conectividad de red a las implementaciones en las que varias direcciones MAC están configuradas detrás de una vNIC, por ejemplo, en una implementación de hipervisor anidado en el que una máquina virtual ESXi se ejecuta en un host ESXi y varias máquinas virtuales se ejecutan dentro de la máquina virtual ESXi. Sin el aprendizaje de direcciones MAC, cuando la vNIC de la máquina virtual ESXi se conecta a un puerto del segmento, su dirección MAC es estática. Las máquinas virtuales que se ejecutan dentro de la máquina virtual ESXi no tienen conectividad de red debido a que sus paquetes tienen distintas direcciones MAC de origen. Con el aprendizaje de direcciones MAC, el vSwitch inspecciona la dirección MAC de origen de cada paquete que provenga de la vNIC, aprende la dirección MAC y permite la transmisión del paquete. Si una dirección MAC aprendida no se usa durante un periodo de tiempo, esta se eliminará. Este periodo de tiempo no se puede configurar. El campo **Tiempo de caducidad de aprendizaje de MAC** muestra el valor predeterminado, que es 600.

El aprendizaje de direcciones MAC también admite la inundación de unidifusión desconocida. Normalmente, cuando un puerto recibe un paquete con una dirección MAC de destino desconocido, el paquete se descarta. Cuando el desbordamiento de unidifusión desconocida está habilitado, el puerto envía el tráfico de unidifusión desconocida a cada puerto del conmutador que tenga habilitadas las opciones de desbordamiento de unidifusión desconocida y de aprendizaje de direcciones MAC. Esta propiedad está habilitada de forma predeterminada, pero solo si el aprendizaje de direcciones MAC está habilitado.

El número de direcciones MAC que se pueden aprender se puede configurar. El valor máximo es 4096, que es el valor predeterminado. También puede establecer la directiva para cuando se alcance el límite. Las opciones son:

- **Anular:** Se descartan los paquetes de direcciones MAC de origen desconocido. Los paquetes entrantes dirigidos a esta dirección MAC se tratarán como unidifusión desconocida. El puerto recibirá los paquetes solo si tiene habilitado el desbordamiento de unidifusión desconocida.
- **Permitir:** Los paquetes procedentes de una dirección MAC de origen desconocido se reenvían, aunque no se conocerá la dirección. Los paquetes entrantes dirigidos a esta dirección MAC se tratarán como unidifusión desconocida. El puerto recibirá los paquetes solo si tiene habilitado el desbordamiento de unidifusión desconocida.

Si habilita el aprendizaje de direcciones MAC o el cambio de estas direcciones, también deberá configurar SpoofGuard para mejorar la seguridad.

Crear un perfil de segmento de detección de MAC

Puede crear un perfil de segmento de detección de MAC para administrar las direcciones MAC.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Segmentos > Perfiles de segmentos**.
- 3 Haga clic en **Agregar perfil de segmento** y seleccione **Detección de MAC**.
- 4 Complete los detalles del perfil de detección de direcciones MAC.

Opción	Descripción
Nombre	Escriba un nombre para el perfil.
Cambio de dirección MAC	Habilite o deshabilite la función para cambiar de dirección MAC. Esta opción está deshabilitada de forma predeterminada.
Aprendizaje de MAC	Habilite o deshabilite la función para detectar la dirección MAC. Esta opción está deshabilitada de forma predeterminada.
Directiva de límite de MAC	Seleccione Permitir o Anular . La opción predeterminada es Permitir . Esta opción está disponible si habilita el aprendizaje de direcciones MAC.
Desborde de unidif. desconocido	Habilite o deshabilite la función de desbordamiento de unidifusión desconocida. Esta opción está habilitada de forma predeterminada. Esta opción está disponible si habilita el aprendizaje de direcciones MAC.
Límite de MAC	Configure el número máximo de direcciones MAC. El valor predeterminado es 4096. Esta opción está disponible si habilita el aprendizaje de direcciones MAC.
Tiempo de caducidad de aprendizaje de MAC	Solo con fines informativos. Esta opción no se puede configurar. El valor predeterminado es 600.

- 5 Haga clic en **Guardar**.

Agregar un segmento

Un segmento se conecta a las máquinas virtuales y las puertas de enlace. Un segmento realiza las funciones de un conmutador lógico.

Para obtener información sobre cómo encontrar el identificador de VIF de una máquina virtual, consulte [Conectar una VM a un conmutador lógico](#).

Nota Un conmutador N-VDS configurado en el modo Ruta de datos mejorada es compatible con los perfiles de detección de IP, SpoofGuard e IPFIX.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Segmentos**.
- 3 Haga clic en **Agregar segmento**.
- 4 Introduzca un nombre para el segmento.
- 5 Seleccione una puerta de enlace conectada.
Puede seleccionar una puerta de enlace de nivel 0 o de nivel 1 existente, o bien seleccionar **Ninguno**. El valor predeterminado es **Ninguno**, lo que significa que el segmento es simplemente un conmutador lógico. Con una subred configurada, puede redirigir a una puerta de enlace de nivel 0 o de nivel 1.
- 6 Si la puerta de enlace conectada es de nivel 1, seleccione un tipo (**Flexible** o **Fijo**).
Un segmento flexible puede desvincularse de las puertas de enlace. Un segmento fijo se puede eliminar, pero no puede desvincularse de una puerta de enlace.
- 7 Para especificar una subred, haga clic en **Establecer subredes**.
- 8 Seleccione una zona de transporte, que puede ser una superposición o una VLAN.
- 9 Si la zona de transporte es de tipo VLAN, especifique una lista de identificadores de VLAN.
- 10 Si desea utilizar la VPN de capa 2 para ampliar el segmento, haga clic en el cuadro de texto **VPN L2** y seleccione una sesión de cliente o servidor de VPN de capa 2.
Puede seleccionar más de una.
- 11 En **Identificador de túnel VPN**, introduzca un valor único que se use para identificar el segmento.
- 12 Haga clic en **Guardar**.
- 13 Para agregar puertos de segmentos, haga clic en **Sí** cuando se le pregunte si desea seguir configurando el segmento.
 - a Haga clic en **Puertos** y en **Establecer**.
 - b Haga clic en **Agregar puerto de segmento**.

- c Introduzca un nombre de puerto.
- d En **Identificador**, especifique el UUID de VIF de la máquina virtual o del servidor que se conecta a este puerto.
- e Seleccione un tipo: **Principal**, **Secundario** o **Independiente**.

Deje este cuadro de texto en blanco, excepto para casos prácticos como contenedores o VMware HCX. Si este puerto es para un contenedor en una máquina virtual, seleccione **Secundario**. Si es para un contenedor de máquina virtual de host, seleccione **Principal**. Si este puerto es para un servidor o un contenedor sin sistema operativo, seleccione **Independiente**.

- f Escriba un identificador de contexto.

Introduzca el identificador de VIF principal si la opción de **Tipo** es **Secundario**, o si el **Tipo** de identificador de nodo de transporte es **Independiente**.

- g Introduzca una etiqueta de tráfico.

Introduzca el identificador de VLAN en un contenedor y otros casos prácticos.

- h Seleccione un método de asignación de dirección: **Grupo de direcciones IP**, **Grupo de direcciones MAC**, **Ambos** o **Ninguno**.

- i Especifique las etiquetas.

- j Aplique el enlace de direcciones especificando la dirección IP (dirección IPv4, dirección IPv6 o subred IPv6) y la dirección MAC del puerto lógico al que desea aplicar el enlace de direcciones. Por ejemplo, para IPv6, 2001::/64 es una subred IPv6, 2001::1 es una IP de host, mientras que 2001::1/64 es una entrada no válida. También puede especificar un identificador de VLAN.

Los enlaces de direcciones manuales, si se especifican, reemplazarán los enlaces de direcciones detectados automáticamente.

- k Seleccione perfiles de segmentos para este puerto.

14 Para seleccionar los perfiles de segmentos, haga clic en **Perfiles de segmentos**.

15 Haga clic en **Guardar**.

Red privada virtual (VPN)

5

NSX-T Data Center es compatible con la red privada virtual de IPsec (VPN de IPsec) y la VPN de Capa 2 en un nodo de NSX Edge. La VPN de IPsec ofrece conectividad de sitio a sitio entre un nodo de NSX Edge y los sitios remotos. Con la VPN de Capa 2, es posible ampliar el centro de datos al permitir que las máquinas virtuales mantengan la conectividad de red a través de fronteras geográficas mientras se utiliza la misma dirección IP.

Nota La VPN de IPsec y la VPN de Capa 2 no admiten la versión Limited Export de NSX-T Data Center.

Antes de establecer los ajustes de un servicio VPN, debe tener un nodo de NSX Edge operativo con al menos una puerta de enlace de nivel 0 o 1 configurada. Para obtener más información, consulte "Instalación de NSX Edge" en *Guía de instalación de NSX-T Data Center*.

A partir de NSX-T Data Center 2.4, también es posible configurar nuevos servicios de VPN mediante la interfaz de usuario de NSX Manager. En versiones anteriores de NSX-T Data Center, solo es posible configurar servicios de VPN mediante llamadas de REST API.

Importante Cuando se utiliza NSX-T Data Center 2.4 o versiones posteriores para configurar servicios de VPN, es necesario utilizar objetos nuevos, como puertas de enlace de nivel 0, creados mediante la interfaz de usuario de NSX Manager o las API de directivas que se incluyen con NSX-T Data Center 2.4 o las versiones posteriores. Para usar enrutadores lógicos de nivel 0 o 1 existentes que se hayan configurado antes de la versión NSX-T Data Center 2.4, debe seguir usando las llamadas API para configurar un servicio de VPN.

Existen perfiles de configuración predeterminada del sistema con valores predefinidos y opciones se encuentran disponibles para su uso durante la configuración de un servicio de VPN. También es posible definir nuevos perfiles con valores diferentes y seleccionarlos durante la configuración del servicio de VPN.

Este capítulo incluye los siguientes temas:

- [Información de VPN de IPsec](#)
- [Comprender la VPN de capa 2](#)
- [Agregar servicios de VPN](#)
- [Agregar sesiones de VPN de IPsec](#)

- [Agregar sesiones de VPN de capa 2](#)
- [Agregar endpoints locales](#)
- [Agregar perfiles](#)
- [Agregar una instancia de Edge autónoma como cliente VPN de Capa 2](#)
- [Comprobar el estado realizado de una sesión de VPN de IPsec](#)
- [Supervisar y solucionar problemas de sesiones de VPN](#)

Información de VPN de IPsec

La VPN de protocolo de seguridad de Internet (Internet Protocol Security, IPsec) protege el tráfico que fluye entre dos redes conectadas mediante una red pública a través de puertas de enlace de IPsec llamadas endpoints. NSX Edge solo admite un modo de túnel que utiliza el túnel IP con carga de seguridad encapsuladora (Encapsulating Security Payload, ESP). ESP funciona directamente en la parte superior de la IP usando el número de protocolo de IP 50.

IPsec VPN utiliza el protocolo IKE para negociar los parámetros de seguridad. El puerto UDP predeterminado se establece como 500. Si se detecta NAT en la puerta de enlace, el puerto se establece como UDP 4500.

NSX Edge admite una VPN de IPsec basada en directivas o basada en rutas.

Los servicios de VPN de IPsec se admiten en las puertas de enlace de nivel 0 que deben estar en modo de alta disponibilidad *Active-Standby*. Para obtener más información, consulte [Agregar una puerta de enlace de nivel 0](#). A partir de NSX-T Data Center 2.5, la VPN de IPsec también se admite en las puertas de enlace de nivel 1. Puede utilizar segmentos conectados a puertas de enlace de nivel 0 o nivel 1 al configurar un servicio de VPN de IPsec.

El servicio de VPN de IPsec en NSX-T Data Center usa la función de conmutación por error de nivel de puerta de enlace para admitir un servicio de alta disponibilidad. Se restablecen los túneles en la conmutación por error y se sincronizan los datos de configuración de VPN. El estado de VPN de IPsec no se sincroniza mientras se restablecen los túneles.

Se admiten la autenticación de modo de clave compartida previamente y el tráfico de unidifusión de direcciones IP entre el nodo de NSX Edge y los sitios VPN remotos. Además, se admite la autenticación de certificados a partir de NSX-T Data Center 2.4. Solo se admiten tipos de certificados firmados por uno de los siguientes algoritmos hash de firma.

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

Usar una VPN de IPSec basada en directivas

Las VPN de IPSec basadas en directivas requieren una directiva de VPN que se aplique a los paquetes para determinar el tipo de tráfico que se debe proteger mediante IPSec antes de que se transfiera a través del túnel de VPN.

Este tipo de VPN se considera estático porque, cuando cambia la topología de la red local y la configuración, hay que actualizar también la configuración de la directiva de VPN para adaptarla a los cambios.

Cuando se utiliza una VPN de IPSec basada en directivas con NSX-T Data Center, los túneles de IPSec se conectan a una o varias subredes locales detrás del nodo de NSX Edge con las subredes del mismo nivel en el sitio VPN remoto.

Puede implementar un nodo de NSX Edge detrás de un dispositivo NAT. En esta implementación, el dispositivo NAT traduce la dirección de la VPN de un nodo de NSX Edge a una dirección de acceso público a la que puede accederse desde Internet. Los sitios de VPN remotos utilizan esta dirección pública para acceder al nodo de NSX Edge.

También es posible colocar sitios de VPN remotos detrás de un dispositivo NAT. Debe proporcionar la dirección IP pública del sitio VPN remoto y su identificador (dirección IP o FQDN) para configurar el túnel de IPSec. En ambos extremos, se requiere una NAT estática individual para la dirección de la VPN.

Nota DNAT no es compatible con una puerta de enlace de nivel 1 donde está configurada la VPN de IPSec basada en directivas.

El tamaño del nodo de NSX Edge determina el número máximo de túneles admitidos, como aparecen en la siguiente tabla.

Tabla 5-1. Cantidad de túneles de IPSec admitidos

Tamaño del nodo de Edge	N.º de túneles de IPSec por sesión de VPN (basada en directivas)	N.º de sesiones por servicio VPN	N.º de túneles de IPSec por servicio de VPN (16 túneles por sesión)
Pequeño	N/D (solo validación técnica/laboratorio)	N/D (solo validación técnica/laboratorio)	N/D (solo validación técnica/laboratorio)
Mediano	128	128	2048
Grande	128 (límite débil)	256	4096
Sin sistema operativo	128 (límite débil)	512	6.000

Restricción La arquitectura inherente de VPN de IPSec basada en directivas impide que pueda configurar una redundancia del túnel VPN.

Para obtener más información sobre cómo configurar una VPN de IPSec basada en directivas, consulte [Agregar un servicio de VPN de IPSec](#).

Usar una VPN de IPSec basada en rutas

La VPN de IPSec basada en rutas proporciona el túnel para el tráfico basado en las rutas estáticas o aprendidas de forma dinámica en una interfaz especial denominada interfaz de túnel virtual (Virtual Tunnel Interface, VTI) que utiliza, por ejemplo, BGP como protocolo. IPSec protege todo el tráfico que circula a través de la VTI.

Nota

- El enrutamiento dinámico de OSPF no se admite para enrutar mediante túneles de VPN IPSec.
 - No se admite el enrutamiento dinámico para VTI en una VPN basada en puertas de enlace de nivel 1.
-

La VPN IPSec basada en rutas es similar a la encapsulación de enrutamiento genérico (GRE) mediante IPSec, con la excepción de que ninguna encapsulación adicional se agrega al paquete antes de aplicar el procesamiento de IPSec.

En este enfoque de túneles de VPN, las VTI se crean en el nodo de NSX Edge. Cada VTI se asocia a un túnel de IPSec. El tráfico cifrado está enrutado de un sitio a otro mediante las interfaces VTI. El procesamiento de IPSec solo sucede en la VTI.

Redundancia de túnel de VPN

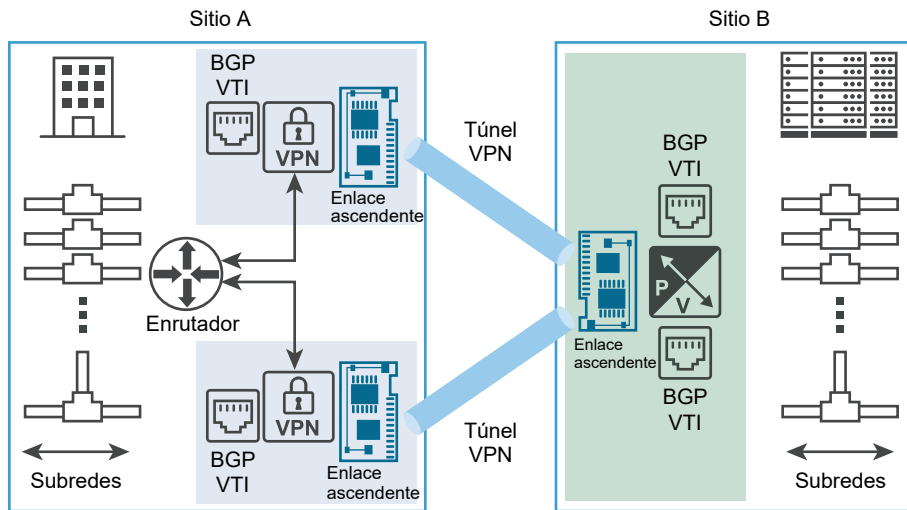
Puede configurar la redundancia del túnel VPN con una sesión de VPN de IPSec basada en rutas que esté configurada en una puerta de enlace de nivel 0. Con la redundancia de túnel, se pueden configurar varios túneles entre dos sitios, usándose un túnel como principal con conmutación por error a otros túneles cuando deja de estar disponible. Esta función es más útil cuando un sitio tiene varias opciones de conectividad, como los distintos ISP para la redundancia de vínculos.

Importante

- En NSX-T Data Center, la redundancia de túnel de VPN de IPSec solo se admite usando BGP.
 - No utilice el enrutamiento estático en túneles de VPN IPSec basada en rutas para conseguir la redundancia del túnel de VPN.
-

La siguiente imagen muestra una representación lógica de la redundancia del túnel de VPN IPSec entre dos sitios. En esta imagen, el Sitio A y el Sitio B representan dos centros de datos. En este ejemplo, se supone que NSX-T Data Center no administra las puertas de enlace de VPN de Edge en el sitio A y que NSX-T Data Center administra un dispositivo virtual de puerta de enlace Edge en el sitio B.

Figura 5-1. Redundancia de túnel en la VPN de IPsec basada en rutas



Como aparece en la imagen, puede configurar dos túneles VPN IPsec independientes usando VTI. El enrutamiento dinámico se configura usando el protocolo BGP para conseguir la redundancia del túnel. Si ambos túneles de VPN de IPsec se encuentran disponibles, permanecen en servicio. Todo el tráfico destinado del Sitio A al Sitio B mediante el nodo de NSX Edge se enruta a través de la VTI. El tráfico de datos se somete al procesamiento de IPsec y sale de su interfaz de enlace ascendente asociada del nodo de NSX Edge. Todo el tráfico IPsec entrante recibido desde la puerta de enlace VPN del Sitio B en la interfaz de enlace ascendente del nodo de NSX Edge se reenvía a la VTI después de que se descifre y, a continuación, tiene lugar el enrutamiento habitual.

Debe configurar los valores de temporizador Mantenimiento y Supresión de BGP para detectar la pérdida de conectividad con el mismo nivel dentro del tiempo de conmutación por error requerido. Consulte [Configurar BGP](#).

Comprender la VPN de capa 2

Con VPN de capa 2 (VPN de capa 2), es posible ampliar redes de capa 2 (VNI o VLAN) en varios sitios del mismo dominio de difusión. Esta conexión se protege con un túnel de IPsec basado en rutas entre el servidor de VPN de capa 2 y el cliente de VPN de capa 2.

Nota Esta función de VPN de capa 2 solo está disponible para NSX-T Data Center, y no tiene interoperabilidad con terceros.

La red ampliada es una subred única con un solo dominio de difusión, por lo que las máquinas virtuales permanecen en la misma subred cuando se mueven entre sitios y sus direcciones IP no cambian. Por lo tanto, las empresas pueden migrar máquinas virtuales sin problemas entre sitios de red. Las máquinas virtuales se pueden ejecutar en redes basadas en VNI o VLAN. Con respecto a los proveedores de nube, la VPN de Capa 2 les proporciona un mecanismo para incorporar empresas sin modificar las direcciones IP existentes usadas por las cargas de trabajo y las aplicaciones.

Además de admitir la migración de centros de datos, una red local ampliada con una VPN de capa 2 resulta útil para los planes de recuperación ante desastres y para involucrar recursos informáticos externos de forma dinámica para satisfacer el aumento de la demanda.

Cada sesión de VPN de capa 2 tiene un túnel de encapsulación de enrutamiento genérico (GRE). No se admite la redundancia de túnel. Una sesión de VPN de capa 2 se puede ampliar hasta 4094 segmentos de capa 2.

En NSX-T Data Center, los servicios de VPN de capa 2 solo son compatibles con las puertas de enlace de nivel 0. Los segmentos se pueden conectar a puertas de enlace de nivel 0 o nivel 1 y pueden utilizar servicios de VPN de capa 2.

A partir de NSX-T Data Center 2.5, los segmentos basados en VLAN se pueden ampliar mediante el servicio de VPN de capa 2 en una instancia de NSX Edge administrada en un entorno de NSX-T Data Center. Esta compatibilidad permite la ampliación de redes de capa 2 de VLAN a VNI, VLAN a VLAN y VNI a VNI.

También se admite el enlace troncal de VLAN usando un conmutador virtual distribuido administrado por ESX NSX (N-VDS). Si los recursos de E/S e informáticos lo permiten, el enlace troncal de VLAN permite que un clúster de NSX Edge extienda varias redes VLAN a través de una misma interfaz.

El soporte del servicio de VPN de capa 2 se proporciona en los siguientes escenarios.

- Entre un servidor VPN de Capa 2 de NSX-T Data Center y un cliente VPN de Capa 2 alojado en una instancia de NSX Edge administrada en un entorno de NSX Data Center for vSphere. Los clientes VPN de Capa 2 administrados admiten VLAN y VNI.
- Entre un servidor de VPN de capa 2 de NSX-T Data Center y un cliente de VPN de capa 2 alojado en una instancia de NSX Edge independiente o no administrada. Los clientes VPN de Capa 2 no administrados admite solo VLAN.
- Entre un servidor VPN de capa 2 de NSX-T Data Center y un cliente VPN de Capa 2 alojado en una instancia de NSX Edge autónoma. Los clientes VPN de Capa 2 autónomos admite solo VLAN.
- A partir de NSX-T Data Center 2.4, el soporte del servicio de VPN de capa 2 está disponible entre un servidor de VPN de capa 2 de NSX-T Data Center y clientes de VPN de capa 2 de NSX-T Data Center. En este escenario, puede ampliar los segmentos lógicos de Capa 2 entre dos centros de datos definidos por software (SDDC) en las instalaciones

Agregar servicios de VPN

Puede agregar una VPN de IPSec (basada en directivas o en rutas) o una VPN de Capa 2 mediante la interfaz de usuario de NSX Manager.

En las secciones siguientes se proporciona información sobre los flujos de trabajo necesarios para configurar el servicio VPN que necesita. Los temas que siguen a estas secciones proporcionan detalles sobre cómo agregar una VPN de IPSec o una VPN de Capa 2 mediante la interfaz de usuario de NSX Manager.

Flujo de trabajo de configuración de una VPN de IPSec basada en directivas

Para configurar un flujo de trabajo de servicio de VPN de IPSec basada en directivas, se requieren los siguientes pasos de alto nivel.

- 1 Cree y habilite un servicio VPN de IPSec mediante una puerta de enlace de nivel 0 o 1 existente. Consulte [Agregar un servicio de VPN de IPSec](#).
- 2 Cree un perfil de DPD (Dead Peer Detection) si prefiere no utilizar el valor predeterminado del sistema. Consulte [Agregar perfiles de DPD](#).
- 3 Para utilizar un perfil de IKE predeterminado que no sea del sistema, defina un perfil de IKE (intercambio de claves por red). Consulte [Agregar perfiles de IKE](#).
- 4 Configure un perfil de IPSec mediante [Agregar perfiles de IPSec](#).
- 5 Use [Agregar endpoints locales](#) para crear un servidor VPN alojado en la instancia de NSX Edge.
- 6 Configure una sesión de VPN de IPSec basada en directivas, aplique los perfiles y asocie el endpoint local a él. Consulte [Agregar una sesión de IPSec basada en directivas](#). Especifique las subredes locales y del mismo nivel que se van a utilizar para el túnel. El tráfico de una subred local dirigido a la subred del mismo nivel se protege mediante el túnel definido en la sesión.

Flujo de trabajo de configuración de una VPN de IPSec basada en rutas

El flujo de trabajo de configuración de una VPN de IPSec basada en rutas requiere los siguientes pasos de alto nivel.

- 1 Configure y habilite un servicio VPN de IPSec mediante una puerta de enlace de nivel 0 o 1 existente. Consulte [Agregar un servicio de VPN de IPSec](#).
- 2 Defina un perfil de IKE si prefiere no utilizar el predeterminado. Consulte [Agregar perfiles de IKE](#).
- 3 Si decide no utilizar el perfil de IPSec predeterminado del sistema, cree uno mediante [Agregar perfiles de IPSec](#).
- 4 Cree un perfil de DPD si no desea utilizar el perfil de DPD predeterminado. Consulte [Agregar perfiles de DPD](#).
- 5 Agregue un endpoint local mediante [Agregar endpoints locales](#).
- 6 Configure una sesión de VPN de IPSec basada en rutas, aplique los perfiles y asocie el endpoint local a la sesión. Proporcione una IP de VTI en la configuración y use la misma IP para configurar el enrutamiento. Las rutas pueden ser estáticas o dinámicas (mediante BGP). Consulte [Agregar una sesión de IPSec basada en rutas](#).

Flujo de trabajo de configuración de una VPN de Capa 2

Para configurar una VPN de Capa 2, se requiere que configure un servicio de VPN de Capa 2 en modo de servidor y, a continuación, otro servicio de VPN de Capa 2 en modo de cliente. También debe configurar las sesiones para el servidor VPN de capa 2 y el cliente VPN de capa 2 mediante el código del mismo nivel generado por el servidor VPN de capa 2. A continuación se muestra un flujo de trabajo de alto nivel para configurar un servicio VPN de Capa 2.

- 1 Cree un servicio VPN de Capa 2 en modo de servidor.
 - a Configure un túnel de VPN de IPSec basada en rutas con una puerta de enlace de nivel 0 y un servicio de servidor VPN de Capa 2 mediante ese túnel de IPSec basada en rutas. Consulte [Agregar un servicio de servidor VPN de Capa 2](#).
 - b Configure una sesión de servidor VPN de Capa 2, que enlaza el servicio de VPN de IPSec basada en rutas recién creado y el servicio del servidor VPN de Capa 2, y asigna automáticamente las direcciones IP de GRE. Consulte [Agregar una sesión del servidor VPN de capa 2](#).
 - c Agregue segmentos a las sesiones del servidor VPN de Capa 2. Este paso también se describe en [Agregar una sesión del servidor VPN de capa 2](#).
 - d Utilice [Descargar el archivo de configuración de VPN de capa 2 de lado remoto](#) para obtener el código del mismo nivel de la sesión del servicio de servidor VPN de capa 2, que se utiliza para configurar la sesión del cliente VPN de capa 2 automáticamente.
- 2 Cree un servicio de VPN de Capa 2 en modo de cliente.
 - a Configure otro servicio de VPN de IPSec basada en rutas mediante otra puerta de enlace de nivel 0 y configure un servicio de cliente VPN de Capa 2 mediante esa puerta de enlace de nivel 0 que acaba de configurar. Para obtener más información, consulte [Agregar un servicio de cliente VPN de Capa 2](#).
 - b Defina las sesiones de cliente VPN de Capa 2. Para ello, importe el código del mismo nivel que generó con el servicio del servidor VPN de Capa 2. Consulte [Agregar una sesión de cliente VPN de Capa 2](#).
 - c Agregue segmentos a las sesiones de cliente VPN de Capa 2 que se definieron en el paso anterior. Este paso se describe en [Agregar una sesión de cliente VPN de Capa 2](#).

Agregar un servicio de VPN de IPSec

NSX-T Data Center admite un servicio VPN de IPSec de sitio a sitio entre una puerta de enlace de nivel 0 y sitios remotos. Puede crear un servicio VPN de IPSec basado en rutas o en directivas. Debe crear el servicio VPN de IPSec antes de poder configurar una sesión de VPN de IPSec basada en rutas o en directivas.

Nota IPsec VPN no se admite en la versión Limited Export de NSX-T Data Center.

No se admite VPN de IPSec cuando la dirección IP del endpoint local pasa por NAT en el mismo enrutador lógico en el que está configurada la sesión VPN de IPSec.

Requisitos previos

- Familiarícese con IPsec VPN. Consulte [Información de VPN de IPsec](#).
- Al menos una puerta de enlace de nivel 0 o 1 debe estar configurada y lista para usarse. Consulte [Agregar una puerta de enlace de nivel 0](#) o [Agregar una puerta de enlace de nivel 1](#) para obtener más información.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Redes > VPN > Servicios de VPN**.
- 3 Seleccione **Agregar servicio > IPsec**.
- 4 Escriba un nombre para el servicio de IPsec.
Este nombre es obligatorio.
- 5 En el menú desplegable **Puerta de enlace**, seleccione la puerta de enlace de nivel 0 o 1 que se va a asociar con este servicio VPN de IPsec.
- 6 Habilite o deshabilite **Estado de administración**.
De forma predeterminada, se establece el valor `Enabled`, lo que significa que el servicio VPN de IPsec está habilitado en la puerta de enlace de nivel 0 o 1 después de configurar el nuevo servicio VPN de IPsec.
- 7 Establezca el valor de **Nivel de registro de IKE**.
El valor predeterminado se define en el nivel `Info`.
- 8 Si desea incluir este servicio en un grupo de etiquetas, introduzca un valor para **Etiquetas**.
- 9 Haga clic en **Reglas de omisión globales** si quiere permitir el intercambio de paquetes de datos entre las direcciones IP de los sitios locales y remotos indicadas sin la protección de IPsec, incluso en el caso de que las direcciones IP se especifiquen en las reglas de sesión de IPsec. En los cuadros de texto **Redes locales** y **Redes remotas**, introduzca la lista de subredes locales y remotas entre las que se aplican las reglas de omisión.
De manera predeterminada, se usa la protección de IPsec cuando los datos se intercambian entre los sitios locales y remotos. Estas reglas corresponden a todas las sesiones de VPN de IPsec creadas dentro de este servicio VPN de IPsec.
- 10 Haga clic en **Guardar**.
Una vez que cree correctamente el nuevo servicio VPN de IPsec, se le preguntará si desea continuar con el resto de la configuración de VPN de IPsec. Si hace clic en **Sí**, volverá al panel **Agregar servicio VPN de IPsec**. El vínculo **Sesiones** se habilitará y podrá hacer clic en él para agregar una sesión de VPN de IPsec.

Pasos siguientes

Utilice la información en [Agregar sesiones de VPN de IPsec](#) como guía para agregar una sesión de VPN de IPsec. También debe proporcionar información para los perfiles y el endpoint local que se necesitan para finalizar la configuración de VPN de IPsec.

Agregar un servicio VPN de Capa 2

Configure un servicio VPN de Capa 2 en una puerta de enlace de nivel 0. Para habilitar el servicio VPN de Capa 2, primero debe crear un servicio VPN de IPsec en la puerta de enlace de nivel 0, si aún no existe. A continuación, configure un túnel de VPN de Capa 2 entre un servidor VPN de Capa 2 (puerta de enlace de destino) y un cliente VPN de Capa 2 (puerta de enlace de origen).

Para configurar un servicio VPN de Capa 2, utilice la información incluida en los temas que siguen en esta sección.

Requisitos previos

- Familiarícese con la VPN de IPsec y VPN de Capa 2. Consulte [Información de VPN de IPsec y Comprender la VPN de capa 2](#).
- Al menos una puerta de enlace de nivel 0 debe estar configurada y lista para usarla. Consulte [Agregar una puerta de enlace de nivel 0](#).

Procedimiento

1 [Agregar un servicio de servidor VPN de Capa 2](#)

Para configurar un servicio de servidor VPN de Capa 2, debe configurar el servicio VPN de Capa 2 en modo de servidor en la instancia de NSX Edge de destino con la que se conectará el cliente VPN de Capa 2.

2 [Agregar un servicio de cliente VPN de Capa 2](#)

Después de configurar el servicio del servidor VPN de Capa 2, configure el servicio VPN de Capa 2 en el modo cliente en otra instancia de NSX Edge.

Agregar un servicio de servidor VPN de Capa 2

Para configurar un servicio de servidor VPN de Capa 2, debe configurar el servicio VPN de Capa 2 en modo de servidor en la instancia de NSX Edge de destino con la que se conectará el cliente VPN de Capa 2.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

- 2 (opcional) Si aún no existe un servicio VPN de IPSec en la puerta de enlace de nivel 0 que desea configurar como servidor VPN de Capa 2, créelo siguiendo estos pasos.
 - a Desplácese hasta la pestaña **Redes > VPN > Servicios de VPN** y seleccione **Agregar servicio > IPSec**.
 - b Introduzca un nombre para el servicio VPN de IPSec.
 - c En el menú desplegable **Puerta de enlace de nivel 0**, seleccione una puerta de enlace de nivel 0 para utilizarla con el servidor VPN de Capa 2.
 - d Si desea usar valores distintos a los valores predeterminados del sistema, establezca el resto de las propiedades en el panel Agregar servicio de IPSec según corresponda.
 - e Haga clic en **Guardar** y, cuando se le pregunte si desea seguir configurando el servicio de VPN de IPSec, seleccione **No**.
- 3 Desplácese hasta la pestaña **Redes > VPN > Servicios de VPN** y seleccione **Agregar servicio > Servidor VPN de capa 2** para crear un servidor VPN de Capa 2.
- 4 Introduzca un nombre para el servidor VPN de Capa 2.
- 5 En el menú desplegable **Puerta de enlace de nivel 0**, seleccione la misma puerta de enlace de nivel 0 que utilizó con el servicio de IPSec que creó hace un momento.
- 6 Si lo desea, puede escribir una descripción para este servidor VPN de Capa 2.
- 7 Si desea incluir este servicio en un grupo de etiquetas, introduzca un valor para **Etiquetas**.
- 8 Habilite o deshabilite la propiedad **Hub y radio**.

De forma predeterminada, el valor se establece como `Disabled`, lo que significa que el tráfico que proviene de los clientes VPN de Capa 2 solo se replica en los segmentos conectados al servidor VPN de Capa 2. Si esta propiedad se establece como `Enabled`, el tráfico que proviene de cualquier cliente VPN de Capa 2 se replica en todos los otros clientes VPN de Capa 2.

- 9 Haga clic en **Guardar**.

Una vez que cree correctamente el nuevo servidor VPN de capa 2, se le preguntará si desea continuar con el resto de la configuración del servicio de VPN de capa 2. Si hace clic en **Sí**, volverá al panel Agregar servidor VPN de Capa 2 y se habilitará el vínculo **Sesión**. Puede usar ese vínculo para crear una sesión de servidor VPN de Capa 2 o puede usar la pestaña **Redes > VPN > Sesiones de VPN de capa 2**.

Pasos siguientes

Configure una sesión de servidor VPN de Capa 2 para el servidor VPN de Capa 2 que configuró con base en la información de [Agregar una sesión del servidor VPN de capa 2](#).

Agregar un servicio de cliente VPN de Capa 2

Después de configurar el servicio del servidor VPN de Capa 2, configure el servicio VPN de Capa 2 en el modo cliente en otra instancia de NSX Edge.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 (opcional) Si aún no existe, cree un servicio VPN de IPSec para el servicio cliente de VPN de Capa 2 siguiendo estos pasos.
 - a Desplácese hasta la pestaña **Redes > VPN > Servicios de VPN** y seleccione **Agregar servicio > IPSec**.
 - b Introduzca un nombre para el servicio VPN de IPSec.
 - c En el menú desplegable **Puerta de enlace de nivel 0**, seleccione una puerta de enlace de nivel 0 para utilizarla con el cliente VPN de Capa 2.
 - d Si desea usar valores distintos a los valores predeterminados del sistema, establezca el resto de las propiedades en el panel Agregar servicio de IPSec según corresponda.
 - e Haga clic en **Guardar** y, cuando se le pregunte si desea seguir configurando el servicio de VPN de IPSec, seleccione **No**.
- 3 Desplácese hasta la pestaña **Redes > VPN > Servicios de VPN** y seleccione **Agregar servicio > Cliente VPN de capa 2**.
- 4 Introduzca un nombre para el servicio de cliente VPN de Capa 2.
- 5 En el menú desplegable **Puerta de enlace de nivel 0**, seleccione la misma puerta de enlace de nivel 0 que utilizó con el túnel de IPSec basado en rutas que creó hace un momento.
- 6 De forma opcional, establezca los valores de **Descripción** y **Etiquetas**.
- 7 Haga clic en **Guardar**.

Después de crear correctamente el nuevo servicio de cliente VPN de Capa 2, se le pregunta si desea continuar con el resto de la configuración de dicho cliente. Al hacer clic en **Sí**, se regresa al panel Agregar cliente VPN de Capa 2 y se habilita el vínculo **Sesión**. Puede usar dicho vínculo para crear una sesión de cliente VPN de Capa 2, o bien utilizar la pestaña **Redes > VPN > Sesiones de VPN de capa 2**.

Pasos siguientes

Configure una sesión de cliente VPN de Capa 2 para el servicio de cliente de VPN de Capa 2 que configuró. Utilice la información de [Agregar una sesión de cliente VPN de Capa 2](#) a modo de guía.

Agregar sesiones de VPN de IPSec

Después de haber configurado un servicio VPN de IPSec, debe agregar una sesión de VPN de IPSec basada en directivas o una sesión de VPN de IPSec basada en rutas, en función del tipo de VPN de IPSec que desee configurar. Proporcione también la información de los perfiles y el endpoint local que se deben usar para finalizar la configuración del servicio de VPN de IPSec.

Agregar una sesión de IPSec basada en directivas

Cuando se agrega una VPN de IPSec basada en directivas, los túneles de IPSec se utilizan para conectar varias subredes locales que se encuentran detrás del nodo de NSX Edge con las subredes del mismo nivel en el sitio de VPN remoto.

En los siguientes pasos se utiliza la pestaña **Sesiones de IPSec** de la interfaz de usuario de NSX Manager para crear una sesión de IPSec basada en directivas. Se agrega también información de los perfiles de túnel, IKE y DPD, y se selecciona un endpoint local existente para emplearlo con la VPN de IPSec basada en directivas.

Nota También puede agregar una sesión de servidor de VPN de IPSec justo después de configurar correctamente el servicio del servidor de VPN de IPSec. Haga clic en **Sí** cuando se solicite para continuar con la configuración del servicio de VPN de IPSec, y seleccione **Sesiones > Agregar sesiones** en el panel Agregar servicio de IPSec. Para los primeros pasos del siguiente procedimiento, se presupone que seleccionó **No** para continuar con la configuración del servicio de VPN de IPSec. Si seleccionó **Sí**, vaya al tercero de los pasos siguientes para obtener instrucciones sobre lo que queda de la configuración de la sesión de VPN de IPSec basada en directivas.

Requisitos previos

- Debe configurar un servicio de servidor de VPN de IPSec antes de continuar. Consulte [Agregar un servicio de VPN de IPSec](#).
- Obtenga la información del endpoint local, la dirección IP del sitio del mismo nivel, la subred de la red local y la subred de la red remota que se van a usar con la sesión de VPN de IPSec basada en directivas que está agregando. Para crear un endpoint local, consulte [Agregar endpoints locales](#).
- Si utiliza una clave precompartida (PSK) para la autenticación, obtenga el valor de PSK.
- Si utiliza un certificado para la autenticación, asegúrese de que se hayan importado los certificados de servidor necesarios y los certificados firmados por CA correspondientes. Consulte [Configurar certificados](#).
- Si no desea utilizar los valores predeterminados para los perfiles de túnel de IPSec, IKE o Dead Peer Detection (DPD) que NSX-T Data Center proporciona, configure los perfiles que desea utilizar en su lugar. Para obtener más información, consulte [Agregar perfiles](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta la pestaña **Redes > VPN > Sesiones de IPSec**.
- 3 Seleccione **Agregar sesión de IPSec > Basada en directivas**.
- 4 Introduzca un nombre para la sesión de VPN de IPSec basada en directivas.

- 5 En el menú desplegable **Servicio de VPN**, seleccione el servicio de VPN de IPSec al que desee agregar esta nueva sesión de IPSec.

Nota Si agrega esta sesión de IPSec desde el cuadro de diálogo **Agregar sesiones de IPSec**, el nombre del servicio de VPN se indica encima del botón **Agregar sesión de IPSec**.

- 6 Seleccione un endpoint local existente en el menú desplegable.

Este valor de endpoint local es obligatorio e identifica el nodo local de NSX Edge. Si desea crear otro endpoint local, haga clic en el menú de tres puntos (⋮) y seleccione **Agregar endpoint local**.

- 7 En el cuadro de texto **Dirección IP remota**, introduzca la dirección IP del sitio remoto requerida.

Este valor es obligatorio.

- 8 Si lo desea, puede escribir una descripción para esta sesión de VPN de IPSec basada en directivas.

La longitud máxima es de 1024 caracteres.

- 9 Para habilitar o deshabilitar la sesión de VPN de IPSec, haga clic en **Estado de administración**.

De forma predeterminada, el valor se establece como `Enabled`, lo que significa que la sesión de VPN de IPSec se debe configurar hasta el nodo de NSX Edge.

- 10 (opcional) En el menú desplegable **Suite de cumplimiento**, seleccione una suite de cumplimiento de seguridad.

Nota Las suites de cumplimiento se admiten a partir de NSX-T Data Center 2.5. Consulte [Información sobre las suites de cumplimiento admitidas](#) para obtener más información.

El valor predeterminado seleccionado es `None`. Si selecciona una suite de cumplimiento, el **Modo de autenticación** se establecerá en `Certificate` y, en la sección **Propiedades avanzadas**, los valores para **Perfil de IKE** y **Perfil de IPSec** se establecerán en perfiles definidos por el sistema para la suite de cumplimiento de seguridad seleccionada. No puede editar estos perfiles definidos por el sistema.

- 11 Si se establece `None` para la **Suite de cumplimiento**, seleccione un modo en el menú desplegable **Modo de autenticación**.

El modo de autenticación predeterminado utilizado es `PSK`, lo que significa que se utiliza una clave secreta compartida entre NSX Edge y el sitio remoto para la sesión de VPN de IPSec. Si selecciona `Certificate`, se utilizará el certificado del sitio que se usó para configurar el endpoint local para la autenticación.

- 12 En los cuadros de texto Redes locales y Redes remotas, introduzca al menos una dirección IP de subred para usarla en esta sesión de VPN de IPSec basada en directivas.

Debe utilizar el formato CIDR con estas subredes.

- 13 Si se establece **PSK** como **Modo de autenticación** , introduzca el valor de la clave en el cuadro de texto **Clave precompartida**.

Esta clave secreta puede ser una cadena con un máximo de 128 bytes de caracteres de longitud.

Precaución Tenga cuidado al compartir y almacenar un valor de PSK porque contiene información confidencial.

- 14 Para identificar el sitio del mismo nivel, introduzca un valor en **Identificador remoto**.

Para los sitios del mismo nivel que utilicen una autenticación de PSK, el valor de este identificador debe ser la dirección IP pública o el FQDN del sitio del mismo nivel. Para los sitios del mismo nivel con autenticación por certificado, el valor de este identificador debe ser el nombre común (Common Name, CN) o el nombre distintivo (Distinguished Name, DN) indicado en el certificado para el sitio del mismo nivel.

Nota Si el certificado para el sitio del mismo nivel contiene una dirección de correo electrónico en la cadena de DN, como en este ejemplo:

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

Introduzca el valor del **Identificador remoto** con el formato del ejemplo siguiente.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

Si se usa una dirección de correo electrónico en la cadena de DN del certificado para el sitio local y el sitio del mismo nivel utiliza la implementación de IPsec strongSwan, introduzca el identificador del sitio local en el sitio del mismo nivel. A continuación se muestra un ejemplo.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 15 Para cambiar los perfiles, el modo de inicio, el modo de fijación de MSS de TCP y las etiquetas utilizadas por la sesión de VPN de IPsec basadas en directivas, haga clic en **Propiedades avanzadas**.

De forma predeterminada, se utilizan los perfiles generados por el sistema. Seleccione otro perfil disponible si no desea usar el predeterminado. Si desea utilizar un perfil que aún no se ha configurado, haga clic en el menú de tres puntos (⋮) para crear otro perfil. Consulte [Agregar perfiles](#).

- Si el menú desplegable **Perfiles de IKE** está habilitado, seleccione el perfil de IKE.
- Seleccione el perfil de túnel de IPsec si el menú desplegable **Perfiles de IPsec** no está deshabilitado.
- Seleccione el perfil de DPD que prefiera si el menú desplegable **Perfiles de DPD** está habilitado.

- d Seleccione el modo preferido en el menú desplegable **Modo de inicio de conexión**.

El modo de inicio de conexión define la directiva utilizada por el endpoint local en el proceso de creación del túnel. El valor predeterminado es **Iniciador**. En la siguiente tabla, se describen los diferentes modos de inicio de conexión disponibles.

Tabla 5-2. Modos de inicio de conexión

Modo de inicio de conexión	Descripción
Initiator	El valor predeterminado. En este modo, el endpoint local inicia la creación del túnel VPN de IPsec y responde a las solicitudes entrantes de instalación del túnel de la puerta de enlace del mismo nivel.
On Demand	En este modo, el endpoint local inicia la creación del túnel VPN de IPsec después de recibir el primer paquete que coincide con la regla de directiva. También responde a la solicitud de inicio entrante.
Respond Only	La VPN de IPsec nunca inicia una conexión. El sitio del mismo nivel siempre inicia la solicitud de conexión, y el endpoint local responde a dicha solicitud de conexión.

- e Si desea reducir la carga del tamaño de segmento máximo (MSS) de la sesión de TCP durante la conexión de IPsec, habilite **Fijación de MSS de TCP**, seleccione el valor **Dirección de MSS de TCP** y, opcionalmente, establezca el **Valor de MSS de TCP**.

Consulte [Fijación de MSS de TCP](#) para obtener más información.

- f Si desea incluir esta sesión como parte de un grupo específico, escriba el nombre de etiqueta en **Etiquetas**.

16 Haga clic en **Guardar**.

Resultados

Cuando la nueva sesión de VPN de IPsec basada en directivas se configure correctamente, esta se agregará a la lista de sesiones de VPN de IPsec disponibles. Está en modo de solo lectura.

Pasos siguientes

- Compruebe que el estado del túnel VPN de IPsec sea Activo. Para obtener más información, consulte [Supervisar y solucionar problemas de sesiones de VPN](#).
- Si es necesario, administre la información de la sesión de VPN de IPsec; para ello, haga clic en el menú de tres puntos (⋮) a la izquierda de la fila de la sesión. Seleccione una de las acciones que puede realizar.

Agregar una sesión de IPsec basada en rutas

Cuando se agrega una VPN de IPsec basada en rutas, se proporciona tunelización en el tráfico basado en rutas que se aprendieron dinámicamente a través de una interfaz de túnel virtual (VTI)

utilizando el protocolo preferido, como BGP. IPSec protege todo el tráfico que circula a través de la VTI.

Los pasos descritos en este tema utilizan la pestaña **Sesiones de IPSec** para crear una sesión de IPSec basada en rutas. También deberá añadir información de los perfiles de túnel, IKE y DPD, así como seleccionar el endpoint local existente que se usará con la VPN de IPSec basada en rutas.

Nota También puede agregar una sesión de servidor de VPN de IPSec justo después de configurar correctamente el servicio del servidor de VPN de IPSec. Haga clic en **Sí** cuando se solicite para continuar con la configuración del servicio de VPN de IPSec, y seleccione **Sesiones > Agregar sesiones** en el panel Agregar servicio de IPSec. Para los primeros pasos del siguiente procedimiento, se presupone que seleccionó **No** para continuar con la configuración del servicio de VPN de IPSec. Si ha seleccionado **Sí**, vaya al paso 3 de la lista para seguir configurando la sesión del servicio de VPN de IPSec basada en rutas.

Requisitos previos

- Debe configurar un servicio de servidor de VPN de IPSec antes de continuar. Consulte [Agregar un servicio de VPN de IPSec](#).
- Obtenga la información del endpoint local, la dirección IP del sitio del mismo nivel y la dirección de subred IP del servicio de túnel que se usarán con la sesión de IPSec basada en rutas que va a agregar. Para crear un endpoint local, consulte [Agregar endpoints locales](#).
- Si utiliza una clave precompartida (PSK) para la autenticación, obtenga el valor de PSK.
- Si utiliza un certificado para la autenticación, asegúrese de que se hayan importado los certificados de servidor necesarios y los certificados firmados por CA correspondientes. Consulte [Configurar certificados](#).
- Si no desea utilizar los valores predeterminados de los perfiles de túnel de IPSec, IKE o Dead Peer Detection (DPD) proporcionados por NSX-T Data Center, configure los perfiles que desee utilizar en su lugar. Para obtener más información, consulte [Agregar perfiles](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Redes > VPN > Sesiones de IPSec**.
- 3 Seleccione **Agregar sesión de IPSec > Con base en rutas**.
- 4 Escriba un nombre para la sesión de IPSec basada en rutas.
- 5 En el menú desplegable **Servicio de VPN**, seleccione el servicio de VPN de IPSec al que desee agregar esta nueva sesión de IPSec.

Nota Si agrega esta sesión de IPSec desde el cuadro de diálogo **Agregar sesiones de IPSec**, el nombre del servicio de VPN se indica encima del botón **Agregar sesión de IPSec**.

- 6 Seleccione un endpoint local existente en el menú desplegable.

Este valor de endpoint local es obligatorio e identifica el nodo local de NSX Edge. Si desea crear otro endpoint local, haga clic en el menú de tres puntos (⋮) y seleccione **Agregar endpoint local**.

- 7 En el cuadro de texto **Dirección IP remota**, introduzca la dirección IP del sitio remoto.

Este valor es obligatorio.

- 8 Escriba una descripción opcional para la sesión de VPN de IPsec basada en rutas.

La longitud máxima es de 1024 caracteres.

- 9 Para habilitar o deshabilitar la sesión de VPN de IPsec, haga clic en **Estado de administración**.

De forma predeterminada, el valor se establece como `Enabled`, lo que significa que la sesión de IPsec se debe configurar hasta el nodo de NSX Edge.

- 10 (opcional) En el menú desplegable **Suite de cumplimiento**, seleccione una suite de cumplimiento de seguridad.

Nota Las suites de cumplimiento se admiten a partir de NSX-T Data Center 2.5. Consulte [Información sobre las suites de cumplimiento admitidas](#) para obtener más información.

El valor predeterminado es `None`. Si selecciona una suite de cumplimiento, el **Modo de autenticación** se establecerá en `Certificate` y, en la sección **Propiedades avanzadas**, los valores para **Perfil de IKE** y **Perfil de IPsec** se establecerán en perfiles definidos por el sistema para la suite de cumplimiento seleccionada. No puede editar estos perfiles definidos por el sistema.

- 11 Escriba una dirección de subred IP en **Interfaz de túnel** en formato CIDR.

Esta dirección es obligatoria.

- 12 Si se establece `None` para la **Suite de cumplimiento**, seleccione un modo en el menú desplegable **Modo de autenticación**.

El modo de autenticación predeterminado utilizado es `PSK`, lo que significa que se utiliza una clave secreta compartida entre NSX Edge y el sitio remoto para la sesión de VPN de IPsec. Si selecciona `Certificate`, se utilizará el certificado del sitio que se usó para configurar el endpoint local para la autenticación.

- 13 Si seleccionó `PSK` para el modo de autenticación, introduzca el valor de clave en el cuadro de texto **Clave precompartida**.

Esta clave secreta puede ser una cadena con un máximo de 128 bytes de caracteres de longitud.

Precaución Tenga cuidado al compartir y almacenar un valor de PSK porque contiene información confidencial.

14 Introduzca un valor en **Identificador remoto**.

Para los sitios del mismo nivel que utilicen una autenticación de PSK, el valor de este identificador debe ser la dirección IP pública o el FQDN del sitio del mismo nivel. Para los sitios del mismo nivel con autenticación por certificado, el valor de este identificador debe ser el nombre común (Common Name, CN) o el nombre distintivo (Distinguished Name, DN) indicado en el certificado para el sitio del mismo nivel.

Nota Si el certificado para el sitio del mismo nivel contiene una dirección de correo electrónico en la cadena de DN, como en este ejemplo:

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

Introduzca el valor del **Identificador remoto** con el formato del ejemplo siguiente.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

Si se usa una dirección de correo electrónico en la cadena de DN del certificado para el sitio local y el sitio del mismo nivel utiliza la implementación de IPsec strongSwan, introduzca el identificador del sitio local en el sitio del mismo nivel. A continuación se muestra un ejemplo.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 15 Si desea incluir esta sesión de IPsec como parte de una etiqueta de grupo específico, escriba el nombre de la etiqueta en **Etiquetas**.
- 16 Para cambiar los perfiles, el modo de inicio, el modo de fijación de MSS de TCP y las etiquetas utilizadas por la sesión de VPN de IPsec basadas en rutas , haga clic en **Propiedades avanzadas**.

De forma predeterminada, se utilizan los perfiles generados por el sistema. Seleccione otro perfil disponible si no desea usar el predeterminado. Si desea utilizar un perfil que aún no se ha configurado, haga clic en el menú de tres puntos (⋮) para crear otro perfil. Consulte [Agregar perfiles](#).

- a Si el menú desplegable **Perfiles de IKE** está habilitado, seleccione el perfil de IKE.
- b Seleccione el perfil de túnel de IPsec si el menú desplegable **Perfiles de IPsec** no está deshabilitado.

- c Seleccione el perfil de DPD que prefiera si el menú desplegable **Perfiles de DPD** está habilitado.
- d Seleccione el modo preferido en el menú desplegable **Modo de inicio de conexión**.

El modo de inicio de conexión define la directiva utilizada por el endpoint local en el proceso de creación del túnel. El valor predeterminado es **Iniciador**. En la siguiente tabla, se describen los diferentes modos de inicio de conexión disponibles.

Tabla 5-3. Modos de inicio de conexión

Modo de inicio de conexión	Descripción
Initiator	El valor predeterminado. En este modo, el endpoint local inicia la creación del túnel VPN de IPsec y responde a las solicitudes entrantes de instalación del túnel de la puerta de enlace del mismo nivel.
On Demand	No utilice con la VPN basada en rutas. Este modo se aplica únicamente a la VPN basada en directivas.
Respond Only	La VPN de IPsec nunca inicia una conexión. El sitio del mismo nivel siempre inicia la solicitud de conexión, y el endpoint local responde a dicha solicitud de conexión.

- 17 Si desea reducir la carga del tamaño de segmento máximo (MSS) de la sesión de TCP durante la conexión de IPsec, habilite **Fijación de MSS de TCP**, seleccione el valor **Dirección de MSS de TCP** y, opcionalmente, establezca el **Valor de MSS de TCP**. []

Consulte la sección [Fijación de MSS de TCP](#) para obtener más información.

- 18 Si desea incluir esta sesión de IPsec como parte de una etiqueta de grupo específico, escriba el nombre de la etiqueta en **Etiquetas**.
- 19 Haga clic en **Guardar**.

Resultados

Cuando la nueva sesión de VPN de IPsec basada en rutas se configura correctamente, se agrega a la lista de sesiones de VPN de IPsec disponibles. Está en modo de solo lectura.

Pasos siguientes

- Compruebe que el estado del túnel VPN de IPsec sea Activo. Para obtener más información, consulte [Supervisar y solucionar problemas de sesiones de VPN](#).
- Configure el enrutamiento mediante una ruta estática o BGP. Consulte [Configurar una ruta estática](#) o [Configurar BGP](#).
- Si es necesario, administre la información de la sesión de VPN de IPsec; para ello, haga clic en el menú de tres puntos (⋮) a la izquierda de la fila de la sesión. Seleccione una de las acciones que puede realizar.

Información sobre las suites de cumplimiento admitidas

A partir de NSX-T Data Center 2.5, puede especificar qué suites de cumplimiento de seguridad desea usar para configurar los perfiles de seguridad utilizados para una sesión de VPN de IPSec.

Una suite de cumplimiento de seguridad tiene valores predefinidos que se utilizan para distintos parámetros de seguridad y que no se pueden modificar. Al seleccionar una suite de cumplimiento, los valores predefinidos se utilizan automáticamente para el perfil de seguridad de la sesión de VPN de IPSec que se está configurando.

En la siguiente tabla, se incluyen las suites de cumplimiento admitidas para los perfiles de IKE en NSX-T Data Center y los valores predefinidos para cada uno de ellas.

Nombre de la suite de cumplimiento	Versión de IKE	Algoritmo de cifrado	Algoritmo de resumen	Grupo Diffie Hellman
CNSA	IKEv2	AES 256	SHA2 384	Grupo 15, grupo 20
FIPS	IKE-Flex	AES 128	SHA2 256	Grupo 20
Perfil base	IKEv1	AES 128	SHA2 256	Grupo 14
PRIME	IKEv2	AES GCM 128	No establecido	Grupo 19
Suite-B-GCM-128	IKEv2	AES 128	SHA2 256	Grupo 19
Suite-B-GCM-256	IKEv2	AES 256	SHA2 384	Grupo 20

En la siguiente tabla, se incluyen las suites de cumplimiento admitidas para los perfiles de IPSec en NSX-T Data Center y los valores predefinidos para cada una de ellas.

Nombre de la suite de cumplimiento	Algoritmo de cifrado	Algoritmo de resumen	Grupo de PFS	Grupo Diffie-Hellman
CNSA	AES 256	SHA2 384	Habilitado	Grupo 15, grupo 20
FIPS	AES GCM 128	No establecido	Habilitado	Grupo 20
Perfil base	AES 128	SHA2 256	Habilitado	Grupo 14
PRIME	AES GCM 128	No establecido	Habilitado	Grupo 19
Suite-B-GCM-128	AES GCM 128	No establecido	Habilitado	Grupo 19
Suite-B-GCM-256	AES GCM 256	No establecido	Habilitado	Grupo 20

Fijación de MSS de TCP

La fijación de MSS de TCP permite reducir el valor del tamaño de segmento máximo (MSS) utilizado por una sesión TCP durante el establecimiento de la conexión a través de un túnel IPSec. Esta función se admite a partir de NSX-T Data Center 2.5.

El MSS de TCP es la cantidad máxima de datos en bytes que un host está dispuesto a aceptar en un único segmento TCP. Cada extremo de una conexión TCP envía su valor de MSS deseado a su extremo del mismo nivel durante un protocolo de enlace de tres vías, en el que MSS es una de las opciones de encabezado TCP que se utilizan en un paquete SYN de TCP. El MSS de TCP se calcula en función de la unidad de transmisión máxima (MTU) de la interfaz de salida del host del remitente.

Cuando un tráfico TCP pasa por una VPN de IPsec o cualquier tipo de túnel VPN, se agregan encabezados adicionales al paquete original para mantenerlos seguros. En el modo de túnel IPsec, se utilizan los encabezados adicionales IP, ESP y, opcionalmente, UDP (si la traducción de puertos está presente en la red). Debido a estos encabezados adicionales, el tamaño del paquete encapsulado supera la MTU de la interfaz de VPN. El paquete puede quedar fragmentado o descartado en función de la directiva DF.

Para evitar la fragmentación o el descarte de paquetes, puede ajustar el valor de MSS para la sesión de IPsec habilitando la función de fijación de MSS de TCP. Desplácese hasta **Redes > VPN > Sesiones de IPsec**. Cuando agregue una sesión de IPsec o edite una existente, expanda la sección **Propiedades avanzadas** y habilite **Fijación de MSS de TCP**.

Puede configurar el valor de MSS calculado previamente adecuado para la sesión de IPsec configurando las opciones **Dirección de MSS de TCP** y **Valor de MSS de TCP**. El valor de MSS configurado se utiliza para la fijación de MSS. Puede optar por utilizar el cálculo de MSS dinámico configurando la opción **Dirección de MSS de TCP** y dejando **Valor de MSS de TCP** en blanco. El valor de MSS se calcula automáticamente basándose en la MTU de la interfaz de la VPN, la sobrecarga de la VPN y la MTU de la ruta (PMTU) cuando está definida. El MSS efectivo se vuelve a calcular durante cada protocolo de enlace TCP para controlar dinámicamente los cambios de la MTU o la PMTU.

Agregar sesiones de VPN de capa 2

Después de haber configurado un servidor VPN de Capa 2 y un cliente VPN de Capa 2, debe agregar las sesiones de VPN de Capa 2 para ambos a fin de completar la configuración del servicio VPN de Capa 2.

Agregar una sesión del servidor VPN de capa 2

Después de crear un servicio de servidor de VPN de capa 2, debe agregar una sesión de VPN de capa 2 y asociarla a un segmento existente.

Los siguientes pasos utilizan la pestaña **Sesiones de VPN de capa 2** de la interfaz de usuario de NSX Manager para crear una sesión del servidor de VPN de capa 2. Seleccione también un endpoint local existente y el segmento que desee asociar a la sesión del servidor de VPN de capa 2.

Nota También puede agregar una sesión de servidor de VPN de capa 2 inmediatamente después de configurar correctamente el servicio del servidor de VPN de capa 2. Haga clic en **Sí** cuando se solicite para continuar con la configuración del servidor de VPN de capa 2, y seleccione **Sesiones > Agregar sesiones** en el panel Agregar servidor de VPN de capa 2. Para los primeros pasos del siguiente procedimiento, se presupone que ha seleccionado **No** para continuar con la configuración del servidor de VPN de capa 2. Si ha seleccionado **Sí**, vaya al paso 3 de la lista para seguir configurando la sesión del servidor de VPN de capa 2.

Requisitos previos

- Debe configurar un servicio de servidor de VPN de capa 2 antes de continuar. Consulte [Agregar un servicio de servidor VPN de Capa 2](#).
- Obtenga la información del endpoint local y la dirección IP remota que se usará con la sesión del servidor de VPN de capa 2 que desee agregar. Para crear un endpoint local, consulte [Agregar endpoints locales](#).
- Obtenga los valores de la clave precompartida (PSK) y la subred de la interfaz de túnel que se usará con la sesión del servidor de VPN de capa 2.
- Obtenga el nombre del segmento existente que desee asociar a la sesión del servidor de VPN de capa 2 que va a crear. Para obtener más información, consulte [Agregar un segmento](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta la pestaña **Redes > VPN > Sesiones de VPN de capa 2**.
- 3 Seleccione **Agregar sesión de VPN L2 > Servidor VPN de capa 2**.
- 4 Escriba un nombre para la sesión del servidor de VPN de capa 2.
- 5 En el menú desplegable **Servicio de VPN de capa 2**, seleccione el servicio del servidor de VPN de capa 2 para el que desee crear la sesión de VPN de capa 2.

Nota Si agrega esta sesión del servidor de VPN de capa 2 desde el cuadro de diálogo Establecer sesiones del servidor de VPN de capa 2, el servicio del servidor de VPN de capa 2 se indicará sobre el botón **Agregar sesión de L2**.

- 6 Seleccione un endpoint local existente en el menú desplegable.

Si desea crear otro endpoint local, haga clic en el menú de tres puntos (⋮) y seleccione **Agregar endpoint local**.

- 7 Introduzca la dirección IP del sitio remoto.

- 8 Para habilitar o deshabilitar la sesión del servidor de VPN de capa 2, haga clic en **Estado de administración**.

De forma predeterminada, el valor se establece como **Habilitado**, lo que significa que la sesión del servidor de VPN de Capa 2 se configurará hacia abajo hasta el nodo de NSX Edge.

- 9 Introduzca el valor de clave secreta en **Clave precompartida**.

Precaución Tenga cuidado al compartir y almacenar un valor de PSK porque se considera información confidencial.

- 10 Escriba una dirección de subred IP en **Interfaz de túnel** en formato CIDR.

Por ejemplo, 4.5.6.6/24. Esta subred es obligatoria.

- 11 Introduzca un valor en **Identificador remoto**.

Para los sitios del mismo nivel con autenticación por certificado, este identificador debe ser el nombre común indicado en el certificado para el sitio del mismo nivel. Para los elementos del mismo nivel con PSK, este identificador puede ser cualquier cadena. Se prefiere el uso de la dirección IP pública de la red VPN o un nombre FQDN para los servicios VPN como `Remote ID`.

- 12 Si desea incluir esta sesión como parte de un grupo específico, escriba el nombre de etiqueta en **Etiquetas**.

- 13 Haga clic en **Guardar** y en **Sí** cuando se le pregunte si desea continuar con la configuración del servicio de VPN.

Volverá al panel Agregar sesiones de VPN de capa 2, donde ahora estará habilitado el vínculo **Segmentos**.

- 14 Asocie un segmento existente a la sesión del servidor de VPN de capa 2.

- a Haga clic en **Segmentos > Establecer segmentos**.
- b En el cuadro de diálogo **Establecer segmentos**, haga clic en **Establecer segmento** para asociar un segmento existente a la sesión del servidor de VPN de capa 2.
- c En el menú desplegable **Segmento**, seleccione el segmento basado en VNI o VLAN que desea asociar a la sesión.
- d Introduzca un valor único en **Identificador de túnel VPN** que se utilizará para identificar el segmento seleccionado.
- e Haga clic en **Guardar** y luego en **Cerrar**.

En el panel o el cuadro de diálogo Establecer sesiones de L2VPN, el sistema ha aumentado el recuento de **Segmentos** de la sesión del servidor de VPN de capa 2.

- 15 Para finalizar la configuración de la sesión del servidor de VPN de capa 2, haga clic en **Cerrar edición**.

Resultados

En la pestaña **Servicios de VPN**, el sistema aumenta el recuento de **Sesiones** del servicio del servidor de VPN de capa 2 que ha configurado.

Pasos siguientes

Para completar la configuración del servicio de VPN de capa 2, también debe crear un servicio de VPN de capa 2 en el modo de cliente y una sesión de cliente de VPN de capa 2. Consulte [Agregar un servicio de cliente VPN de Capa 2](#) y [Agregar una sesión de cliente VPN de Capa 2](#).

Agregar una sesión de cliente VPN de Capa 2

Después de crear un servicio de cliente VPN de Capa 2, debe agregar una sesión de cliente VPN de Capa 2 y asociarla a un segmento existente.

En los siguientes pasos se utiliza la pestaña **Sesiones de VPN L2** de la interfaz de usuario de NSX Manager para crear una sesión de cliente VPN de Capa 2. Igualmente, se selecciona un endpoint local existente y el segmento que se asociará a la sesión de cliente VPN de Capa 2.

Nota También puede agregar una sesión de cliente VPN de Capa 2 inmediatamente después de configurar correctamente el servicio de cliente VPN de Capa 2. Haga clic en **Sí** cuando se le solicite continuar con la configuración del cliente VPN de Capa 2 y seleccione **Sesiones > Agregar sesiones** en el panel Agregar cliente VPN de Capa 2. En los primeros pasos del siguiente procedimiento se supone que seleccionó **No** en el aviso en el que se le preguntó si deseaba continuar con la configuración del cliente VPN de Capa 2. Si seleccionó **Sí**, vaya al tercero de los pasos siguientes para obtener instrucciones sobre lo que queda de la configuración de la sesión de cliente VPN de Capa 2.

Requisitos previos

- Se debe configurar un servicio de cliente VPN de Capa 2 antes de continuar. Consulte [Agregar un servicio de cliente VPN de Capa 2](#).
- Obtenga la información de direcciones IP para la IP local y la IP remota que se usarán con la sesión de cliente VPN de Capa 2 que se va a agregar.
- Obtenga el código del mismo nivel que se generó durante la configuración del servidor VPN de Capa 2. Consulte [Descargar el archivo de configuración de VPN de capa 2 de lado remoto](#).
- Obtenga el nombre del segmento existente que desea asociar a la sesión de cliente VPN de Capa 2 que está creando. Consulte [Agregar un segmento](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > VPN > Sesiones de VPN de capa 2**.
- 3 Seleccione **Agregar sesión de VPN L2 > Cliente VPN de capa 2**.

- 4 Introduzca un nombre para la sesión de cliente VPN de Capa 2.
- 5 En el menú desplegable **Servicio VPN**, seleccione el servicio de cliente VPN de Capa 2 con el que se asociará la sesión de VPN de Capa 2.

Nota Si va a agregar esta sesión de cliente VPN de Capa 2 en el cuadro de diálogo Establecer sesiones de cliente VPN de Capa 2, el servicio de cliente VPN de Capa 2 ya aparecerá indicado sobre el botón **Agregar sesión de L2**.

- 6 En el cuadro de texto **Dirección IP local**, escriba la dirección IP de la sesión de cliente VPN de Capa 2.
- 7 Introduzca la dirección IP remota del túnel de IPsec que se va a utilizar para la sesión del cliente VPN de Capa 2.
- 8 En el cuadro de texto **Configuración del mismo nivel**, introduzca el código del mismo nivel que se generó cuando configuró el servicio del servidor VPN de Capa 2.
- 9 Habilite o deshabilite **Estado de administración**.
De forma predeterminada, el valor se establece como **Habilitado**, lo que significa que la sesión del servidor de VPN de Capa 2 se configurará hacia abajo hasta el nodo de NSX Edge.
- 10 Haga clic en **Guardar** y en **Sí** cuando se le pregunte si desea continuar con la configuración del servicio de VPN.
- 11 Asocie un segmento existente a la sesión de cliente VPN de Capa 2.
 - a Seleccione **Segmentos > Agregar segmentos**.
 - b En el cuadro de diálogo **Establecer segmentos**, haga clic en **Agregar segmento**.
 - c En el menú desplegable **Segmento**, seleccione el segmento basado en VNI o VLAN que desea asociar a la sesión del cliente VPN de capa 2.
 - d Introduzca un valor único en **Identificador de túnel VPN** que se utilizará para identificar el segmento seleccionado.
 - e Haga clic en **Cerrar**.
- 12 Para finalizar la configuración de la sesión de cliente VPN de Capa 2, haga clic en **Cerrar edición**.

Resultados

En la pestaña **Servicios VPN**, el recuento de sesiones se actualiza para el servicio de cliente VPN de Capa 2 que configuró.

Descargar el archivo de configuración de VPN de capa 2 de lado remoto

Para configurar la sesión del cliente VPN de Capa 2, debe obtener el código del mismo nivel que se generó al configurar la sesión del servidor VPN de Capa 2.

Requisitos previos

- Antes de continuar, debe tener configurados correctamente un servicio del servidor VPN de Capa 2 y una sesión. Consulte [Agregar un servicio de servidor VPN de Capa 2](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta la pestaña **Redes > VPN > Sesiones de VPN de capa 2**.
- 3 En la tabla de sesiones de VPN de Capa 2, expanda la fila de la sesión del servidor VPN de Capa 2 que desea usar para configurar la sesión de cliente VPN de Capa 2.
- 4 Haga clic en **Descargar configuración** y, a continuación, en **Sí** en el cuadro de diálogo de advertencia.

Se descarga un archivo de texto con el nombre `L2VPNSession_<nombre-de-la-sesión-del-servidor-VPN-de-Capa-2>_config.txt`. Contiene el código del mismo nivel para la configuración de VPN de Capa 2 de lado remoto.

Precaución Tenga cuidado al almacenar y compartir el código del mismo nivel porque contiene un valor PSK, que se considera información confidencial.

Por ejemplo, `L2VPNSession L2VPNServer config.txt` contiene la siguiente configuración.

```
[
{
    "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/l-  
policyconnectivity-693/ipsec-vpn-services/IpsecService1/sessions/Routebase1",
    "peer_code":
        "MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFWsXAiOiIxNjkuMjU0LjY0LjIiLCJKc3RUYX  
BJcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1  
vbiI6ImlrZXlyIiwic2l0ZW5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0Iiwic2l0ZW5jcmlldEFuZERpZ2  
VzdCI6ImFlcylnY20vc2hhLTIlNiIsInBzayI  
6IlNd2FyZTEyMyIsInRlbm5lbHMlOlt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlc2lkIjoiaTAuNTAuNTAuMS  
IsImxvY2FsVnRpSXAiOiIxNjkuMi4yLjMvMzeifV19"
}
]
```

- 5 Copie el código del mismo nivel, que se utiliza para configurar la sesión y el servicio del cliente de VPN de capa 2.

Usando el archivo de configuración de ejemplo anterior, debe copiar el siguiente código del mismo nivel para utilizarlo con la configuración del cliente de VPN de capa 2.

MCw3ZjBjYzZjLHsic2l0ZU5hbWUoiOiJSb3V0ZWJhc2UxIiwic3JjVGFWsXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
JcCI6IjE2OS4yNTQunQnJQuMSIsImlrZU9wdG1
vbiI6ImlrZXZyYiIiwic2Z5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0IiwiZW5jcnlwdEFuZERpZ2
VzdCI6ImFlcylnY20vc2hhLTI1NiIsInBzayI
6IlZNd2FyZTEyMyIsInR1bm5lbHMiOlt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwic2Z5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0IiwiZW5jcnlwdEFuZERpZ2
VzdCI6ImFlcylnY20vc2hhLTI1NiIsInBzayI
IsImxvY2FsVnRwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
JcCI6IjE2OS4yNTQunQnJQuMSIsImlrZU9wdG1

Pasos siguientes

Configure el servicio de cliente de VPN de Capa 2 y su sesión. Consulte [Agregar un servicio de cliente VPN de Capa 2](#) y [Agregar una sesión de cliente VPN de Capa 2](#).

Agregar endpoints locales

Debe configurar un endpoint local para usarlo con la VPN de IPSec que va a configurar.

Los siguientes pasos utilizan la pestaña **Endpoints locales** de la interfaz de usuario de NSX Manager. También puede crear un endpoint local durante en el proceso de adición de una sesión de VPN de IPSec. Para ello, haga clic en el menú de tres puntos (⋮) y seleccione **Agregar endpoint local**. Si se encuentra en pleno proceso de configuración de una sesión de VPN de IPSec, vaya al paso 3 de la lista para continuar con la creación de un nuevo endpoint local.

Requisitos previos

- Si utiliza un modo de autenticación basada en certificados para la sesión de VPN de IPSec que usará el endpoint local que va a configurar, obtenga la información del certificado que debe usar el endpoint local.
- Asegúrese de haber configurado un servicio de VPN de IPSec al que se asociará este endpoint local.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta **Redes > VPN > Endpoints locales**, y haga clic en **Agregar endpoint local**.
- 3 Escriba un nombre para el endpoint local.
- 4 En el menú desplegable **Servicio VPN**, seleccione el servicio VPN de IPSec con el que se asociará este endpoint local.
- 5 Introduzca una dirección IP para el endpoint local.

Para un servicio VPN de IPSec que se ejecuta en una puerta de enlace de nivel 0, la dirección IP del endpoint local debe ser diferente de la dirección IP de la interfaz de enlace superior de la puerta de enlace de nivel 0. La dirección IP del endpoint local que proporcione está asociada con la interfaz de bucle invertido para la puerta de enlace de nivel 0 y también se publica como una dirección IP enrutable a través de la interfaz de enlace superior. Para que el servicio VPN de IPSec se ejecute en una puerta de enlace de nivel 1, para que la dirección IP del endpoint local pueda enrutarse, el anuncio de ruta para los endpoints locales de IPSec debe estar habilitado en la configuración de la puerta de enlace de nivel 1. Consulte [Agregar una puerta de enlace de nivel 1](#) para obtener más información.

- 6 Si utiliza el modo de autenticación basada en certificados para la sesión de VPN de IPSec, en el menú desplegable **Certificado del sitio**, seleccione el certificado que utilizará el endpoint local.

- 7 (opcional) De forma opcional, puede agregar una descripción en **Descripción**.
- 8 Introduzca el valor del **Identificador local** que se utiliza para identificar la instancia local de NSX Edge.

Este identificador local es el identificador del sitio remoto de mismo nivel. El identificador local debe ser la dirección IP pública o el FQDN del sitio remoto. Para las sesiones de VPN basadas en certificados que se definieron con el endpoint local, el identificador local se derivará del certificado asociado con el endpoint local. Se omitirá el identificador especificado en el cuadro de texto **Identificador local**. El identificador local derivado del certificado para una sesión de VPN depende de las extensiones presentes en el certificado.

- Si la extensión X509v3 `Subject Alternative Name` de X509v3 no está presente en el certificado, se utilizará el nombre distintivo (DN) como el valor del identificador local.
- Si la extensión X509v3 `X509v3 Subject Alternative Name` se encuentra en el certificado, se tomará uno de los nombres alternativos del asunto como el valor del identificador local.

- 9 En los menús desplegables **Certificados de CA de confianza** y **Lista de revocación de certificados**, seleccione los certificados adecuados necesarios para el endpoint local.
- 10 Especifique una etiqueta si es necesario.
- 11 Haga clic en **Guardar**.

Agregar perfiles

NSX-T Data Center proporciona el perfil del túnel de IPsec generado por el sistema y un perfil de IKE que se asignan de forma predeterminada cuando se configura un servicio VPN de Capa 2 o VPN de IPsec. Se crea un perfil de DPD generado por el sistema para una configuración de VPN de IPsec.

Los perfiles de IKE e IPsec ofrecen información acerca de los algoritmos que se utilizan para autenticar, cifrar y establecer un secreto compartido entre los sitios de red. El perfil de DPD proporciona información acerca del número de segundos que se debe esperar entre los sondeos.

Si decide no utilizar los perfiles predeterminados que proporciona NSX-T Data Center, puede configurar el suyo propio con la información que se ofrece en los temas que siguen en esta sección.

Agregar perfiles de IKE

Los perfiles de intercambio de claves por red (Internet Key Exchange, IKE) ofrecen información acerca de los algoritmos que se utilizan para autenticar, cifrar y establecer un secreto compartido entre sitios de red cuando se establece un túnel de IKE.

NSX-T Data Center proporciona perfiles de IKE generados por el sistema que se asignan de forma predeterminada cuando se configura un servicio de VPN de IPsec o un servicio de VPN de Capa 2. En la siguiente tabla se muestran los perfiles predeterminados que se proporcionan.

Tabla 5-4. Perfiles de IKE predeterminados que se utilizan para los servicios VPN de IPsec o VPN de Capa 2

Nombre de perfil de IKE predeterminado	Descripción
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> ■ Se utiliza para una configuración de servicio VPN de Capa 2. ■ Se configura con IKE V2, el algoritmo de cifrado AES 128, el algoritmo SHA2 256 y el algoritmo de intercambio de claves de grupo 14 de Diffie-Hellman.
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> ■ Se utiliza para una configuración de servicio de VPN de IPsec. ■ Se configura con IKE V2, el algoritmo de cifrado AES 128, el algoritmo SHA2 256 y el algoritmo de intercambio de claves de grupo 14 de Diffie-Hellman.

En lugar de los perfiles IKE predeterminados, también puede seleccionar uno de los conjuntos de cumplimiento compatibles a partir de NSX-T Data Center 2.5. Consulte [Información sobre las suites de cumplimiento admitidas](#) para obtener más información.

Si decide no usar las suites de cumplimiento o los perfiles IKE predeterminados que se proporcionan, puede configurar sus propios perfiles IKE siguiendo estos pasos.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Haga clic en la pestaña **Redes > VPN > Perfiles**.
- 3 Seleccione el tipo de perfil **Perfiles de IKE** y haga clic en **Agregar perfil de IKE**.
- 4 Introduzca un nombre para el perfil de IKE.
- 5 En el menú desplegable **Versión de IKE**, seleccione la versión de IKE que se va a usar para configurar una asociación de seguridad (Security Association, SA) en el paquete de protocolos IPsec.

Tabla 5-5. Versiones de IKE

Versión de IKE	Descripción
IKEv1	Cuando se selecciona, la VPN de IPsec se inicia y solo responde a un protocolo IKEv1.
IKEv2	Esta es la versión predeterminada. Cuando se seleccione, la VPN de IPsec se iniciará y responderá a un solo protocolo IKEv2.
IKE Flex	Si se selecciona esta versión y se produce un error al establecer el túnel con el protocolo IKEv2, el sitio de origen no se revierte e iniciará una conexión con el protocolo IKEv1. En lugar de eso, si el sitio remoto inicia una conexión con el protocolo IKEv1, la conexión se aceptará.

- 6 Seleccione el cifrado, el resumen y los algoritmos del grupo Diffie-Hellman de los menús desplegables. Puede seleccionar varios algoritmos para aplicarlos o anular la selección de cualquier algoritmo ya seleccionado que no desee aplicar.

Tabla 5-6. Algoritmos utilizados

Tipo de algoritmo	Valores válidos	Descripción
Cifrado	<ul style="list-style-type: none"> ■ AES 128 (predeterminado) ■ AES 256 ■ AES GCM 128 ■ AES GCM 192 ■ AES GCM 256 	<p>El algoritmo de cifrado que se utiliza durante la negociación de intercambio de claves por red (Internet Key Exchange, IKE).</p> <p>Los algoritmos AES-GCM son compatibles cuando se usan con IKEv2. No se admiten cuando se utiliza con IKEv1.</p>
Resumen	<ul style="list-style-type: none"> ■ SHA2 256 (predeterminado) ■ SHA1 ■ SHA2 384 ■ SHA2 512 	<p>El algoritmo de hash seguro usado durante la negociación de IKE.</p> <p>Si AES-GCM es el único algoritmo de cifrado seleccionado en el cuadro de texto Algoritmo de cifrado, no se podrán especificar algoritmos hash en el cuadro de texto Algoritmo de resumen, según la sección 8 de RFC 5282. Además, se selecciona y utiliza implícitamente el algoritmo de función pseudoaleatoria PRF-HMAC-SHA2-256 en la negociación de la asociación de seguridad (SA) de IKE. El algoritmo PRF-HMAC-SHA2-256 también debe configurarse en la puerta de enlace del mismo nivel para que la fase 1 de la negociación de la SA de IKE se realice correctamente.</p> <p>Si se especifican más algoritmos en el cuadro de texto Algoritmo de cifrado, además del algoritmo AES-GCM, se pueden seleccionar uno o varios algoritmos hash en el cuadro de texto Algoritmo de resumen. Además, el algoritmo PRF utilizado en la negociación de la SA de IKE se determina implícitamente en función de los algoritmos hash configurados. Al menos uno de los algoritmos PRF que coinciden también deben configurarse en la puerta de enlace del mismo nivel para que la fase 1 de la negociación de la SA de IKE se realice correctamente. Por ejemplo, si el cuadro de texto Algoritmo de cifrado contiene AES 128 y AES GCM 128 y se especifica SHA1 en el cuadro de texto Algoritmo de resumen, el algoritmo PRF-HMAC-SHA1 se utilizará durante la negociación de la SA de IKE. También debe configurarse en la puerta de enlace del mismo nivel.</p>
Grupo Diffie-Hellman	<ul style="list-style-type: none"> ■ Grupo 14 (predeterminado) ■ Grupo 2 ■ Grupo 5 ■ Grupo 15 ■ Grupo 16 ■ Grupo 19 ■ Grupo 20 	<p>Los esquemas de criptografía que utilizan el sitio del mismo nivel y NSX Edge para establecer un secreto compartido a través de un canal de comunicaciones no seguro.</p>

Tabla 5-6. Algoritmos utilizados (continuación)

Tipo de algoritmo	Valores válidos	Descripción
	■ Grupo 21	

Nota Cuando intenta establecer un túnel de VPN de IPSec con un cliente VPN GUARD (anteriormente, cliente VPN QuickSec) a través de dos algoritmos de cifrado o dos algoritmos de resumen, el cliente VPN GUARD agrega otros algoritmos a la lista de negociación propuesta. Por ejemplo, si especificó AES 128 y AES 256 como algoritmos de cifrado, y SHA2 256 y SHA2 512 como algoritmos de resumen en el perfil de IKE que se va a usar para establecer el túnel de VPN de IPSec, el cliente VPN GUARD también propondrá AES 192 y SHA2 384 en la lista de negociación. En este caso, NSX-T Data Center utilizará el primer algoritmo de cifrado que seleccionó al establecer el túnel de VPN de IPSec.

- 7 Introduzca un valor de vigencia en segundos para la asociación de seguridad (Security Association, SA) si quiere que sea diferente al valor predeterminado de 86.400 segundos (24 horas).
- 8 Proporcione una descripción y agregue una etiqueta según corresponda.
- 9 Haga clic en **Guardar**.

Resultados

Se agregará una fila nueva a la tabla de perfiles de IKE disponibles. Para editar o eliminar un perfil que no haya creado el sistema, haga clic en el menú de tres puntos (⋮) y seleccione una opción de la lista de acciones disponibles.

Agregar perfiles de IPSec

Los perfiles del protocolo de seguridad de Internet (Internet Protocol Security, IPSec) ofrecen información acerca de los algoritmos que se utilizan para autenticar, cifrar y establecer un secreto compartido entre los sitios de red cuando se establece un túnel de IPSec.

NSX-T Data Center proporciona perfiles de IPSec generados por el sistema que se asignan de forma predeterminada cuando se configura un servicio de VPN de IPSec o un servicio de VPN de Capa 2. En la siguiente tabla se muestran los perfiles de IPSec predeterminados que se proporcionan.

Tabla 5-7. Perfiles de IPSec predeterminados que se utilizan para los servicios VPN de IPSec o VPN de Capa 2

Nombre del perfil de IPSec predeterminado	Descripción
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> ■ Se utiliza para la VPN de Capa 2. ■ Se configura con el algoritmo de cifrado AES GCM 128 y el algoritmo de intercambio de claves del grupo 14 de Diffie-Hellman.
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> ■ Se utiliza para la VPN de IPSec. ■ Se configura con el algoritmo de cifrado AES GCM 128 y el algoritmo de intercambio de claves del grupo 14 de Diffie-Hellman.

En lugar del perfil de IPSec predeterminado, también puede seleccionar uno de los conjuntos de cumplimiento compatibles a partir de NSX-T Data Center 2.5. Consulte [Información sobre las suites de cumplimiento admitidas](#) para obtener más información.

Si decide no usar las suites de cumplimiento o los perfiles IPSec predeterminados que se proporcionan, puede configurar sus propios perfiles IPSec siguiendo estos pasos.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta la pestaña **Redes > VPN > Perfiles**.
- 3 Seleccione el tipo de perfil **Perfiles de IPSec** y haga clic en **Agregar perfil de IPSec**.
- 4 Introduzca un nombre para el perfil de IPSec.
- 5 En los menús desplegables, seleccione el cifrado, el resumen y los algoritmos de Diffie-Hellman. Puede seleccionar varios algoritmos para aplicarlos.
Anule la selección de los que no quiera usar.

Tabla 5-8. Algoritmos utilizados

Tipo de algoritmo	Valores válidos	Descripción
Cifrado	<ul style="list-style-type: none"> ■ AES GCM 128 (predeterminado) ■ AES 128 ■ AES 256 ■ AES GCM 192 ■ AES GCM 256 ■ No hay autenticación de cifrado AES GMAC 128 ■ No hay autenticación de cifrado AES GMAC 192 ■ No hay autenticación de cifrado AES GMAC 256 ■ Sin cifrado 	El algoritmo de cifrado que se utiliza durante la negociación de IPSec (seguridad de protocolos de Internet).
Resumen	<ul style="list-style-type: none"> ■ SHA1 ■ SHA2 256 ■ SHA2 384 ■ SHA2 512 	El algoritmo de hash seguro usado durante la negociación de IPSec.
Grupo Diffie-Hellman	<ul style="list-style-type: none"> ■ Grupo 14 (predeterminado) ■ Grupo 2 ■ Grupo 5 ■ Grupo 15 ■ Grupo 16 ■ Grupo 19 ■ Grupo 20 ■ Grupo 21 	Los esquemas de criptografía que utilizan el sitio del mismo nivel y NSX Edge para establecer un secreto compartido a través de un canal de comunicaciones no seguro.

- 6** Anule la selección de **Grupo de PFS** si decide no utilizar el protocolo Grupo PFS en el servicio VPN.

Esta opción está seleccionado de forma predeterminada.

- 7** En el cuadro de texto **Vigencia de SA**, modifique el número predeterminado de segundos que deben transcurrir hasta que se deba restablecer el túnel de IPSec.

De forma predeterminada, se utiliza una vigencia de SA de 24 horas (86.400 segundos).

- 8** Seleccione el valor de **Bit de DF** que se usará con el túnel de IPSec.

Este valor determina cómo se procesa el bit de "No fragmentar" (Don't Fragment, DF) que se incluye en el paquete de datos recibido. Los valores aceptables se describen en la siguiente tabla.

Tabla 5-9. Valores de bit de DF

Valor de bit de DF	Descripción
COPY	El valor predeterminado. Cuando se selecciona este valor, NSX-T Data Center copia el valor del bit de DF del paquete recibido al paquete que se reenvía. Este valor implica que, si se estableció el bit de DF en el paquete de datos recibido, también estará configurado en el paquete tras el cifrado.
CLEAR	Cuando se selecciona este valor, NSX-T Data Center omite el valor del bit de DF del paquete de datos recibido y el bit de DF es siempre 0 en el paquete cifrado.

9 Proporcione una descripción y agregue una etiqueta, si lo considera necesario.

10 Haga clic en **Guardar**.

Resultados

Se agregará una fila nueva a la tabla de perfiles de IPSec disponibles. Para editar o eliminar un perfil que no haya creado el sistema, haga clic en el menú de tres puntos (⋮) y seleccione una opción de la lista de acciones disponibles.

Agregar perfiles de DPD

Un perfil de DPD (Dead Peer Detection) proporciona información sobre la cantidad de segundos que se espera entre sondeos para detectar si un elemento del mismo nivel de IPSec está activo o no.

NSX-T Data Center proporciona un perfil de DPD generado por el sistema con el nombre `nsx-default-l3vpn-dpd-profile`, el cual se asigna de forma predeterminada cuando se configura un servicio VPN de IPSec.

Si decide no utilizar el perfil de DPD predeterminado que se ofrece, puede configurar uno propio mediante los siguientes pasos.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Redes > VPN > Perfiles**.
- 3 Seleccione el tipo de perfil **Perfiles de DPD** y haga clic en **Agregar perfil de DPD**.
- 4 Introduzca un nombre para el perfil de DPD.
- 5 En el cuadro de texto **Intervalo de sondeo de DPD**, introduzca el número de segundos que desea que espere NSX-T Data Center antes de enviar el siguiente sondeo DPD. El valor predeterminado es de 60 segundos.

Si el nodo NSX Edge recibe una respuesta del sitio remoto del mismo nivel, se reiniciará el temporizador del intervalo de sondeo DPD. Si el nodo NSX Edge no recibe respuesta del sitio del mismo nivel pasados 0,5 segundos desde el envío del siguiente sondeo DPD,

se establecerá un temporizador de retransmisión en 0,5 segundos. El nodo NSX Edge retransmitirá el siguiente sondeo de DPD después de que se alcance el temporizador de retransmisión. Si el sitio remoto del mismo nivel sigue sin responder, el temporizador de retransmisión aumentará exponencialmente hasta un límite máximo de 6 segundos. El nodo NSX Edge seguirá retransmitiendo el sondeo DPD cada vez que expire el temporizador de retransmisión. El nodo NSX Edge se retransmite hasta un máximo de 30 veces antes de declarar que el sitio del mismo nivel está inactivo y anular la asociación de seguridad (SA) en el vínculo del elemento del mismo nivel inactivo. El tiempo total que se tarda en retransmitir el sondeo DPD 30 veces es aproximadamente 2 minutos y 45 segundos.

6 Proporcione una descripción y agregue una etiqueta según corresponda.

7 Haga clic en **Guardar**.

Resultados

Se agrega una nueva fila en la tabla de perfiles DPD disponibles. Para editar o eliminar un perfil que no haya creado el sistema, haga clic en el menú de tres puntos (⋮) y seleccione una opción de la lista de acciones disponibles.

Agregar una instancia de Edge autónoma como cliente VPN de Capa 2

Puede usar una VPN de Capa 2 para ampliar las redes de Capa 2 a un sitio que no administre NSX-T Data Center. Puede implementar una instancia de NSX Edge autónoma en el sitio como cliente VPN de Capa 2. La instancia de NSX Edge autónoma es fácil de implementar y programar. Además ofrece una VPN de alto rendimiento. Para implementar la instancia de NSX Edge autónoma, se utiliza un archivo OVF de un host que no administre NSX-T Data Center. También puede habilitar el modo de HA para la redundancia de VPN mediante la implementación de una instancia de Edge autónoma principal y secundaria como cliente de VPN de Capa 2.

Requisitos previos

- Cree un grupo de puertos y asócielo al vSwitch del host.
- Cree un grupo de puertos para el puerto de extensión de Capa 2 interno.
- Obtenga las direcciones IP para la IP local y la IP remota que se usarán con la sesión de cliente VPN de Capa 2 que se va a agregar.
- Obtenga el código del mismo nivel que se generó durante la configuración del servidor VPN de Capa 2.

Procedimiento

- 1** Utilice vSphere Web Client para iniciar sesión en vCenter Server, que administra el entorno que no es NSX.
- 2** Seleccione **Hosts y clústeres** y expanda los clústeres para ver los hosts disponibles.

- 3 Haga clic con el botón derecho en el host en el que desea instalar la instancia NSX Edge autónoma y seleccione **Implementar plantilla OVF**.
- 4 Introduzca la URL para descargar e instalar el archivo OVF desde Internet, o bien haga clic en **Examinar** para buscar la carpeta en el equipo que contiene el archivo OVF de la instancia de NSX Edge autónoma y, a continuación, haga clic en **Siguiente**.
- 5 En la página **Seleccionar nombre y carpeta**, introduzca un nombre para la instancia de NSX Edge autónoma y seleccione la carpeta o el centro de datos donde desee implementarla. A continuación, haga clic en **Siguiente**.
- 6 En la página **Seleccionar recurso informático**, seleccione el destino del recurso informático.
- 7 En la página Detalles de plantilla de OVF, revise la información de la plantilla y haga clic en **Siguiente**.
- 8 En la página **Configuración**, seleccione una opción de configuración para la implementación.
- 9 En la página **Seleccionar almacenamiento**, seleccione la ubicación para almacenar los archivos de la configuración y los archivos del disco.
- 10 En la página **Seleccionar redes**, configure las redes que debe utilizar la plantilla implementada. Seleccione el grupo de puertos creado para la interfaz de vínculo superior, así como el grupo de puertos que creó para el puerto de extensión de Capa 2, e introduzca la interfaz de HA. Haga clic en **Siguiente**.
- 11 En la página **Personalizar plantilla**, introduzca los siguientes valores y haga clic en **Siguiente**.
 - a Escriba la contraseña de administrador de la CLI y, a continuación, vuelva a escribirla.
 - b Escriba la contraseña de habilitación de la CLI y, a continuación, vuelva a escribirla.
 - c Escriba la contraseña raíz de la CLI y, a continuación, vuelva a escribirla.
 - d Introduzca la dirección IPv4 para la red de administración.
 - e Introduzca la siguiente información del **puerto externo**: el identificador de VLAN, la interfaz de salida, la dirección IP y la longitud del prefijo de IP de forma que la interfaz de salida se asigne a la red con el grupo de puertos de la interfaz de vínculo superior.

Si la interfaz de salida está conectada a un grupo de puertos troncales, especifique un identificador de VLAN. Por ejemplo, **20,eth2,192.168.5.1,24**. También puede configurar el grupo de puertos con un identificador de VLAN y utilizar VLAN 0 para el **puerto externo**.
 - f (opcional) Para configurar el modo de HA, introduzca los detalles del **puerto de HA**, donde la interfaz de salida se asigna a la red de HA correspondiente.
 - g (opcional) Al implementar una instancia de NSX Edge autónoma como nodo secundario para HA, seleccione **Implementar esta instancia de Edge autónoma como nodo secundario**.

Utilice el mismo archivo OVF como nodo principal e introduzca la dirección IP, el nombre de usuario, la contraseña y la huella digital del nodo principal.

Para recuperar la huella digital del nodo principal, inicie sesión en el nodo principal y ejecute el siguiente comando:

```
get certificate api thumbprint
```

Asegúrese de que las direcciones IP de VTEP de los nodos principal y secundario se encuentren en la misma subred y estén conectados al mismo grupo de puertos. Una vez que complete la implementación e inicie el nodo secundario de Edge, se conectará al nodo principal para formar un clúster Edge.

- 12 En la página **Listo para completar**, revise la configuración de la instancia de Edge autónoma y haga clic en **Finalizar**.

Nota Si se producen errores durante la implementación, se mostrará un mensaje del día en la CLI. También puede utilizar una llamada API para buscar errores:

```
GET https://<nsx-mgr>/api/v1/node/status
```

Los errores se clasifican como errores leves y graves. Utilice llamadas de API para resolver los errores leves según sea necesario. Puede borrar el mensaje del día mediante una llamada API:

```
POST /api/v1/node/status?action=clear_bootup_error
```

-
- 13 Encienda el dispositivo de NSX Edge autónomo.
 - 14 Inicie sesión en el cliente de NSX Edge autónomo.
 - 15 Seleccione **VPN de Capa 2 > Agregar sesión** e introduzca los siguientes valores:
 - a Introduzca un nombre de sesión.
 - b Introduzca la dirección IP local y la dirección IP remota.
 - c Introduzca el código del mismo nivel del servidor VPN de Capa 2. Consulte [Descargar el archivo de configuración de VPN de capa 2 de lado remoto](#) para obtener más información sobre cómo obtener el código del mismo nivel.
 - 16 Haga clic en **Guardar**.
 - 17 Seleccione **Puerto > Agregar puerto** para crear un puerto de extensión de Capa 2.
 - 18 Introduzca un nombre, una VLAN y seleccione una interfaz de salida.
 - 19 Haga clic en **Guardar**.
 - 20 Seleccione **VPN de Capa 2 > Adjuntar puerto** e introduzca los siguientes valores:
 - a Seleccione la sesión de VPN de capa 2 que creó.
 - b Seleccione el puerto de extensión de Capa 2 que creó.
 - c Introduzca un identificador de túnel.

21 Haga clic en Asociar.

Puede crear puertos de extensión de Capa 2 adicionales y asociarlos a la sesión si necesita ampliar varias redes de capa 2.

22 Utilice el navegador para iniciar sesión en la instancia de NSX Edge autónoma o use llamadas API para ver el estado de la sesión de VPN de Capa 2.

Nota Si se modifica la configuración del servidor VPN de Capa 2, asegúrese de volver a descargar el código del mismo nivel y actualizar la sesión con ese código nuevo.

Comprobar el estado realizado de una sesión de VPN de IPSec

Después de enviar una solicitud de actualización de configuración para una sesión de VPN de IPSec, puede comprobar si el estado solicitado se procesó correctamente en el plano de control local NSX-T Data Center en los nodos de transporte.

Cuando se crea una sesión de VPN de IPSec, se crean varias entidades: un perfil de IKE, un perfil de DPD, un perfil de túnel, un endpoint local, el servicio de VPN de IPSec y una sesión de VPN de IPSec. Todas estas entidades comparten el mismo intervalo de `IPSecVPNSession`, por lo que es posible obtener el estado de realización de todas las entidades de la sesión de VPN de IPSec usando la misma llamada API de `GET`. Puede comprobar el estado de realización solo con la API.

Requisitos previos

- Familiarícese con la VPN de IPSec. Consulte [Información de VPN de IPSec](#).
- Compruebe que la VPN de IPSec se haya configurado correctamente. Consulte [Agregar un servicio de VPN de IPSec](#).
- Debe tener acceso a la API de NSX Manager.

Procedimiento

- 1 Envíe una solicitud de llamada API de `POST`, `PUT` o `DELETE`.

Por ejemplo:

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
```

```

    "id": "1026",
    "sources": [
      {
        "subnet": "1.1.1.0/24"
      }
    ],
    "logged": true,
    "destinations": [
      {
        "subnet": "2.1.4..0/24"
      }
    ],
    "action": "PROTECT",
    "enabled": true,
    "_revision": 1
  }
]
}

```

- 2 Busque y copie el valor de `x-nsx-requestid` en el encabezado de respuesta devuelto.

Por ejemplo:

```
x-nsx-requestid    e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 Solicite el estado de realización de la sesión de VPN de IPsec mediante la siguiente llamada de GET.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

La siguiente llamada API utiliza los valores de `id` y `x-nsx-requestid` en los ejemplos de los pasos anteriores.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

A continuación, se muestra un ejemplo de una respuesta recibida cuando el estado de realización es `in_progress`.

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebe174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ]
}

```

```

],
"state": "in_progress",
"failure_message": "The state realization is in progress at transport nodes."
}

```

A continuación, se muestra un ejemplo de una respuesta recibida cuando el estado de realización es `in_sync`.

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ],
  "state": "in_sync"
}

```

Los siguientes son ejemplos de posibles respuestas que aparecen cuando el estado de realización es `unknown`.

```

{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation after some time."
}

```

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable to get response from the node. Please retry operation after some time."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",
      "state": "in_sync"
    }
  ],
  "state": "unknown",
  "failure_message": "The state realization is unknown at transport nodes"
}

```


Después de realizar una operación `DELETE` de una entidad, podría recibir el estado `NOT_FOUND`, tal como se muestra en el ejemplo siguiente.

```
{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}
```

Si el servicio de VPN de IPsec asociado a la sesión está deshabilitado, recibirá como respuesta `BAD_REQUEST`, como se muestra en el ejemplo siguiente.

```
{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization status."
}
```

Supervisar y solucionar problemas de sesiones de VPN

Después de configurar una sesión de IPsec o de VPN de Capa 2, puede supervisar el estado del túnel de VPN y solucionar cualquier problema con el túnel que se haya informado mediante la interfaz de usuario de NSX Manager.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta la pestaña **Redes > VPN > Sesiones de IPsec** o **Redes > VPN > Sesiones de VPN de capa 2**.
- 3 Expanda la fila de la sesión de VPN que desea supervisar o cuyos problemas va a solucionar.
- 4 Para ver el estado del túnel de VPN, haga clic en el icono de información.

Aparecerá el cuadro de diálogo Estado, que muestra los estados disponibles.

- 5 Para ver las estadísticas de tráfico del túnel de VPN, haga clic en **Ver estadísticas** en la columna Estado.

El cuadro de diálogo Estadísticas muestra las estadísticas de tráfico correspondientes al túnel de VPN.

- 6 Para ver las estadísticas de errores, haga clic en el vínculo **Más** en el cuadro de diálogo Estadísticas.
- 7 Para cerrar el cuadro de diálogo **Estadísticas**, haga clic en **Cerrar**.

Traducción de direcciones de red

6

La traducción de direcciones de red (NAT) asigna un espacio de direcciones IP con otro. Puede configurar la NAT en puertas de enlace de nivel 0 y nivel 1.

Este capítulo incluye los siguientes temas:

- [Configurar NAT en una puerta de enlace](#)

Configurar NAT en una puerta de enlace

Puede configurar una NAT de origen (Source NAT, SNAT), una NAT de destino (Destination NAT, DNAT) o una NAT reflexiva en una puerta de enlace de nivel 0 o nivel 1.

Cuando una puerta de enlace de nivel 0 se ejecuta en modo activo-activo, no se pueden configurar la SNAT ni la DNAT, ya que las rutas asimétricas podrían causar problemas. Solo se puede configurar la NAT reflexiva (en ocasiones denominada NAT sin estado). Si una puerta de enlace de nivel 0 se está ejecutando en modo activo-en espera, se pueden configurar la SNAT, la DNAT o la NAT reflexiva.

También se puede deshabilitar SNAT o DNAT para una dirección IP o un rango de direcciones. Si una dirección tiene varias reglas NAT, se aplica la regla con la prioridad más alta.

Nota DNAT no es compatible con una puerta de enlace de nivel 1 donde está configurada la VPN de IPsec basada en directivas.

La SNAT configurada en la interfaz externa de una puerta de enlace de nivel 0 procesará tráfico desde una puerta de enlace de nivel 1, así como desde otra interfaz externa en la puerta de enlace de nivel 0.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > NAT**.
- 3 Seleccione una puerta de enlace.
- 4 Haga clic en **Agregar regla NAT**.

5 Seleccione una acción.

Para una puerta de enlace de nivel 1, las acciones disponibles son **SNAT**, **DNAT**, **Reflexivo**, **No hay SNAT** y **No hay DNAT**.

Para una puerta de enlace de nivel 0 en modo activo-en espera, las acciones disponibles son **SNAT**, **DNAT**, **No hay SNAT** y **No hay DNAT**.

Para una puerta de enlace de nivel 0 en modo activo-activo, la acción disponible es **Reflexiva**.

6 En la columna **Servicio**, haga clic en **Establecer** para seleccionar los servicios.

7 (Requerido) Para **IP de origen**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

Si deja vacío este campo, esta regla NAT se aplicará a todos los orígenes fuera de la subred local.

8 Para **IP de destino**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

9 Para **IP traducida**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

10 Introduzca un valor en **Puerto traducido**.

11 Seleccione una de las siguientes configuraciones de firewall:

- **Hacer coincidir con dirección externa:** el paquete se procesa mediante reglas de firewall que coinciden con la combinación de dirección IP traducida y puerto traducido.
 - Para SNAT, la dirección externa es la dirección de origen traducida después de que se haya realizado la NAT.
 - Para DNAT, la dirección externa es la dirección de destino original antes de que se haya realizado la NAT.
 - Para REFLEXIVE, para el tráfico de salida, el firewall se aplica a la dirección de origen traducida después de que se haya realizado la NAT. Para el tráfico de entrada, el firewall se aplica a la dirección de destino original antes de que se haya realizado la NAT.
- **Hacer coincidir con dirección interna :** el paquete se procesa mediante las reglas de firewall que coinciden con la combinación de dirección IP original y puerto original.
 - Para SNAT, la dirección interna es la dirección de origen original antes de que se haya realizado la NAT.
 - Para DNAT, la dirección interna es la dirección de destino traducida después de que se haya realizado la NAT.
 - Para REFLEXIVE, para el tráfico de salida, el firewall se aplica a la dirección de origen original antes de que se realice la NAT. Para el tráfico de entrada, el firewall se aplica a la dirección de destino traducida después de que se haya realizado la NAT.
- **Omitir:** el paquete omite las reglas de firewall.

12 (Requerido) Cambie el estado de registro.

13 (Requerido) Para la opción **Se aplica a**, seleccione los objetos a los que se aplica esta regla.

Los objetos disponibles son **Puertas de enlace de nivel 0**, **Interfaces**, **Etiquetas**, **Endpoints de instancia de servicio** y **Endpoints virtuales**.

14 Especifique un valor de prioridad.

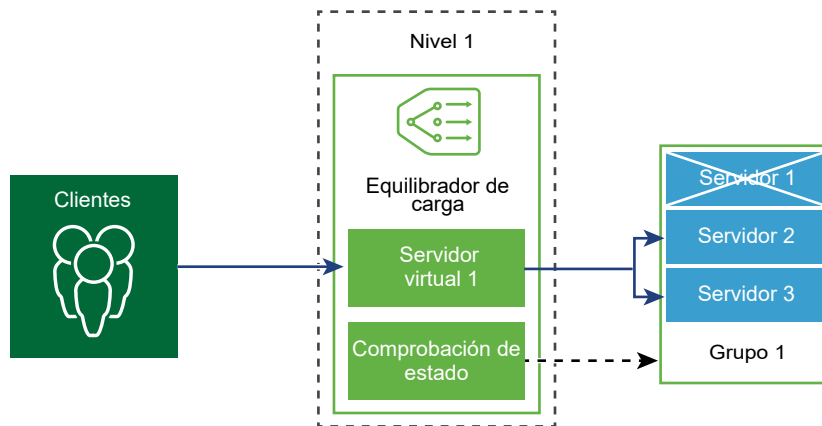
Un valor inferior significa una prioridad más elevada. El valor predeterminado es 100.

15 Haga clic en **Guardar**.

Equilibrio de carga

7

El equilibrador de carga lógico NSX-T Data Center ofrece servicios de alta disponibilidad para aplicaciones y distribuye la carga de tráfico de red entre varios servidores.



El equilibrador de carga distribuye las solicitudes de servicio entrantes de manera uniforme entre varios servidores de forma tal que la distribución de carga sea transparente para los usuarios. El equilibrio de carga ayuda a lograr una utilización de recursos óptima, maximizar la capacidad de proceso, minimizar el tiempo de respuesta y evitar la sobrecarga.

Puede asignar una dirección IP virtual a un conjunto de servidores de grupo para equilibrio de carga. El equilibrador de carga acepta las solicitudes TCP, UDP, HTTP o HTTPS en la dirección IP virtual y decide qué grupo de servidores se va a utilizar.

Según las necesidades de su entorno, puede ampliar el rendimiento del equilibrador de carga mediante el aumento de los servidores virtuales y los miembros del grupo existentes para controlar el tráfico de red intenso.

Nota El equilibrador de carga lógico solo se admite en la puerta de enlace de nivel 1. Por lo tanto, un equilibrador de carga solo puede asociarse a una puerta de enlace de nivel 1.

Este capítulo incluye los siguientes temas:

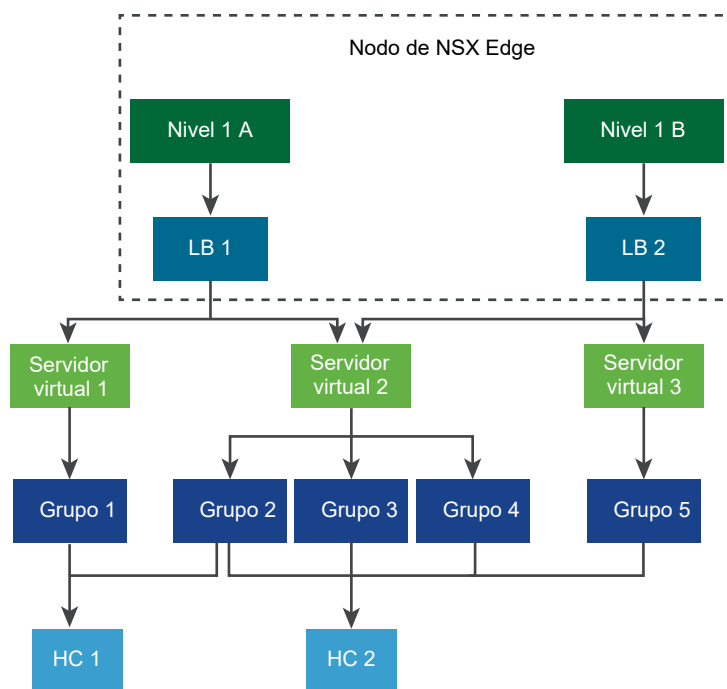
- [Conceptos clave sobre el equilibrador de carga](#)
- [Configurar los componentes del equilibrador de carga](#)
- [Grupos creados para grupos de servidores y servidores virtuales](#)

Conceptos clave sobre el equilibrador de carga

El equilibrador de carga incluye servidores virtuales, grupos de servidores y monitores de comprobación de estado.

Un equilibrador de carga se conecta a un enrutador lógico de nivel 1. El equilibrador de carga aloja uno o varios servidores virtuales. Un servidor virtual es un resumen de un servicio de aplicación, representado por una combinación única de IP, puerto y protocolo. El servidor virtual está asociado a uno o varios grupos de servidores. Un grupo de servidores consta de varios servidores. Los grupos de servidores incluyen miembros de grupo de servidores individuales.

Para determinar si cada servidor ejecuta correctamente la aplicación, puede agregar monitores de comprobación de estado que comprueben el estado de mantenimiento de un servidor.



Ajustar la escala de los recursos del equilibrador de carga

Cuando configure un equilibrador de carga, puede especificar un tamaño (pequeño, mediano o grande). El tamaño determina el número de servidores virtuales, grupos de servidores y miembros de grupo que puede admitir el equilibrador de carga.

Un equilibrador de carga se ejecuta en una puerta de enlace de nivel 1, que debe estar en modo activo-en espera. La puerta de enlace se ejecuta en nodos de NSX Edge. El formato del nodo de NSX Edge (nativo, pequeño, mediano o grande) determina el número de equilibradores de carga que puede admitir el nodo de NSX Edge. Tenga en cuenta que la pestaña **Opciones avanzadas de redes y seguridad**, el término "enrutador lógico" se utiliza para hacer referencia a una puerta de enlace.

Para obtener más información sobre los distintos tamaños de equilibrio de carga y los formatos que admite NSX Edge, consulte <https://configmax.vmware.com>.

Tenga en cuenta que no se recomienda usar un nodo de NSX Edge pequeño para ejecutar un equilibrador de carga pequeño en un entorno de producción.

Puede ejecutar una API para obtener la información de uso del equilibrador de carga de un nodo de NSX Edge. Si utiliza la pestaña **Redes** para configurar el equilibrio de carga, ejecute el siguiente comando:

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

Si utiliza la pestaña **Opciones avanzadas de redes y seguridad** para configurar el equilibrio de carga, ejecute el siguiente comando:

```
GET /api/v1/loadbalancer/usage-per-node/<node-id>
```

La información de uso incluye el número de objetos del equilibrador de carga (como los servicios del equilibrador de carga, los servidores virtuales, los grupos de servidores y los miembros de los grupos) configurados en el nodo. Para obtener más información, consulte la *Guía de la API de NSX-T Data Center*.

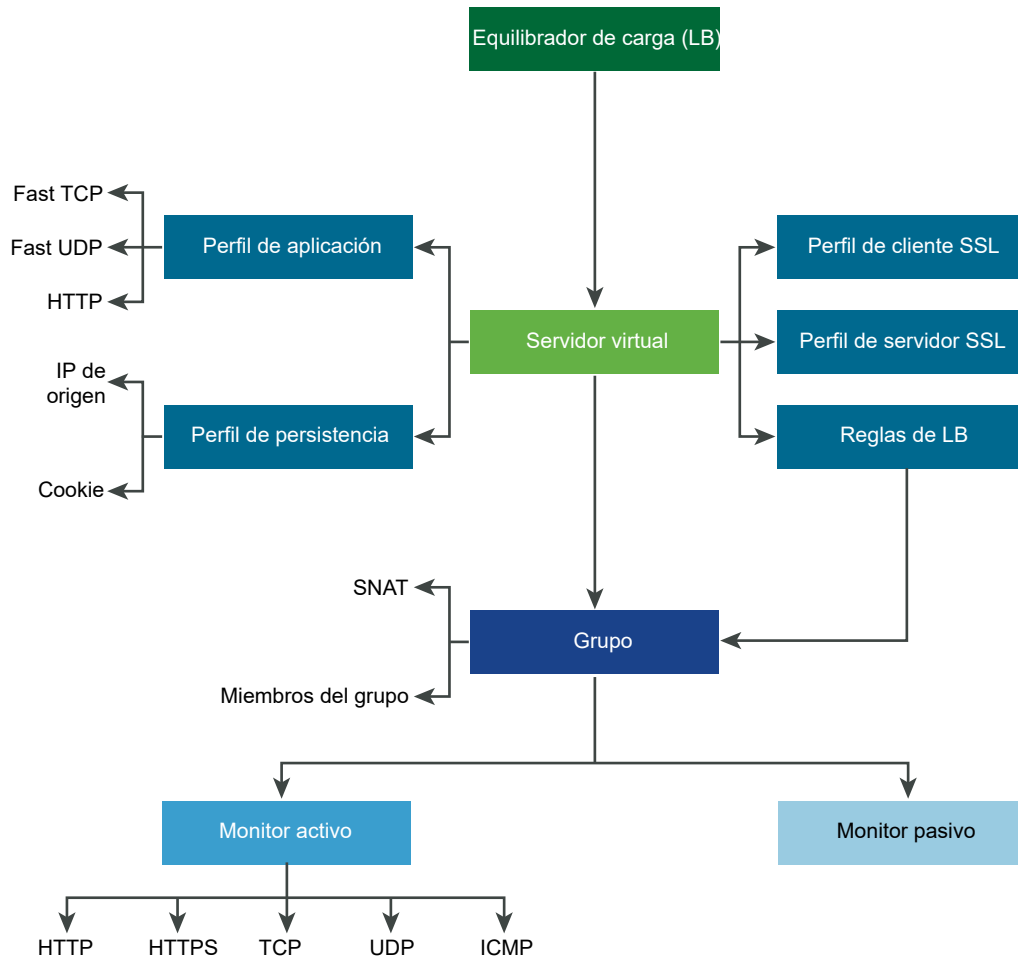
Funciones admitidas del equilibrador de carga

El equilibrador de carga de NSX-T Data Center admite las siguientes funciones.

- Capa 4: TCP y UDP.
- Capa 7: HTTP y HTTPS con compatibilidad con reglas de equilibrador de carga.
- Grupos de servidores: estáticos y dinámicos con NSGroup.
- Persistencia: modo de persistencia de IP de origen y de cookie.
- Monitores de comprobación de estado: un monitor activo que incluye HTTP, HTTPS, TCP, UDP e ICMP, así como un monitor pasivo.
- SNAT: lista de IP, transparente y asignación automática.
- Actualización HTTP: para las aplicaciones que usan la actualización HTTP, como WebSocket, el cliente o el servidor solicitan la actualización de HTTP, que es compatible. De forma predeterminada, NSX-T Data Center admite y acepta la solicitud del cliente de actualización HTTPS con el perfil de aplicación de HTTP.

Para detectar un cliente inactivo o la comunicación del servidor, el equilibrador de carga utiliza la función de tiempo de espera de respuesta del perfil de aplicación de HTTP configurada en 60 segundos. Si el servidor no envía tráfico en un intervalo de 60 segundos, NSX-T Data Center finaliza la conexión en el lado del cliente y el servidor.

Nota: El modo de finalización y el modo de proxy de SSL no se admiten en NSX-T Data Center Limited Export.

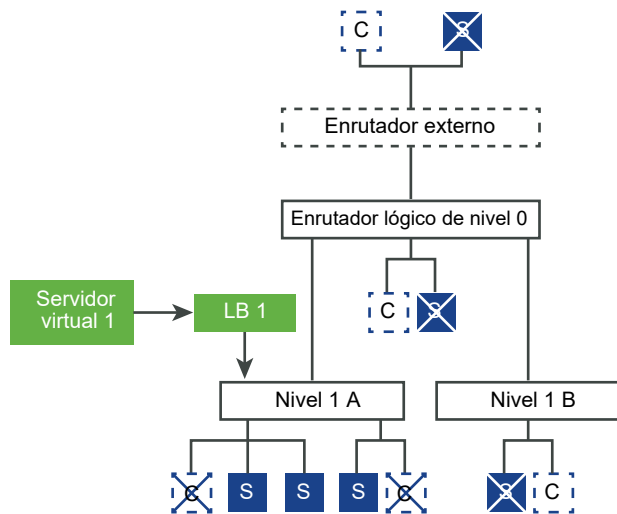


Topologías de equilibrador de carga

Los equilibradores de carga se suelen implementar en el modo en línea o one-arm. El modo one-arm requiere una configuración de NAT de origen (SNAT) de servidor virtual, mientras que el modo Inline no.

Topología en línea

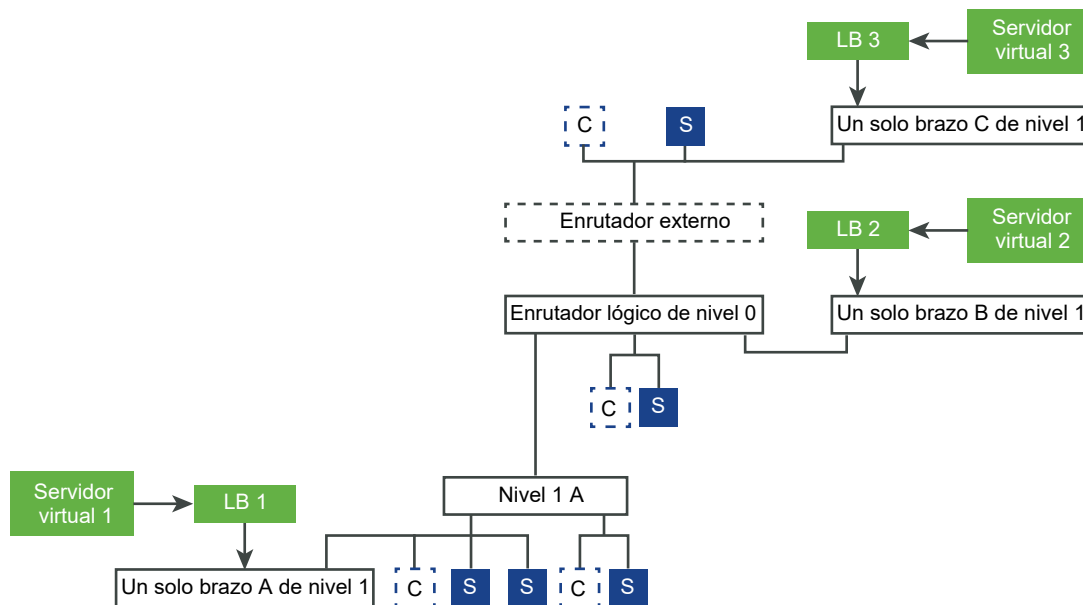
En el modo en línea, el equilibrador de carga se encuentra en la ruta de acceso del tráfico entre el cliente y el servidor. Los clientes y los servidores no deben estar conectados a segmentos superpuestos en el mismo enrutador lógico de nivel 1 si no se desea SNAT en el equilibrador de carga. Si los clientes y los servidores están conectados a segmentos superpuestos en el mismo enrutador lógico de nivel 1, SNAT será necesario.



Topología one-arm

En el modo one-arm, el equilibrador de carga no se encuentra en la ruta de acceso del tráfico entre el cliente y el servidor. En este modo, el cliente y el servidor pueden estar en cualquier lugar. El equilibrador de carga realiza NAT de origen (SNAT) para forzar el tráfico de retorno desde el servidor destinado al cliente para que pase por el equilibrador de carga. Esta topología requiere que SNAT de servidor virtual esté habilitado.

Cuando el equilibrador de carga recibe el tráfico de cliente hacia la dirección IP virtual, selecciona un miembro del grupo de servidores y reenvía a él el tráfico de cliente. En el modo one-arm, el equilibrador de carga reemplaza la dirección IP del cliente por la dirección IP del equilibrador de carga para que siempre se envíe la respuesta del servidor al equilibrador de carga. El equilibrador de carga reenviará la respuesta al cliente.



Encadenamiento de servicios de nivel 1

Si un enrutador lógico o una puerta de enlace de nivel 1 alojan diferentes servicios, como NAT, firewall y equilibrador de carga, los servicios se aplicarán en el siguiente orden:

- Entrada

DNAT - Firewall - Equilibrador de carga

Nota: Si DNAT se configura con Omisión de firewall, se omitirá el firewall, pero no el equilibrador de carga.

- Salida

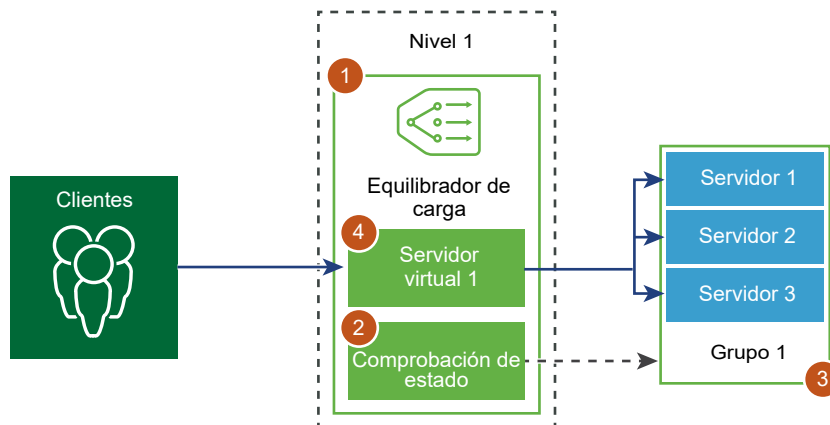
Equilibrador de carga - Firewall - SNAT

Configurar los componentes del equilibrador de carga

Para utilizar equilibradores de carga lógicos, primero debe configurar un equilibrador de carga y asociarlo a una puerta de enlace de nivel 1.

Nota En la pestaña **Opciones avanzadas de redes y seguridad**, el enrutador lógico de nivel 1 del terminal se utiliza para hacer referencia a una puerta de enlace de nivel 1.

A continuación, podrá configurar la supervisión de comprobación de estado para los servidores. Después debe configurar grupos de servidores para el equilibrador de carga. Por último, debe crear un servidor virtual de Capa 4 o Capa 7 para el equilibrador de carga y asociar el servidor que acaba de crear con el equilibrador de carga.



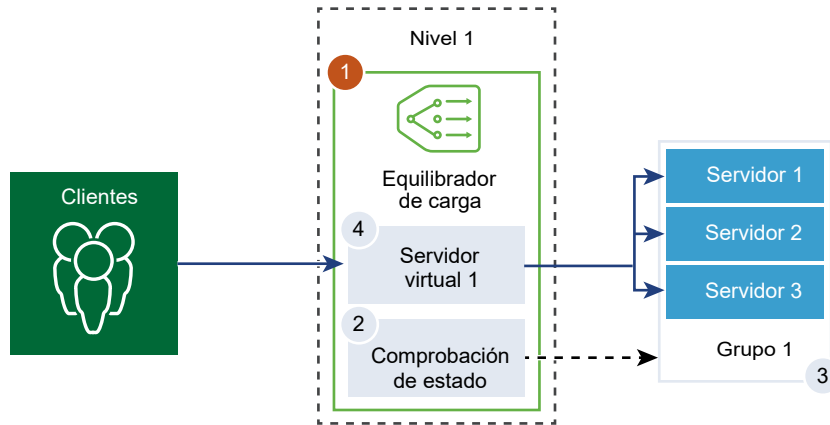
Agregar equilibradores de carga

El equilibrador de carga se crea y se asocia a la puerta de enlace de nivel 1.

Nota En la pestaña **Opciones avanzadas de redes y seguridad**, el enrutador lógico de nivel 1 del terminal se utiliza para hacer referencia a una puerta de enlace de nivel 1.

Puede configurar el nivel de mensajes de error que desea que el equilibrador de carga agregue al registro de errores.

Nota Evite establecer el nivel de registro como **DEPURACIÓN** en los equilibradores de carga con tráfico pesado debido al número de mensajes impresos en el registro que afectan el rendimiento.



Requisitos previos

Compruebe que la puerta de enlace de nivel 1 esté configurada. Consulte [Capítulo 3 Puerta de enlace de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Agregar equilibrador de carga**.
- 3 Introduzca un nombre y una descripción para el equilibrador de carga.
- 4 Seleccione el tamaño del servidor virtual del equilibrador de carga y la cantidad de miembros de grupo en función de los recursos disponibles.
- 5 Seleccione la puerta de enlace de nivel 1 ya configurada para asociar este equilibrador de carga en el menú desplegable.

La puerta de enlace de nivel 1 debe estar en el modo activo-en espera.

- 6 En el menú desplegable, defina el nivel de gravedad del registro de errores.
El equilibrador de carga recopila información sobre problemas de distintos niveles de gravedad detectados en el registro de errores.
- 7 (opcional) Introduzca etiquetas para facilitar la búsqueda.
Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

8 Haga clic en **Guardar**.

Para crear el equilibrador de carga y asociarlo a la puerta de enlace de nivel 1 se requieren aproximadamente tres minutos; el estado de configuración se muestra en verde y activo.

Si el estado es inactivo, haga clic en el icono de información y resuelva el error antes de continuar.

9 (opcional) Elimine el equilibrador de carga.

- a Separe el equilibrador de carga respecto del servidor virtual y la puerta de enlace de nivel 1.
- b Seleccione el equilibrador de carga.
- c Haga clic en el botón de tres puntos verticales.
- d Seleccione **Eliminar**.

Agregar un monitor activo

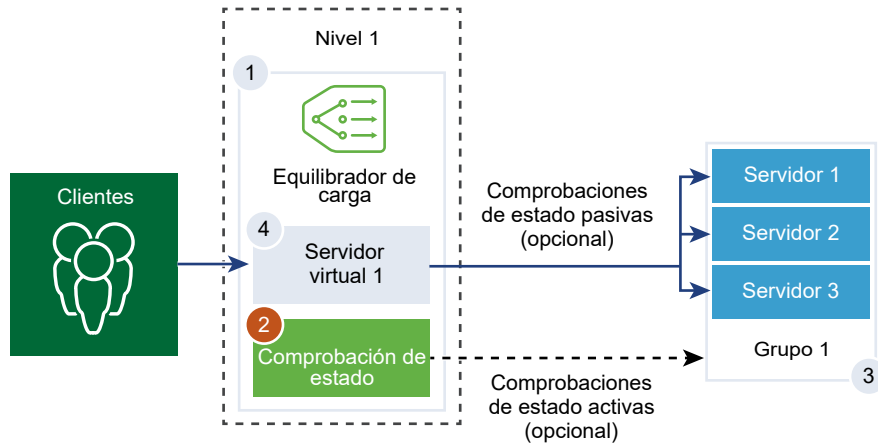
El monitor de estado activo se utiliza para comprobar si un servidor está disponible. El monitor de estado activo utiliza varios tipos de pruebas, como el envío de un ping básico a los servidores o solicitudes HTTP avanzadas para supervisar el estado de una aplicación.

Nota En la pestaña **Opciones avanzadas de redes y seguridad**, el enrutador lógico de nivel 1 del terminal se utiliza para hacer referencia a una puerta de enlace de nivel 1.

Los servidores que no responden en un periodo de tiempo específico o bien responden con errores, se excluyen del posterior manejo de conexiones hasta que una comprobación de estado periódica efectuada más adelante confirma que funcionan correctamente.

Las comprobaciones de estado activas se realizan en miembros de un grupo de servidores después de asociar el miembro del grupo a un servidor virtual y de asociar dicho servidor virtual a una puerta de enlace de nivel 1. La dirección IP de vínculo superior de nivel 1 se utiliza para la comprobación de estado.

Nota Se puede configurar un monitor de estado activo por grupo de servidores.



Procedimiento

1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

2 Seleccione **Redes > Equilibrio de carga > Monitores > Activo > Agregar monitor activo**.

3 En el menú desplegable, seleccione un protocolo para el servidor.

También puede utilizar los protocolos predefinidos; HTTP, HTTPS, ICMP, TCP y UDP para NSX Manager.

4 Seleccione el protocolo **HTTP**.

5 Configure los valores para supervisar un grupo de servicios.

También puede aceptar los valores predeterminados del monitor de estado activo.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el monitor de estado activo.
Puerto de supervisión	Defina el valor del puerto de supervisión.
Intervalo de supervisión	Establezca los segundos que tarda el monitor en enviar otra solicitud de conexión al servidor.
Período de tiempo de espera	Establezca el número de veces que se probará el servidor antes de considerarlo como INACTIVO.
Recuento de errores	Establezca un valor de errores consecutivos a partir del cual el servidor se considere temporalmente no disponible.
Recuento de subida	Establezca un número que indique el periodo de tiempo que se debe esperar para volver a intentar una nueva conexión con el servidor y comprobar si este está disponible.
Etiquetas	Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

Por ejemplo, si el intervalo de supervisión se establece como 5 segundos y el tiempo de espera como 15 segundos, el equilibrador de carga envía solicitudes al servidor cada 5 segundos. En cada sondeo, si la respuesta esperada se recibe del servidor en un plazo de 15 segundos, el resultado de la comprobación de estado será CORRECTO. En caso contrario, el resultado será CRÍTICO. Si los resultados de las tres comprobaciones de estado recientes indican ACTIVO, el servidor se considera ACTIVO.

6 Haga clic en **Configurar**.

7 Introduzca los detalles de configuración de la solicitud y la respuesta HTTP.

Opción	Descripción
Método HTTP	Seleccione el método para detectar el estado del servidor en el menú desplegable: GET, OPTIONS, POST, HEAD y PUT.
URL de solicitud HTTP	Introduzca el URI de la solicitud para el método.
Versión de solicitud HTTP	En el menú desplegable, seleccione la versión de solicitud compatible. También puede aceptar la versión predeterminada: HTTP_VERSION_1.
Encabezado de respuesta HTTP	Haga clic en Agregar e introduzca el nombre del encabezado de respuesta HTTP y el valor correspondiente. El valor de encabezado predeterminado es 4000. El valor de encabezado máximo es 64.000.
Cuerpo de solicitud HTTP	Introduzca el cuerpo de la solicitud. Válido para los métodos POST y PUT.
Código de respuesta HTTP	Introduzca la cadena de la cual el monitor espera encontrar una coincidencia en la línea de estado del cuerpo de la respuesta HTTP. El código de respuesta es una lista separada por comas. Por ejemplo, 200, 301, 302, 401.
Cuerpo de respuesta HTTP	Si la cadena del cuerpo de respuesta HTTP y el cuerpo de la respuesta de la comprobación de estado HTTP coinciden, se considerará que el servidor funciona correctamente.

8 Seleccione el protocolo **HTTPS**.

9 Complete el paso 5.

10 Haga clic en **Configurar**.

11 Introduzca los detalles de configuración de SSL, y la respuesta y la solicitud HTTP.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el monitor de estado activo.
Método HTTP	Seleccione el método para detectar el estado del servidor en el menú desplegable: GET, OPTIONS, POST, HEAD y PUT.
URL de solicitud HTTP	Introduzca el URI de la solicitud para el método.
Versión de solicitud HTTP	En el menú desplegable, seleccione la versión de solicitud compatible. También puede aceptar la versión predeterminada: HTTP_VERSION_1.

Opción	Descripción
Encabezado de respuesta HTTP	Haga clic en Agregar e introduzca el nombre del encabezado de respuesta HTTP y el valor correspondiente. El valor de encabezado predeterminado es 4000. El valor de encabezado máximo es 64.000.
Cuerpo de solicitud HTTP	Introduzca el cuerpo de la solicitud. Válido para los métodos POST y PUT.
Código de respuesta HTTP	Introduzca la cadena de la cual el monitor espera encontrar una coincidencia en la línea de estado del cuerpo de la respuesta HTTP. El código de respuesta es una lista separada por comas. Por ejemplo, 200, 301, 302, 401.
Cuerpo de respuesta HTTP	Si la cadena del cuerpo de respuesta HTTP y el cuerpo de la respuesta de la comprobación de estado HTTP coinciden, se considerará que el servidor funciona correctamente.
SSL de servidor	Alterne el botón para habilitar el servidor SSL.
Certificado de cliente	(Opcional) Seleccione un certificado en el menú desplegable que se utilizará si el servidor no alojar varios nombres de host en la misma dirección IP, o si el cliente no es compatible con una extensión SNI.
Perfil SSL de servidor	(Opcional) Asigne un perfil SSL predeterminado del menú desplegable que defina las propiedades SSL reutilizables del lado cliente e independiente de la aplicación. Haga clic en los puntos suspensivos verticales y cree un perfil de SSL personalizado.
Certificados de CA de confianza	(Opcional) Puede requerir que el cliente tenga un certificado de CA para la autenticación.
Autenticación del servidor obligatoria	(Opcional) Alterne el botón para habilitar la autenticación de servidor.
Profundidad de cadena de certificados	(Opcional) Establezca la profundidad de autenticación de la cadena de certificados del cliente.
Lista de revocación de certificados	(Opcional) Establezca una lista de revocación de certificados (CRL) en el perfil SSL del lado cliente para rechazar los certificados de cliente en riesgo.

12 Seleccione el protocolo **ICMP**.

13 Complete el paso 5 y asigne el tamaño de los datos en bytes del paquete de comprobación de estado ICMP.

14 Seleccione el protocolo **TCP**.

15 Complete el paso 5; puede dejar los parámetros de datos TCP en blanco.

Si no se muestran los datos enviados y los esperados, se establece una conexión TCP de protocolo de enlace triple para validar el estado del servidor. No se enviarán datos.

Los datos esperados, si se enumeran, deben ser una cadena. No se admiten expresiones regulares.

16 Seleccione el protocolo **UDP**.

17 Complete el paso 5 y configure los datos de UDP.

Opción obligatoria	Descripción
Datos de UDP enviados	Introduzca la cadena que se enviará al servidor después de establecer una conexión.
Datos de UDP esperados	Introduzca la cadena que se espera recibir del servidor. El servidor solo se considerará ACTIVO si la cadena recibida coincide con esta definición.

Pasos siguientes

Asocie el monitor de estado activo a un grupo de servidores. Consulte [Agregar un grupo de servidores](#).

Agregar un monitor pasivo

Los equilibradores de carga realizan comprobaciones de estado pasivas para supervisar errores durante las conexiones de cliente y marcar los servidores que generan errores constantes y muestran el estado INACTIVO.

La comprobación de estado pasiva supervisa el tráfico de cliente que pasa a través del equilibrador de carga para ver si tiene errores. Por ejemplo, si un miembro del grupo envía un restablecimiento (Reset, RST) de TCP en respuesta a una conexión de cliente, el equilibrador de carga detecta dicho error. Si se producen varios errores consecutivos, el equilibrador de carga considera que ese miembro del grupo de servidores no está disponible temporalmente y deja de enviarle solicitudes de conexión durante un tiempo. Después de cierto tiempo, el equilibrador de carga envía una solicitud de conexión para comprobar si el miembro del grupo se recuperó. Si esa conexión es correcta, el miembro del grupo se considera en buen estado. De lo contrario, el equilibrador de carga espera un momento y vuelve a intentarlo.

La comprobación de estado pasiva considera los siguientes escenarios como errores en el tráfico de cliente.

- En el caso de los grupos de servidores asociados con servidores virtuales de capa 7, si se produce un error en la conexión con el miembro del grupo. Por ejemplo, si se produce un error cuando el miembro del grupo envía un TCP RST en el momento en que el equilibrador de carga intenta conectarse o establecer un protocolo de enlace SSL entre el equilibrador de carga y el miembro del grupo.
- En el caso de los grupos de servidores asociados con servidores virtuales de TCP de capa 4, si el miembro del grupo envía un TCP RST en respuesta al TCP SYN de cliente o no responde.
- En el caso de los grupos de servidores asociados con servidores virtuales de UDP de capa 4, si se recibe un mensaje de error ICMP que indica que no se puede acceder a un puerto o a un destino en respuesta a un paquete UDP de cliente.

En los grupos de servidores asociados a servidores virtuales de capa 7, el número de errores en la conexión se incrementa cuando se producen errores de conexión de TCP; por ejemplo, se producen errores de TCP RST para el envío de datos o errores de protocolo de enlace SSL.

En los grupos de servidores asociados con servidores virtuales de capa 4, si no se recibe ninguna respuesta a un TCP SYN enviado al miembro del grupo de servidores o si se recibe un TCP RST en respuesta a un TCP SYN, el miembro del grupo de servidores se considera como INACTIVO. Se incrementa el número de errores.

En el caso de los servidores virtuales de UDP de Capa 4, si se recibe un mensaje de error de ICMP (por ejemplo, un mensaje que indica que no es posible acceder al puerto o al destino) en respuesta al tráfico de cliente, se considera INACTIVO.

Nota Puede configurar un monitor de estado pasivo por grupo de servidores.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Monitores > Pasivo > Agregar monitor pasivo**.
- 3 Introduzca un nombre y una descripción para el monitor de estado pasivo.
- 4 Configure los valores para supervisar un grupo de servicios.

También puede aceptar los valores predeterminados del monitor de estado activo.

Opción	Descripción
Recuento de errores	Establezca un valor de errores consecutivos a partir del cual el servidor se considere temporalmente no disponible.
Período de tiempo de espera	Establezca el número de veces que se probará el servidor antes de considerarlo como INACTIVO.
Etiquetas	Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

Por ejemplo, cuando los errores consecutivos alcanzan el valor configurado 5, ese miembro se considera como no disponible temporalmente durante 5 segundos. Tras este período, el miembro se volverá a probar con una nueva conexión para ver si está disponible. Si esa conexión es correcta, se considera que el miembro está disponible y el número de errores se establece en cero. Sin embargo, si se produce un error de conexión, el miembro no se utiliza durante otro intervalo de tiempo de espera de 5 segundos.

Pasos siguientes

Asocie el monitor de estado pasivo con un grupo de servidores. Consulte [Agregar un grupo de servidores](#).

Agregar un grupo de servidores

Un grupo de servidores se compone de uno o varios servidores configurados que ejecutan la misma aplicación. Un solo grupo puede asociarse a servidores virtuales de capa 4 y capa 7.

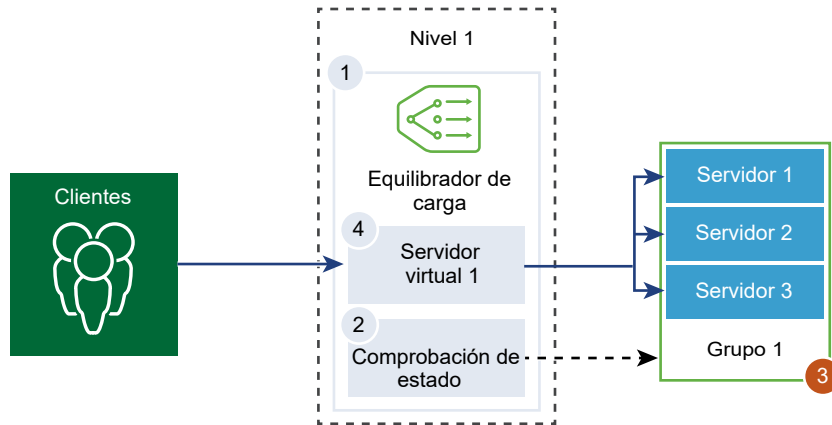
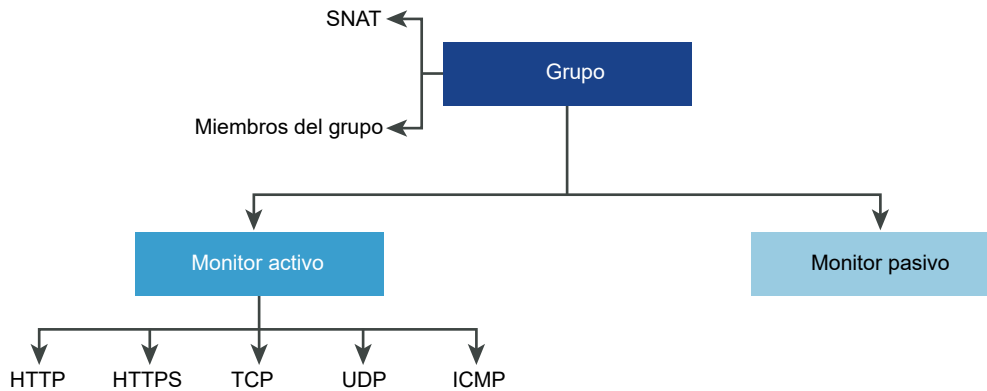


Figura 7-1. Configuración de los parámetros de grupo de servidores



Requisitos previos

- Si usa miembros de grupo dinámico, debe configurar un grupo NSGroup. Consulte [Crear un grupo NSGroup](#).
- Compruebe que hay un monitor de estado pasivo configurado. Consulte [Agregar un monitor pasivo](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Grupos de servidores > Agregar grupo de servidores**.
- 3 Escriba un nombre y una descripción para el grupo de servidores de equilibradores de carga. Opcionalmente, describa las conexiones que administra el grupo de servidores.

4 Seleccione el método de equilibrio de algoritmos del grupo de servidores.

El algoritmo de equilibrio de carga controla la manera en la que se distribuyen las conexiones entrantes entre los miembros. El algoritmo puede utilizarse en un grupo de servidores o directamente en un servidor.

Todos los algoritmos de equilibrio de carga omiten los servidores que cumplen con alguna de las siguientes condiciones:

- El estado de administrador está establecido como DESHABILITADO.
- El estado de administrador está establecido como DESHABILITADO_ESTABLE y no hay ninguna entrada de persistencia coincidente.
- El estado de la comprobación de estado activa o pasiva es INACTIVO.
- Se alcanzó el máximo de conexiones simultáneas del grupo de servidores.

Opción	Descripción
ROUND_ROBIN	Las solicitudes de clientes entrantes pasan por una lista de servidores disponibles capaces de gestionar la solicitud. Ignora la ponderación de los miembros del grupo de servidores, aunque se haya configurado.
WEIGHTED_ROUND_ROBIN	A cada servidor se le asigna un valor de ponderación que indica el rendimiento de ese servidor en relación con los demás servidores del grupo. El valor determina cuántas solicitudes de clientes se envían a un servidor en comparación con otros servidores del grupo. Este algoritmo de equilibrio de carga se centra en distribuir de forma equitativa la carga entre los recursos del servidor disponibles.
LEAST_CONNECTION	Se distribuyen las solicitudes de los clientes entre varios servidores según la cantidad de conexiones existentes en el servidor. Las conexiones nuevas se envían al servidor con menos conexiones. Ignora la ponderación de los miembros del grupo de servidores, aunque se haya configurado.
WEIGHTED_LEAST_CONNECTION	A cada servidor se le asigna un valor de ponderación que indica el rendimiento de ese servidor en relación con los demás servidores del grupo. El valor determina cuántas solicitudes de clientes se envían a un servidor en comparación con otros servidores del grupo. Este algoritmo de equilibrio de carga se centra en utilizar el valor de ponderación para distribuir la carga entre los recursos disponibles del servidor. De forma predeterminada, el valor de ponderación es 1 si no está configurado y si el inicio lento está habilitado.
IP-HASH	Selecciona un servidor según un hash de la dirección IP de origen y el peso total de los servidores en ejecución.

5 Seleccione los miembros del grupo de servidores.

Un grupo de servidores consta de uno o varios miembros del grupo.

Opción	Descripción
Introduzca miembros individuales	<p>Introduzca la dirección IP, un puerto y el nombre de un miembro del grupo.</p> <p>Cada miembro del grupo de servidores se puede configurar con una ponderación para usarla en el algoritmo de equilibrio de carga. La ponderación indica la cantidad de carga aproximada que puede gestionar un determinado miembro del grupo en relación con otros miembros del mismo grupo.</p> <p>Puede establecer el estado de administrador del grupo de servidores. De forma predeterminada, la opción se habilita cuando se agrega un miembro del grupo de servidores.</p> <p>Si la opción está deshabilitada, se procesan las conexiones activas y no se selecciona el miembro del grupo de servidores para las nuevas conexiones. Las conexiones nuevas se asignan a otros miembros del grupo.</p> <p>Si se deshabilita correctamente, le permite quitar servidores para realizar labores de mantenimiento. Se siguen procesando las conexiones existentes con un miembro del grupo de servidores en este estado.</p> <p>Active el botón para definir un miembro del grupo como miembro de copia de seguridad con el fin de que colabore con el monitor de estado para proporcionar un estado Activo-en espera. Se produce una conmutación por error en el tráfico para los miembros de respaldo si los miembros activos fallan en una comprobación de estado. Los miembros de copia de seguridad se omiten durante la selección del servidor. Cuando el grupo de servidores está inactivo, las conexiones entrantes se envían únicamente a los miembros de copia de seguridad que están configurados con una página de disculpa que indica que una aplicación no está disponible.</p> <p>El valor máximo de conexiones simultáneas asigna un número máximo de conexiones para que los miembros del grupo de servidores no se sobrecarguen y se omitan durante la selección del servidor. Si no se especifica un valor, no habrá un límite de conexiones.</p>
Seleccionar un grupo	<p>Seleccione un grupo preconfigurado de miembros del grupo de servidores. Escriba un nombre de grupo y una descripción opcional.</p> <p>Establezca el miembro de equipo de una lista que ya exista o cree una nueva. Puede especificar los criterios de pertenencia, seleccionar los miembros del grupo, agregar direcciones IP y MAC como miembros del grupo, y agregar grupos de Active Directory. Los miembros de identidad se cruzan con el miembro de equipo para definir la pertenencia del grupo.</p> <p>Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p> <p>De forma opcional, puede definir la lista del máximo de direcciones IP del grupo.</p>

6 Seleccione el monitor de comprobación de estado activo para el grupo de servidores del menú desplegable.

El equilibrador de carga envía periódicamente un ping de ICMP a los servidores para comprobar el estado independientemente del tráfico de datos. Puede configurar solo un monitor de comprobación de estado activo por grupo de servidores.

7 Seleccione el modo de traducción de NAT de origen (Source NAT, SNAT).

En función de la topología, SNAT podría ser necesario para que el equilibrador de carga reciba el tráfico del servidor destinado al cliente. SNAT se puede habilitar por grupo de servidores.

Modo	Descripción
Modo de asignación automática	<p>El equilibrador de carga utiliza el puerto efímero y la dirección IP de interfaz para continuar la comunicación con un cliente que inicialmente estaba conectado a uno de los puertos de escucha establecidos del servidor. Se necesita SNAT.</p> <p>Habilite la sobrecarga de puertos para permitir que la misma IP y el mismo puerto de SNAT se utilicen para varias conexiones si la tupla (IP de origen, puerto de origen, IP de destino, puerto de destino y protocolo IP) es exclusiva después de realizar el proceso de SNAT.</p> <p>También puede establecer el factor de sobrecarga de puertos para admitir el número máximo de veces que se puede utilizar un puerto de forma simultánea para varias conexiones.</p>
Deshabilitar	Deshabilite el modo de traducción de SNAT.
Grupo de direcciones IP	<p>Especifique un único rango de direcciones IP (por ejemplo, 1.1.1.1-1.1.1.10) que se utilizará para SNAT al conectarse a cualquiera de los servidores del grupo. De forma predeterminada, se utiliza el rango de puertos de 4000 a 64000 para todas las direcciones IP de SNAT configuradas. Los rangos de puertos de 1000 a 4000 están reservados para fines como las comprobaciones de estado y las conexiones iniciadas desde aplicaciones de Linux. Si existen varias direcciones IP, se seleccionarán mediante Round Robin.</p> <p>Habilite la sobrecarga de puertos para permitir que la misma IP y el mismo puerto de SNAT se utilicen para varias conexiones si la tupla (IP de origen, puerto de origen, IP de destino, puerto de destino y protocolo IP) es exclusiva después de realizar el proceso de SNAT.</p> <p>También puede establecer el factor de sobrecarga de puertos para admitir el número máximo de veces que se puede utilizar un puerto de forma simultánea para varias conexiones.</p>

8 Active el botón para habilitar la multiplexación de TCP.

Con la multiplexación de TCP, es posible utilizar la misma conexión de TCP entre un equilibrador de carga y el servidor para enviar varias solicitudes de clientes de diferentes conexiones de TCP de clientes.

9 Establezca el número máximo de conexiones de multiplexación de TCP por grupo que se mantienen activas para enviar posteriores solicitudes de clientes.

10 Introduzca la cantidad mínima de miembros activos que siempre debe mantener el grupo de servidores.

11 Seleccione un monitor de estado pasivo para el grupo de servidores del menú desplegable.

12 Introduzca etiquetas para facilitar la búsqueda.

Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

Configurar los componentes del servidor virtual

Puede configurar servidores virtuales de Capa 4 y Capa 7 y varios componentes del servidor virtual, como perfiles de aplicación, perfiles persistentes y reglas de equilibrador de carga.

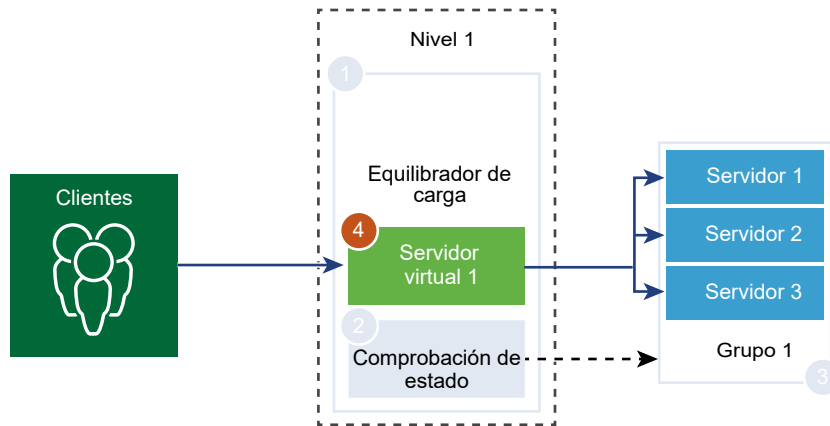
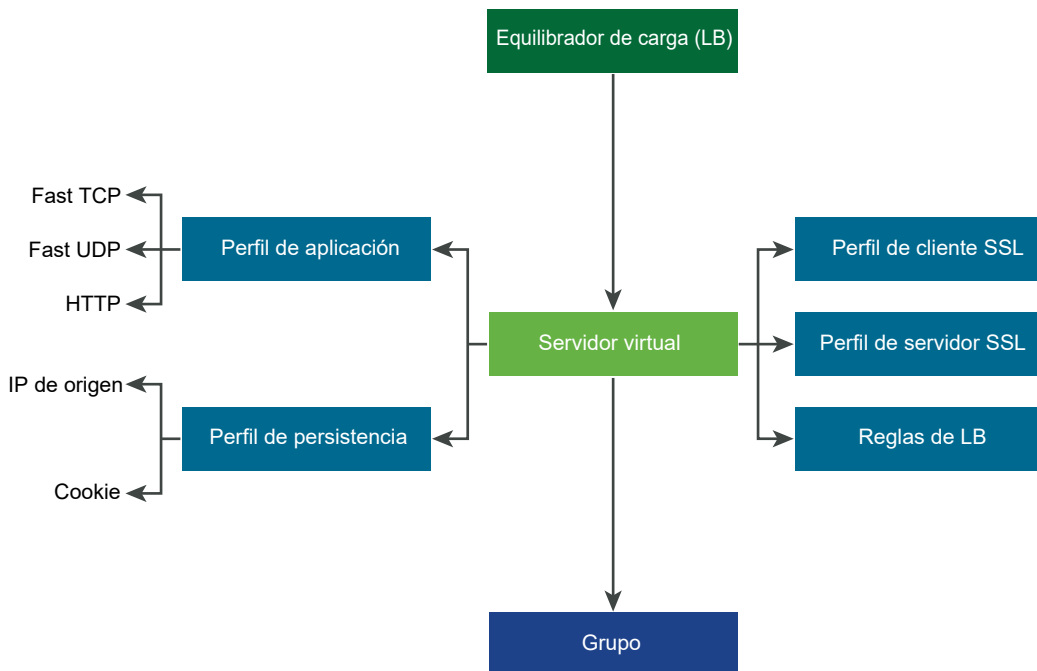


Figura 7-2. Componentes de servidor virtual



Agregar un perfil de aplicación

Los perfiles de aplicaciones se asocian con los servidores virtuales para mejorar el tráfico de red de equilibrio de carga y simplificar las tareas de administración de tráfico.

Los perfiles de aplicaciones definen el comportamiento de un tipo determinado de tráfico de red. El servidor virtual asociado procesa el tráfico de red según los valores especificados en el perfil de aplicación. Los tipos de perfiles de aplicaciones compatibles son FAST TCP, FAST UDP y HTTP.

El perfil de aplicación TCP se utiliza de forma predeterminada cuando no hay ningún perfil de aplicación asociado a un servidor virtual. Los perfiles de aplicaciones TCP y UDP se usan cuando una aplicación está en ejecución en un protocolo TCP o UDP y no requiere un equilibrio de carga de nivel de aplicación, como equilibrio de carga de dirección URL o HTTP. Estos perfiles también se utilizan cuando solo desea el equilibrio de carga de capa 4, que tiene un rendimiento más rápido y es compatible con la creación de reflejo de conexión.

El perfil de aplicación HTTP se utiliza para las aplicaciones HTTP y HTTPS cuando el equilibrador de carga debe realizar acciones en función de la capa 7, como equilibrar la carga de todas las solicitudes de imágenes con un miembro específico del grupo de servidores o detener HTTPS para descargar SSL de los miembros del grupo. A diferencia del perfil de aplicación TCP, el perfil de aplicación HTTP detiene la conexión TCP de cliente antes de seleccionar el miembro del grupo de servidores.

Figura 7-3. Perfiles de aplicaciones TCP y UDP de capa 4

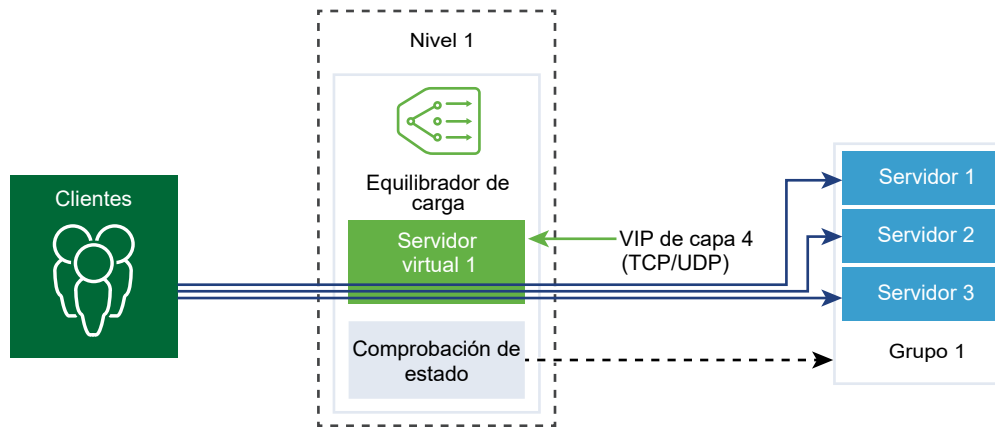
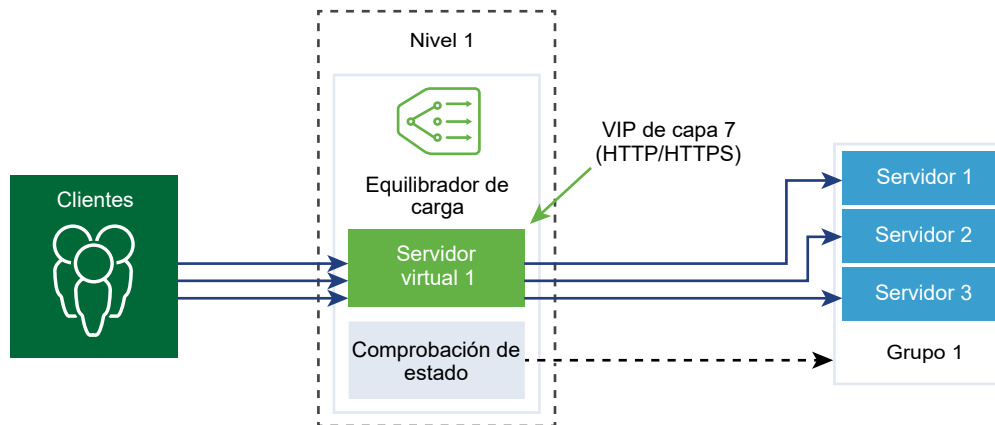


Figura 7-4. Perfil de aplicación HTTPS de capa 7



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

- 2 Seleccione **Redes > Equilibrio de carga > Perfiles > Aplicación > Agregar perfiles de aplicaciones**.

- 3 Seleccione un perfil de aplicación **TCP rápido** e introduzca los detalles del perfil.

También puede aceptar la configuración predeterminada del perfil FAST TCP.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil de aplicación FAST TCP.
Tiempo de espera de inactividad	Introduzca, en segundos, el tiempo que el servidor puede estar inactivo después de que se establece una conexión TCP. El tiempo de inactividad debe ser el tiempo real de inactividad de la aplicación, con algunos segundos más para que el equilibrador de carga no cierre sus conexiones antes que la aplicación.
Creación de reflejo de flujo de HA	Active el botón para que todos los flujos al servidor virtual asociado reflejen el nodo de espera de HA.
Tiempo de espera de cierre de la conexión	Introduzca, en segundos, el tiempo que la conexión TCP FIN o RST se debe mantener para una aplicación antes de cerrar la conexión. Se podría necesitar un tiempo de espera corto para el cierre, de modo que se puedan admitir velocidades de conexión rápidas.
Etiquetas	Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

- 4 Seleccione un perfil de aplicación **UDP rápido** e introduzca los detalles del perfil.

También puede aceptar la configuración predeterminada del perfil UDP.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil de aplicación FAST UDP.
Tiempo de espera de inactividad	Introduzca, en segundos, el tiempo que el servidor puede estar inactivo después de que se establece una conexión UDP. UDP es un protocolo sin conexión. Para equilibrar la carga, se considera que todos los paquetes UDP con la misma firma de flujo, como la dirección IP de origen y la de destino o los puertos y el protocolo IP recibidos dentro del mismo período de tiempo de espera de inactividad, pertenecen a la misma conexión y se envían al mismo servidor. Si no se reciben paquetes durante el período de tiempo de espera de inactividad, se cierra la conexión que se encuentra en una asociación entre la firma de flujo y el servidor seleccionado.
Creación de reflejo de flujo de HA	Active el botón para que todos los flujos al servidor virtual asociado reflejen el nodo de espera de HA.
Etiquetas	Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

- 5 Seleccione un perfil de aplicación **HTTP** e introduzca los detalles del perfil.

También puede aceptar la configuración predeterminada del perfil HTTP.

El perfil de aplicación HTTP se utiliza para las aplicaciones HTTP y HTTPS.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil de aplicación HTTP.
Tiempo de espera de inactividad	Introduzca, en segundos, el tiempo que una aplicación HTTP puede permanecer inactiva, en lugar de la opción de socket TCP que debe estar configurada en el perfil de aplicación TCP.
Tamaño del encabezado de solicitud	Especifique, en bytes, el tamaño máximo de búfer que se utiliza para almacenar los encabezados de solicitud HTTP.
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ Insertar: si el encabezado HTTP XFF no está presente en la solicitud entrante, el equilibrador de carga inserta un encabezado XFF nuevo con la dirección IP del cliente. Si el encabezado HTTP XFF está presente en la solicitud entrante, el equilibrador de carga anexa el encabezado XFF a la dirección IP del cliente. ■ Reemplazar: si el encabezado HTTP XFF está presente en la solicitud entrante, el equilibrador de carga lo reemplaza. <p>Los servidores web registran cada solicitud que controlan con la dirección IP del cliente solicitante. Estos registros se utilizan con fines de depuración y análisis. Si la topología de implementación requiere SNAT en el equilibrador de carga, el servidor utiliza la dirección IP de SNAT del cliente, lo cual va en contra del propósito del registro.</p> <p>Como solución alternativa, puede configurar el equilibrador de carga para insertar el encabezado HTTP XFF con la dirección IP del cliente original. Los servidores pueden configurarse para registrar la dirección IP en el encabezado XFF en lugar de la dirección IP de origen de la conexión.</p>
Tamaño del cuerpo de solicitud	<p>Introduzca el valor del tamaño máximo de búfer utilizado para almacenar el cuerpo de la solicitud HTTP.</p> <p>Si no se especifica este valor, el tamaño del cuerpo de la solicitud será ilimitado.</p>

Opción	Descripción
Redireccionamiento	<ul style="list-style-type: none"> ■ Ninguno: si un sitio web está temporalmente fuera de servicio, el usuario recibe un mensaje de error que indica que no se encontró la página. ■ Redireccionamiento de HTTP: si un sitio web está temporalmente fuera de servicio o se movió, las solicitudes entrantes de ese servidor virtual se pueden redirigir de forma temporal a una URL que se especifique aquí. Solo se admite el redireccionamiento estático. <p>Por ejemplo, si el redireccionamiento de HTTP se establece en <code>http://sitedown.abc.com/sorry.html</code>, independientemente de la solicitud real (por ejemplo, <code>http://original_app.site.com/home.html</code> o <code>http://original_app.site.com/somepage.html</code>), las solicitudes entrantes se redirigen a la URL especificada cuando el sitio web original está fuera de servicio.</p> <ul style="list-style-type: none"> ■ Redireccionamiento de HTTP a HTTPS: es posible que determinadas aplicaciones seguras deseen forzar la comunicación a través de SSL, pero, en lugar de rechazar las conexiones que no son de SSL, pueden redirigir la solicitud del cliente para que use SSL. Con el redireccionamiento de HTTP a HTTPS, puede conservar las rutas de host y URI y redirigir la solicitud del cliente para que use SSL. <p>Para el redireccionamiento de HTTP a HTTPS, el servidor virtual HTTPS debe tener el puerto 443 y se debe configurar la misma dirección IP de servidor virtual en el mismo equilibrador de carga.</p> <p>Por ejemplo, una solicitud de cliente para <code>http://app.com/path/page.html</code> se redirige a <code>https://app.com/path/page.html</code>. Si el nombre de host o el URI deben modificarse durante el redireccionamiento (por ejemplo, redirigir a <code>https://secure.app.com/path/page.html</code>), se deben utilizar reglas de equilibrio de carga.</p>
Autenticación NTLM	<p>Active el botón para que el equilibrador de carga desactive la multiplexación de TCP y habilite HTTP persistente.</p> <p>NTLM es un protocolo de autenticación que puede utilizarse a través de HTTP. Para el equilibrio de carga con autenticación NTLM, se debe deshabilitar la multiplexación de TCP para los grupos de servidores que alojan aplicaciones basadas en NTLM. De lo contrario, una conexión del lado servidor establecida con las credenciales de un cliente puede utilizarse potencialmente para atender las solicitudes de otro cliente.</p> <p>Si NTLM se habilita en el perfil y se asocia a un servidor virtual y la multiplexación de TCP está habilitada en el grupo de servidores, NTLM tiene prioridad. No se realizará la multiplexación de TCP para ese servidor virtual. Sin embargo, si el mismo grupo se asocia a otro servidor virtual que no tiene NTLM, la multiplexación de TCP está disponible para las conexiones a ese servidor virtual.</p> <p>Si el cliente utiliza HTTP/1.0, el equilibrador de carga se actualiza al protocolo HTTP/1.1 y se establece HTTP persistente. Todas las solicitudes HTTP recibidas en la misma conexión TCP del lado cliente se envían al mismo servidor a través de una sola conexión TCP para asegurarse de que no se requiera una nueva autorización.</p>
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>

Agregar un perfil de persistencia

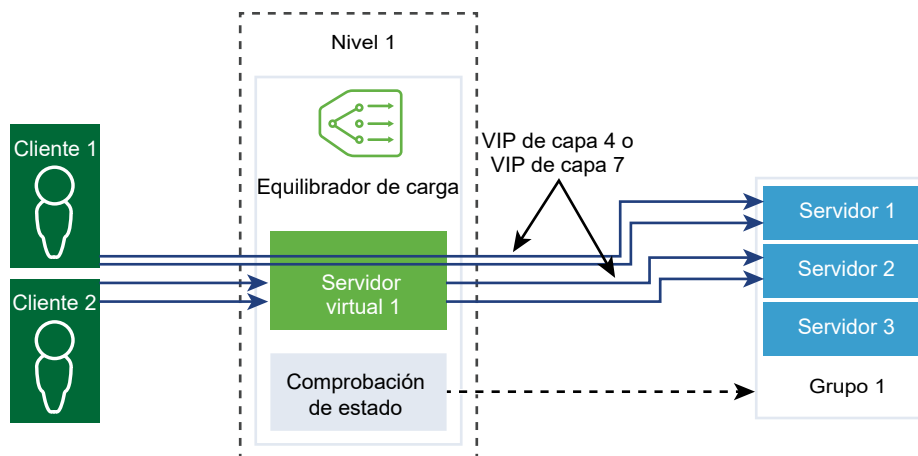
Para garantizar la estabilidad de las aplicaciones con estado, los equilibradores de carga implementan persistencia que dirige todas las conexiones relacionadas al mismo servidor. Se admiten distintos tipos de persistencia para abordar diferentes tipos de necesidades de aplicaciones.

Algunas aplicaciones mantienen el estado del servidor, como los carritos de compra. Dicho estado podría ser por cliente y estar identificado con la dirección IP del cliente, o bien por sesión HTTP. Las aplicaciones pueden acceder a este estado o modificarlo durante el procesamiento de las conexiones relacionadas posteriores desde el mismo cliente o la misma sesión HTTP.

El perfil de persistencia de IP de origen realiza un seguimiento de las sesiones en función de la dirección IP de origen. Cuando un cliente solicita una conexión a un servidor virtual que permite la persistencia de la dirección de origen, el equilibrador de carga comprueba si ese cliente se conectó anteriormente y, si lo hizo, devuelve el cliente al mismo servidor. De lo contrario, puede seleccionar un miembro del grupo de servidores en función del algoritmo de equilibrio de carga del grupo. El perfil de persistencia de IP de origen es utilizado por los servidores virtuales de capa 4 y capa 7.

El perfil de persistencia de cookie inserta una única cookie para identificar la sesión la primera vez que un cliente accede al sitio. El cliente reenvía la cookie HTTP en solicitudes posteriores y el equilibrador de carga utiliza esa información para proporcionar la persistencia de cookie. Los servidores virtuales de capa 7 solo pueden utilizar el perfil de persistencia de cookies. Tenga en cuenta que **no** se admiten espacios en blanco en el nombre de las cookies.

El perfil de persistencia genérico admite la persistencia basada en el encabezado HTTP, la cookie o la URL de la solicitud HTTP. Por lo tanto, admite la persistencia de sesión de aplicación cuando el identificador de la sesión forma parte de la URL. Este perfil no se asocia directamente a un servidor virtual. Puede especificar este perfil cuando configure una regla de equilibrador de carga para el reenvío de solicitudes y la reescritura de respuestas.



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Perfiles > Persistencia > Agregar perfiles de persistencia**.
- 3 Seleccione **IP de origen** para agregar un perfil de persistencia de IP de origen e introduzca los detalles del perfil.

También puede aceptar la configuración predeterminada del perfil de IP de origen.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil de persistencia de IP de origen.
Compartir persistencia	<p>Active el botón para compartir la persistencia de modo que todos los servidores virtuales con los que está asociado este perfil puedan compartir la tabla de persistencia.</p> <p>Si no está habilitada la opción para compartir la persistencia en el perfil de persistencia de IP de origen asociado a un servidor virtual, cada servidor virtual al que el perfil está asociado mantiene una tabla de persistencia privada.</p>
Tiempo de espera de entrada de persistencia	<p>Introduzca el tiempo de caducidad de la persistencia en segundos.</p> <p>La tabla de persistencia del equilibrador de carga mantiene las entradas para registrar que las solicitudes de los clientes se dirigen al mismo servidor.</p> <p>En la primera conexión desde la nueva IP de cliente, se equilibra la carga con un miembro de grupo en función del algoritmo de equilibrio de carga. NSX almacenará esa entrada de persistencia en la tabla de persistencia de LB que se pueda ver en el nodo de Edge que aloja el T1-LB activo a través del comando de la CLI: <code>get load-balancer <LB-UUID> persistence-tables</code>.</p> <ul style="list-style-type: none"> ■ Cuando hay conexiones desde ese cliente a la VIP, se mantiene la entrada de persistencia. ■ Cuando no hay más conexiones desde ese cliente a la VIP, la entrada de persistencia iniciará el recuento de temporizadores especificado en el valor de "Tiempo de espera de entrada de persistencia". Si no se establece una nueva conexión desde ese cliente a la VIP antes de que caduque el temporizador, se eliminará la entrada de persistencia de esa IP de cliente. Si el cliente vuelve a aparecer después de eliminar la entrada, se volverá a equilibrar la carga con un miembro del grupo basado en el algoritmo de equilibrio de carga.
Purgar entradas al llenarse	<p>Un valor de tiempo de espera grande puede hacer que la tabla de persistencia se llene rápidamente si el tráfico es intenso. Cuando esta opción está habilitada, se elimina la entrada más antigua para aceptar la entrada más reciente.</p> <p>Cuando esta opción está deshabilitada, si la tabla de persistencia de IP de origen está llena, se rechazan las nuevas conexiones de cliente.</p>

Opción	Descripción
Creación de reflejo de persistencia de HA	Active el botón para sincronizar entradas de persistencia con el elemento de HA del mismo nivel. Cuando la creación de reflejo de HA está habilitada, la persistencia de la IP del cliente permanece en el caso de la conmutación por error del equilibrador de carga.
Etiquetas	Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.

4 Seleccione un perfil de persistencia **Cookie** e introduzca los detalles del perfil.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil de persistencia de cookie.
Compartir persistencia	Active el botón para compartir la persistencia entre varios servidores virtuales que están asociados a los mismos miembros del grupo. El perfil de persistencia de cookie inserta una cookie con el formato <code><name>.<profile-id>.<pool-id></code> . Si la persistencia compartida no está habilitada en el perfil de persistencia de cookie asociado con un servidor virtual, el miembro del grupo utiliza y completa la persistencia de cookie privada para cada servidor virtual. El equilibrador de carga inserta una cookie con el formato, <code><name>.<virtual_server_id>.<pool_id></code> .
Modo de cookie	Seleccione un modo en el menú desplegable. <ul style="list-style-type: none"> ■ INSERTAR: agrega una cookie exclusiva para identificar la sesión. ■ PREFIJO: se anexa a la información de cookie HTTP existente. ■ REESCRITURA: reescribe la información de cookie HTTP existente.
Nombre de cookie	Introduzca el nombre de la cookie. No se admiten espacios en blanco en el nombre de las cookies.
Dominio de cookie	Introduzca el nombre de dominio. El dominio de la cookie HTTP puede configurarse únicamente en el modo INSERTAR.
Reserva de cookie	Active el botón para que se rechace la solicitud del cliente si la cookie apunta a un servidor que se encuentra en estado DESHABILITADO o INACTIVO. Selecciona un nuevo servidor para controlar una solicitud de cliente si la cookie apunta a un servidor que se encuentra en estado DESHABILITADO o INACTIVO.
Ruta de cookie	Introduzca la ruta de URL de la cookie. La ruta HTTP de la cookie se puede establecer únicamente en el modo INSERTAR.
Cifrado de cookie	Active el botón para deshabilitar el cifrado. Cuando se deshabilita el cifrado, la información de dirección IP de servidor y de puerto de la cookie aparece en texto sin formato. Cifre la información de dirección IP de servidor y la información de puerto de la cookie.

Opción	Descripción
Tipo de cookie	<p>Seleccione el tipo de cookie en el menú desplegable.</p> <p>Cookie de sesión: no almacenada. Se pierde cuando se cierra el navegador.</p> <p>Cookie de persistencia : almacenada por el navegador. No se pierde cuando se cierra el navegador.</p>
Tiempo de inactividad máximo	Introduzca, en segundos, el tiempo que el tipo de cookie puede estar inactivo antes de caducar.
Antigüedad máxima de cookie	Para el tipo de cookie de sesión, introduzca, en segundos, el tiempo que la cookie está disponible.
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>

- 5 Seleccione **Genérico** para agregar un perfil de persistencia genérico e introduzca la información del perfil.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil de persistencia de IP de origen.
Compartir persistencia	Alterne el botón para compartir el perfil entre los servidores virtuales.
Tiempo de espera de entrada de persistencia	<p>Introduzca el tiempo de caducidad de la persistencia en segundos.</p> <p>La tabla de persistencia del equilibrador de carga mantiene las entradas para registrar que las solicitudes de los clientes se dirigen al mismo servidor.</p> <p>En la primera conexión desde la nueva IP de cliente, se equilibra la carga con un miembro de grupo en función del algoritmo de equilibrio de carga. NSX almacenará esa entrada de persistencia en la tabla de persistencia de LB que se pueda ver en el nodo de Edge que aloja el T1-LB activo a través del comando de la CLI: <code>get load-balancer <LB-UUID> persistence-tables</code>.</p> <ul style="list-style-type: none"> ■ Cuando hay conexiones desde ese cliente a la VIP, se mantiene la entrada de persistencia. ■ Cuando no hay más conexiones desde ese cliente a la VIP, la entrada de persistencia iniciará el recuento de temporizadores especificado en el valor de "Tiempo de espera de entrada de persistencia". Si no se establece una nueva conexión desde ese cliente a la VIP antes de que caduque el temporizador, se eliminará la entrada de persistencia de esa IP de cliente. Si el cliente vuelve a aparecer después de eliminar la entrada, se volverá a equilibrar la carga con un miembro del grupo basado en el algoritmo de equilibrio de carga.
Creación de reflejo de persistencia de HA	Active el botón para sincronizar entradas de persistencia con el elemento de HA del mismo nivel.
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>

Agregar un perfil de SSL

Los perfiles SSL configuran las propiedades de SSL independientes de la aplicación, como listas de cifrado, y vuelven a utilizar dichas listas a través de varias aplicaciones. Las propiedades SSL

son diferentes cuando el equilibrador de carga actúa como un cliente y como un servidor; como resultado se admiten perfiles SSL separados para cliente y para servidor.

Nota El perfil de SSL no se admite en la versión NSX-T Data Center Limited Export.

El perfil SSL del lado cliente hace referencia al equilibrador de carga actuando como un servidor SSL y finalizando la conexión SSL de cliente. El perfil SSL del lado servidor hace referencia al equilibrador de carga actuando como un cliente y estableciendo una conexión con el servidor.

Puede especificar una lista de claves de cifrado en los perfiles SSL del lado cliente y del lado servidor.

El almacenamiento en caché de la sesión SSL permite que el cliente SSL y el servidor reutilicen los parámetros de seguridad negociados previamente, lo que evita la costosa operación de clave pública durante el protocolo de enlace SSL. El almacenamiento en caché de la sesión SSL está deshabilitado de forma predeterminada en el lado cliente y el lado servidor.

Los vales de sesión SSL son un mecanismo alternativo que permiten al cliente y al servidor SSL reutilizar los parámetros de sesión negociados previamente. En los vales de sesión SSL, el cliente y el servidor negocian si son compatibles con los vales de sesión SSL durante el intercambio de protocolos de enlace. Si ambos son compatibles, el servidor puede enviar al cliente un vale de SSL, que incluye los parámetros de sesión SSL cifrados. El cliente puede utilizar ese vale en las conexiones posteriores para volver a utilizar la sesión. Los vales de sesión SSL se habilitan en el lado cliente y se deshabilitan en el lado servidor.

Figura 7-5. Descarga de SSL

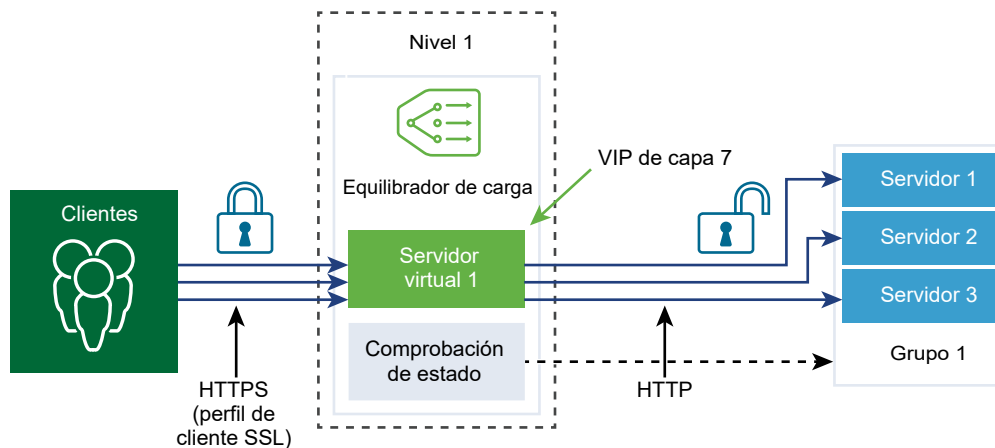
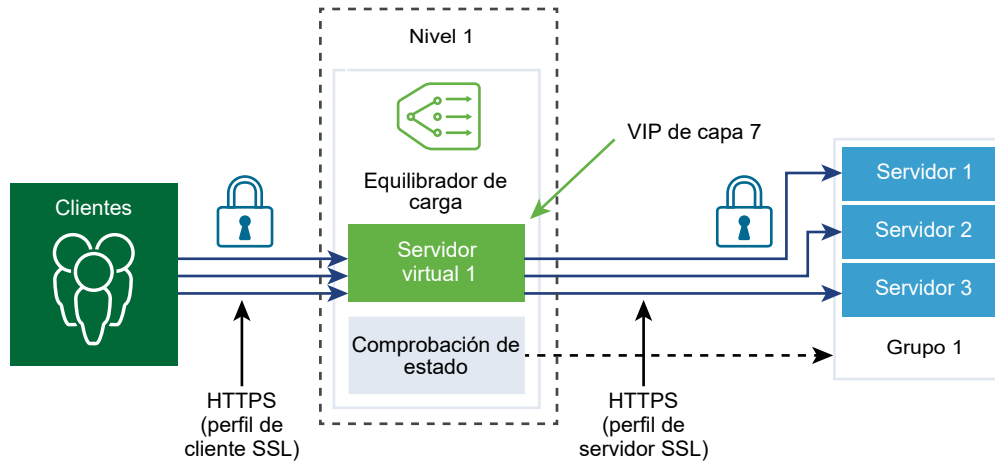


Figura 7-6. SSL de un extremo a otro



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Perfiles > Perfil SSL**.
- 3 Seleccione un **Perfil SSL de cliente** e introduzca los detalles del perfil.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil SSL de cliente.
Conjunto de SSL	<p>Seleccione el grupo de claves de cifrado SSL en el menú desplegable; se rellenan las claves de cifrado SSL y los protocolos SSL que se incluirán en el perfil SSL de cliente.</p> <p>El grupo de claves de cifrado SSL equilibrado es el valor predeterminado.</p>
Almacenamiento en caché de la sesión	Active el botón de alternancia para permitir que el cliente SSL y el servidor reutilicen los parámetros de seguridad negociados previamente; esto evita la costosa operación de clave pública durante un protocolo de enlace SSL.
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>
Claves de cifrado SSL compatibles	<p>Según el conjunto SSL asignado, se rellenan aquí las claves de cifrado SSL admitidas. Haga clic en Ver más para ver toda la lista.</p> <p>Si seleccionó Personalizado, debe seleccionar las claves de cifrado SSL en el menú desplegable.</p>
Protocolos SSL compatibles	<p>Según el conjunto SSL asignado, se rellenan aquí los protocolos SSL admitidos. Haga clic en Ver más para ver toda la lista.</p> <p>Si seleccionó Personalizado, debe seleccionar las claves de cifrado SSL en el menú desplegable.</p>

Opción	Descripción
Tiempo de espera de la entrada de memoria caché de sesión	Introduzca, en segundos, el tiempo de espera de la memoria caché para especificar durante cuánto tiempo se deben mantener y se pueden reutilizar los parámetros de sesión SSL.
Preferir clave de cifrado de servidor	Active el botón para que el servidor pueda seleccionar la primera clave de cifrado compatible de la lista que puede admitir. Durante un protocolo de enlace SSL, el cliente envía al servidor una lista ordenada de las claves de cifrado compatibles.

4 Seleccione un **Servidor de perfil SSL** e introduzca los detalles del perfil.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el perfil SSL de servidor.
Conjunto de SSL	Seleccione el grupo de claves de cifrado SSL en el menú desplegable; se rellenan las claves de cifrado SSL y los protocolos SSL que se incluirán en el perfil SSL de servidor. El grupo de claves de cifrado SSL equilibrado es el valor predeterminado.
Almacenamiento en caché de la sesión	Active el botón de alternancia para permitir que el cliente SSL y el servidor reutilicen los parámetros de seguridad negociados previamente; esto evita la costosa operación de clave pública durante un protocolo de enlace SSL.
Etiquetas	Introduzca etiquetas para facilitar la búsqueda. Puede especificar una etiqueta para establecer un ámbito para la etiqueta.
Claves de cifrado SSL compatibles	Según el conjunto SSL asignado, se rellenan aquí las claves de cifrado SSL admitidas. Haga clic en Ver más para ver toda la lista. Si seleccionó Personalizado , debe seleccionar las claves de cifrado SSL en el menú desplegable.
Protocolos SSL compatibles	Según el conjunto SSL asignado, se rellenan aquí los protocolos SSL admitidos. Haga clic en Ver más para ver toda la lista. Si seleccionó Personalizado , debe seleccionar las claves de cifrado SSL en el menú desplegable.
Tiempo de espera de la entrada de memoria caché de sesión	Introduzca, en segundos, el tiempo de espera de la memoria caché para especificar durante cuánto tiempo se deben mantener y se pueden reutilizar los parámetros de sesión SSL.
Preferir clave de cifrado de servidor	Active el botón para que el servidor pueda seleccionar la primera clave de cifrado compatible de la lista que puede admitir. Durante un protocolo de enlace SSL, el cliente envía al servidor una lista ordenada de las claves de cifrado compatibles.

Agregar servidores virtuales de Capa 4

Los servidores virtuales reciben todas las conexiones de cliente y las distribuyen entre los servidores. Un servidor virtual tiene una dirección IP, un puerto y un protocolo. Para los servidores virtuales de capa 4, se pueden especificar listas de rangos de puertos en lugar de un solo puerto TCP o UDP para admitir protocolos complejos con puertos dinámicos.

Un servidor virtual de capa 4 debe estar asociado a un grupo de servidores principal, también denominado grupo predeterminado.

Si se deshabilita el estado de un servidor virtual, se rechazarán los nuevos intentos de conexión al servidor virtual mediante el envío de un TCP RST para la conexión TCP o un mensaje de error ICMP para UDP. Se rechazarán las nuevas conexiones incluso si hay entradas de persistencia coincidentes para ellas. Se seguirán procesando las conexiones activas. Si un servidor virtual se elimina o desasocia de un equilibrador de carga, las conexiones activas con ese servidor virtual generan un error.

Requisitos previos

- Compruebe que los perfiles de aplicaciones estén disponibles. Consulte [Agregar un perfil de aplicación](#).
- Compruebe que los perfiles persistentes estén disponibles. Consulte [Agregar un perfil de persistencia](#).
- Compruebe que los perfiles de SSL para el cliente y el servidor estén disponibles. Consulte [Agregar un perfil de SSL](#).
- Compruebe que los grupos de servidores estén disponibles. Consulte [Agregar un grupo de servidores](#).
- Compruebe que haya disponible un equilibrador de carga. Consulte [Agregar equilibradores de carga](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Servidores virtuales > Agregar servidor virtual**.
- 3 Seleccione un protocolo **TCP de Capa 4** e introduzca la información del protocolo.

Los servidores virtuales de Capa 4 admiten el protocolo FAST TCP o FAST UDP, pero no ambos.

Para admitir el protocolo FAST TCP o FAST UDP en la misma dirección IP y el mismo puerto, por ejemplo DNS, se debe crear un servidor virtual para cada protocolo.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el servidor virtual de capa 4.
Dirección IP	Introduzca la dirección IP del servidor virtual.
Puertos	Introduzca el número de puerto del servidor virtual.
Equilibrador de carga	Seleccione un equilibrador de carga existente que vaya a asociar a este servidor virtual de Capa 4 en el menú desplegable.

Opción	Descripción
Grupo de servidores	<p>Seleccione un grupo de servidores existente en el menú desplegable.</p> <p>El grupo de servidores consta de uno o varios servidores, también denominados miembros de grupo, que están configurados de manera similar y ejecutan la misma aplicación.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un grupo de servidores.</p>
Perfil de aplicación	<p>En base al tipo de protocolo, se rellenará automáticamente el perfil de aplicación existente.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un perfil de aplicación.</p>
Persistencia	<p>Seleccione un perfil de persistencia existente en el menú desplegable.</p> <p>El perfil de persistencia se puede habilitar en un servidor virtual para permitir que las conexiones de cliente relacionadas con la IP de origen se envíen al mismo servidor.</p>
Máximo de conexiones simultáneas	<p>Establezca la cantidad máxima de conexiones simultáneas permitidas con un servidor virtual de modo que el servidor virtual no consuma recursos de otras aplicaciones alojadas en el mismo equilibrador de carga.</p>
Velocidad máxima de conexión nueva	<p>Establezca el máximo para la nueva conexión con un miembro del grupo de servidores de modo que un servidor virtual no consuma recursos.</p>
Grupo de servidores Sorry	<p>Seleccione un grupo de servidores de respaldo existente en el menú desplegable.</p> <p>El grupo de servidores de respaldo atiende la solicitud cuando un equilibrador de carga no puede seleccionar un servidor de back-end para atender la solicitud del grupo predeterminado.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un grupo de servidores.</p>
Puerto de miembro de grupo predeterminado	<p>Introduzca un puerto de miembro de grupo predeterminado si el puerto de miembro de grupo de un servidor virtual no está definido.</p> <p>Por ejemplo, si se define un servidor virtual con el rango de puertos 2000-2999 y el rango de puertos del miembro de grupo predeterminado se establece en 8000-8999, se envía una conexión de cliente entrante con el puerto de servidor virtual 2500 a un miembro del grupo con un puerto de destino establecido en 8500.</p>
Estado del administrador	<p>Active el botón para deshabilitar el estado de administrador del servidor virtual de Capa 4.</p>
Registro de acceso	<p>Active el botón para habilitar el registro del servidor virtual de Capa 4.</p>
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>

4 Seleccione un protocolo **UDP de Capa 4** e introduzca la información del protocolo.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el servidor virtual de capa 4.
Dirección IP	Introduzca la dirección IP del servidor virtual.
Puertos	Introduzca el número de puerto del servidor virtual.

Opción	Descripción
Equilibrador de carga	Seleccione un equilibrador de carga existente que vaya a asociar a este servidor virtual de Capa 4 en el menú desplegable.
Grupo de servidores	<p>Seleccione un grupo de servidores existente en el menú desplegable.</p> <p>El grupo de servidores consta de uno o varios servidores, también denominados miembros de grupo, que están configurados de manera similar y ejecutan la misma aplicación.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un grupo de servidores.</p>
Perfil de aplicación	<p>En base al tipo de protocolo, se rellenará automáticamente el perfil de aplicación existente.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un perfil de aplicación.</p>
Persistencia	<p>Seleccione un perfil de persistencia existente en el menú desplegable.</p> <p>El perfil de persistencia se puede habilitar en un servidor virtual para permitir que las conexiones de cliente relacionadas con la IP de origen se envíen al mismo servidor.</p>
Máximo de conexiones simultáneas	Establezca la cantidad máxima de conexiones simultáneas permitidas con un servidor virtual de modo que el servidor virtual no consuma recursos de otras aplicaciones alojadas en el mismo equilibrador de carga.
Velocidad máxima de conexión nueva	Establezca el máximo para la nueva conexión con un miembro del grupo de servidores de modo que un servidor virtual no consuma recursos.
Grupo de servidores Sorry	<p>Seleccione un grupo de servidores de respaldo existente en el menú desplegable.</p> <p>El grupo de servidores de respaldo atiende la solicitud cuando un equilibrador de carga no puede seleccionar un servidor de back-end para atender la solicitud del grupo predeterminado.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un grupo de servidores.</p>
Puerto de miembro de grupo predeterminado	<p>Introduzca un puerto de miembro de grupo predeterminado si el puerto de miembro de grupo de un servidor virtual no está definido.</p> <p>Por ejemplo, si se define un servidor virtual con el rango de puertos 2000-2999 y el rango de puertos del miembro de grupo predeterminado se establece en 8000-8999, se envía una conexión de cliente entrante con el puerto de servidor virtual 2500 a un miembro del grupo con un puerto de destino establecido en 8500.</p>
Estado del administrador	Active el botón para deshabilitar el estado de administrador del servidor virtual de Capa 4.
Registro de acceso	Active el botón para habilitar el registro del servidor virtual de Capa 4.
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>

Agregar servidores virtuales HTTP de Capa 7

Los servidores virtuales reciben todas las conexiones de cliente y las distribuyen entre los servidores. Un servidor virtual tiene una dirección IP, un puerto y un protocolo TCP.

Las reglas de equilibrador de carga son compatibles solo con los servidores virtuales de capa 7 con un perfil de aplicación HTTP. Distintos servicios de equilibrador de carga pueden utilizar reglas de equilibrador de carga.

Nota El acceso directo SSL de capa 7 se admite en NSX-T Data Center 3.0 y versiones posteriores.

Cada regla de equilibrador de carga consta de una o varias condiciones de coincidencia y una o varias acciones. Si no se especifican las condiciones de coincidencia, la regla de equilibrador de carga siempre coincide y se utiliza para definir las reglas predeterminadas. Si se especifica más de una condición de coincidencia, la estrategia de coincidencia determina si deben coincidir todas o algunas de las condiciones para que la regla de equilibrador de carga se considere como coincidencia.

Cada regla de equilibrador de carga se implementa en una fase específica del procesamiento de equilibrio de carga: reescritura de solicitud HTTP, reenvío de solicitud HTTP y reescritura de respuesta HTTP. No todas las condiciones de coincidencia y las acciones se aplican a cada fase.

Si se deshabilita el estado de un servidor virtual, se rechazarán los nuevos intentos de conexión al servidor virtual mediante el envío de un TCP RST para la conexión TCP o un mensaje de error ICMP para UDP. Se rechazarán las nuevas conexiones incluso si hay entradas de persistencia coincidentes para ellas. Se seguirán procesando las conexiones activas. Si un servidor virtual se elimina o desasocia de un equilibrador de carga, las conexiones activas con ese servidor virtual generan un error.

Nota El perfil de SSL no se admite en la versión NSX-T Data Center Limited Export.

Si se configura un enlace de perfil SSL del lado cliente en un servidor virtual, pero no un enlace de perfil SSL del lado servidor, el servidor virtual funciona en un modo de finalización de SSL, que tiene una conexión cifrada con el cliente y una conexión de texto sin formato con el servidor. Si se configuran enlaces de perfil SSL del lado cliente y el lado servidor, el servidor virtual funciona en modo de servidor proxy SSL, que tiene una conexión cifrada con el cliente y el servidor.

Actualmente no se permite asociar un enlace de perfil SSL del lado servidor sin asociar un enlace de perfil SSL del lado cliente. Si un enlace de perfil SSL del lado cliente y del lado servidor no está asociado a un servidor virtual y la aplicación está basada en SSL, el servidor virtual funciona en un modo que no es compatible con SSL. En este caso, el servidor virtual debe configurarse para la capa 4. Por ejemplo, el servidor virtual puede asociarse a un perfil FAST TCP.

Requisitos previos

- Compruebe que los perfiles de aplicaciones estén disponibles. Consulte [Agregar un perfil de aplicación](#).
- Compruebe que los perfiles persistentes estén disponibles. Consulte [Agregar un perfil de persistencia](#).
- Compruebe que los perfiles de SSL para el cliente y el servidor estén disponibles. Consulte [Agregar un perfil de SSL](#).

- Compruebe que los grupos de servidores estén disponibles. Consulte [Agregar un grupo de servidores](#).
- Compruebe que el certificado de CA y de cliente estén disponibles. Consulte [Crear un archivo de solicitud de firma del certificado](#).
- Compruebe que exista una lista de revocación de certificación (Certification Revocation List, CRL). Consulte [Importar una lista de revocación de certificados](#).
- Compruebe que haya disponible un equilibrador de carga. Consulte [Agregar equilibradores de carga](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Equilibrio de carga > Servidores virtuales > Agregar servidor virtual**.
- 3 Seleccione un protocolo **HTTP de Capa 7** e introduzca la información del protocolo.

Los servidores virtuales de capa 7 admiten los protocolos HTTP y HTTPS.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y una descripción para el servidor virtual de capa 7.
Dirección IP	Introduzca la dirección IP del servidor virtual.
Puertos	Introduzca el número de puerto del servidor virtual.
Equilibrador de carga	Seleccione un equilibrador de carga existente que vaya a asociar a este servidor virtual de Capa 4 en el menú desplegable.
Grupo de servidores	<p>Seleccione un grupo de servidores existente en el menú desplegable.</p> <p>El grupo de servidores consta de uno o varios servidores, también denominados miembros de grupo, que están configurados de manera similar y ejecutan la misma aplicación.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un grupo de servidores.</p>
Perfil de aplicación	<p>En base al tipo de protocolo, se rellenará automáticamente el perfil de aplicación existente.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un perfil de aplicación.</p>
Persistencia	<p>Seleccione un perfil de persistencia existente en el menú desplegable.</p> <p>El perfil de persistencia se puede habilitar en un servidor virtual para permitir que las conexiones de cliente relacionadas con la IP de origen y las cookies se envíen al mismo servidor.</p>

- 4 Haga clic en **Configurar** para establecer el protocolo SSL de servidor virtual de Capa 7.
- Puede configurar el SSL de cliente y el SSL de servidor.

5 Configure el SSL de cliente.

Opción	Descripción
SSL de cliente	Active el botón para habilitar el perfil. El enlace de perfil SSL del lado cliente permite que haya varios certificados, de modo que los nombres de host se asocien con el mismo servidor virtual.
Certificado predeterminado	Seleccione un certificado predeterminado en el menú desplegable. Este certificado se usa si el servidor no aloja varios nombres de host en la misma dirección IP o si el cliente no admite la extensión de Indicación de nombre de servidor (Server Name Indication, SNI).
Perfil SSL de cliente	Seleccione el perfil SSL del lado cliente en el menú desplegable.
Certificados SNI	Seleccione el certificado de SNI disponible en el menú desplegable.
Certificados de CA de confianza	Seleccione el certificado de CA disponible.
Autenticación de cliente obligatoria	Active el botón para habilitar este elemento de menú.
Profundidad de cadena de certificados	Establezca la profundidad de la cadena de certificados para comprobar la profundidad de la cadena de certificados de servidor.
Lista de revocación de certificados	Seleccione la CRL disponible para no permitir certificados de servidor comprometidos.

6 Configure el SSL de servidor.

Opción	Descripción
SSL de servidor	Active el botón para habilitar el perfil.
Certificado de cliente	Seleccione un certificado de cliente en el menú desplegable. Este certificado se usa si el servidor no aloja varios nombres de host en la misma dirección IP o si el cliente no admite la extensión de Indicación de nombre de servidor (Server Name Indication, SNI).
Perfil SSL de servidor	Seleccione el perfil SSL del lado servidor en el menú desplegable.
Certificados de CA de confianza	Seleccione el certificado de CA disponible.
Autenticación del servidor obligatoria	Active el botón para habilitar este elemento de menú. El enlace de perfil SSL del lado servidor especifica si se debe validar o no el certificado de servidor presentado al equilibrador de carga durante el protocolo de enlace SSL. Cuando se habilita la validación, el certificado de servidor debe estar firmado por una de las CA de confianza cuyos certificados autofirmados se especifican en el mismo enlace de perfil SSL del lado servidor.
Profundidad de cadena de certificados	Establezca la profundidad de la cadena de certificados para comprobar la profundidad de la cadena de certificados de servidor.
Lista de revocación de certificados	Seleccione la CRL disponible para no permitir certificados de servidor comprometidos. OCSP y la asociación de OCSP no se admiten en el lado servidor.

7 Configure las propiedades adicionales del servidor virtual de Capa 7.

Opción	Descripción
Máximo de conexiones simultáneas	Establezca la cantidad máxima de conexiones simultáneas permitidas con un servidor virtual de modo que el servidor virtual no consuma recursos de otras aplicaciones alojadas en el mismo equilibrador de carga.
Velocidad máxima de conexión nueva	Establezca el máximo para la nueva conexión con un miembro del grupo de servidores de modo que un servidor virtual no consuma recursos.
Grupo de servidores Sorry	<p>Seleccione un grupo de servidores de respaldo existente en el menú desplegable.</p> <p>El grupo de servidores de respaldo atiende la solicitud cuando un equilibrador de carga no puede seleccionar un servidor de back-end para atender la solicitud del grupo predeterminado.</p> <p>Puede hacer clic en los puntos suspensivos verticales para crear un grupo de servidores.</p>
Puerto de miembro de grupo predeterminado	<p>Introduzca un puerto de miembro de grupo predeterminado si el puerto de miembro de grupo de un servidor virtual no está definido.</p> <p>Por ejemplo, si se define un servidor virtual con el rango de puertos 2000-2999 y el rango de puertos del miembro de grupo predeterminado se establece en 8000-8999, se envía una conexión de cliente entrante con el puerto de servidor virtual 2500 a un miembro del grupo con un puerto de destino establecido en 8500.</p>
Estado del administrador	Active el botón para deshabilitar el estado de administrador del servidor virtual de Capa 7.
Registro de acceso	Active el botón para habilitar el registro del servidor virtual de Capa 7.
Etiquetas	<p>Introduzca etiquetas para facilitar la búsqueda.</p> <p>Puede especificar una etiqueta para establecer un ámbito para la etiqueta.</p>

8 Haga clic en **Guardar**.

Agregar reglas de equilibrador de carga

Con servidores virtuales HTTP de Capa 7, opcionalmente, puede configurar reglas de equilibrador de carga y personalizar el comportamiento de equilibrio de carga mediante reglas de coincidencia o de acción.

Las reglas del equilibrador de carga admiten REGEX para los tipos de coincidencia. Los patrones REGEX de estilo PCRE se admiten con algunas limitaciones en los casos de uso avanzado. Cuando se utiliza REGEX en condiciones de coincidencia, se admiten grupos de captura con nombre.

Estas son las restricciones de REGEX:

- No se admiten uniones ni intersecciones de caracteres. Por ejemplo, no utilice `[a-z[0-9]]` ni `[a-z&&[aeiou]]`; en su lugar, use `[a-z0-9]` y `[aeiou]`, respectivamente.
- Solo se admiten 9 referencias inversas, y se pueden usar de `\1` a `\9` para hacer referencia a ellas.
- Utilice el formato `\Odd` para hacer coincidir caracteres octales, no el formato `\ddd`.

- No se admiten marcas integradas en el nivel superior; este tipo de marca solo se admite en los grupos. Por ejemplo, no utilice "Case (?i:s)ensitive"; en su lugar, use "Case ((?i:s)ensitive)".
- No se admiten las operaciones de preprocesamiento \l \u, \L ni \U. Donde \l indica que el siguiente carácter será una minúscula; \u indica que el siguiente carácter será una mayúscula; \L indica que el texto estará en minúscula hasta \E; y, por último, \U indica que el texto estará en mayúscula hasta \E.
- (?<condition>X), (?<code>), (?<Code>) y (?<#comment>) no se admiten.
- No se admite la clase de carácter Unicode predefinida \X.
- No se admiten construcciones de caracteres con nombre para los caracteres Unicode. Por ejemplo, no utilice \N{name}; en su lugar, use \u2018.

Cuando se utiliza REGEX en condiciones de coincidencia, se admiten grupos de captura con nombre. Por ejemplo, el patrón de coincidencia REGEX /news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+))/(?(<article>.*)) se puede utilizar para hacer coincidir un URI como /news/2018-06-15/news1234.html.

A continuación, las variables se establecen como se indica a continuación: \$year = "2018" \$month = "06" \$day = "15" \$article = "news1234.html". Después de definir las variables, estas se pueden utilizar en las acciones de regla del equilibrador de carga. Por ejemplo, el URI se puede reescribir con las variables de coincidencia como /news.py?year=\$year&month=\$month&day=\$day&article=\$article. Seguidamente, el URI se reescribirá como /news.py?year=2018&month=06&day=15&article=news1234.html.

Las acciones de reescritura pueden utilizar una combinación de grupos de captura con nombre y variables integradas. Por ejemplo, el URI se puede reescribir como /news.py?year=\$year&month=\$month&day=\$day&article=\$article&user_ip=\$_remote_addr. A continuación, el URI de ejemplo se reescribirá como /news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1.

Nota Para los grupos de captura con nombre, el nombre no puede comenzar con el carácter "_".

Además de los grupos de captura con nombre, se pueden usar las siguientes variables integradas en las acciones de reescritura. Todos los nombres de las variables integradas comienzan con _.

- \$_args: los argumentos de la solicitud.
- \$_arg_<nombre>: el <nombre> del argumento de la línea de solicitud.
- \$_cookie_<nombre>: el valor de la cookie <nombre>.
- \$_upstream_cookie_<nombre>: la cookie con el nombre especificado que envía el servidor upstream del campo de encabezado de respuesta "Set-Cookie".
- \$_upstream_http_<nombre>: un campo de encabezado de respuesta arbitrario, y <nombre> es el nombre del campo convertido en minúscula con guiones reemplazados por guiones bajos.

- `$_host` (en orden de precedencia): el nombre de host de la línea de la solicitud, el nombre de host del campo "Host" del encabezado de la solicitud, o el nombre del servidor que coincida con una solicitud.
- `$_http_<nombre>`: un campo de encabezado de la solicitud arbitrario, y `<nombre>` es el nombre del campo en minúscula con guiones reemplazados por guiones bajos.
- `$_https`: "on" si la conexión funciona en modo SSL; de lo contrario, "".
- `$_is_args`: "?" si una línea de la solicitud tiene argumentos; de lo contrario, "".
- `$_query_string`: igual que `$_args`.
- `$_remote_addr`: la dirección del cliente.
- `$_remote_port`: el puerto del cliente.
- `$_request_uri`: el URI completo de la solicitud original (con argumentos).
- `$_scheme`: el esquema de la solicitud, "http" o "https".
- `$_server_addr`: la dirección del servidor que aceptó una solicitud.
- `$_server_name`: el nombre del servidor que aceptó una solicitud.
- `$_server_port`: el puerto del servidor que aceptó una solicitud.
- `$_server_protocol`: el protocolo de solicitud; suele ser "HTTP/1.0" o "HTTP/1.1".
- (Solo NSX-T Data Center 2.5.0) `$_ssl_client_cert`: devuelve el certificado de cliente en formato PEM para una conexión SSL establecida con cada línea, exceptuando la primera antecedida por el carácter de tabulación.
- (Solo NSX-T Data Center 2.5.1 y versiones posteriores) `$_ssl_client_escaped_cert`: devuelve el certificado de cliente en formato PEM para una conexión SSL establecida.
- `$_ssl_server_name`: devuelve el nombre del servidor solicitado mediante la SNI.
- `$_uri`: la ruta del URI de la solicitud.
- `$_ssl_ciphers`: devuelve los cifrados SSL de cliente
- `$_ssl_client_i_dn`: devuelve la cadena "DN de emisor" del certificado de cliente para una conexión SSL establecida de acuerdo con RFC 2253
- `$_ssl_client_s_dn`: devuelve la cadena "DN de asunto" del certificado de cliente para una conexión SSL establecida de acuerdo con RFC 2253
- `$_ssl_protocol`: devuelve el protocolo de una conexión SSL establecida
- `$_ssl_session_reused`: devuelve "r" si se reutilizó una sesión SSL, o "." en el resto de casos

Requisitos previos

Compruebe que haya disponible un servidor virtual HTTP de Capa 7. Consulte [Agregar servidores virtuales HTTP de Capa 7](#).

Procedimiento

- 1 Abra el servidor virtual HTTP de Capa 7.
- 2 En la sección Reglas de equilibrador de carga, haga clic en **Establecer > Agregar regla** para configurar las reglas de equilibrador de carga para la fase de reescritura de solicitud HTTP.

Los tipos de coincidencia compatibles son REGEX, STARTS_WITH, ENDS_WITH, entre otras, y la opción inversa.

Condición de coincidencia compatible	Descripción
Método de solicitud HTTP	Coincide con un método de solicitud HTTP. http_request.method: valor que debe coincidir.
URI de solicitud HTTP	Coincide con un URI de solicitud HTTP sin argumentos de consulta. http_request.uri: valor que debe coincidir.
Argumentos de URI de solicitud HTTP	Coincide con un argumento de consulta URI de solicitud HTTP. http_request.uri_arguments: valor que debe coincidir.
Versión de solicitud HTTP	Coincide con una versión de solicitud HTTP. http_request.version: valor que debe coincidir.
Encabezado de solicitud HTTP	Coincide con cualquier encabezado de solicitud HTTP. http_request.header_name: nombre de encabezado que debe coincidir. http_request.header_value: valor que debe coincidir.
Cookie de solicitud HTTP	Coincide con cualquier cookie de solicitud HTTP. http_request.cookie_value: valor que debe coincidir.
Cuerpo de solicitud HTTP	Coincide con el contenido del cuerpo de la solicitud HTTP. http_request.body_value: valor que debe coincidir.
SSL de cliente	Coincide con el identificador de perfil SSL del cliente. ssl_profile_id: valor que debe coincidir.
Puerto de encabezado TCP	Coincide con un puerto TCP de origen o destino. tcp_header.source_port: puerto de origen que debe coincidir. tcp_header.destination_port: puerto de destino que debe coincidir.
Origen de encabezado IP	Coincide con una dirección IP de origen o destino. ip_header.source_address: dirección de origen que debe coincidir. ip_header.destination_address: dirección de destino que debe coincidir.

Condición de coincidencia compatible	Descripción
Variable	Cree una variable y asigne un valor a la variable.
Distingue entre mayúsculas y minúsculas	Establezca una marca que distinga mayúsculas de minúsculas para la comparación de valores de encabezado HTTP.
Acciones	Descripción
Reescritura de URI de solicitud HTTP	Modifica un URI. http_request.uri: URI (sin argumentos de consulta) que se debe escribir. http_request.uri_args: argumentos de consulta URI que se deben escribir.
Reescritura de encabezado de solicitud HTTP	Modifica el valor de un encabezado HTTP. http_request.header_name: nombre de encabezado. http_request.header_value: valor que se debe escribir.
Eliminación de encabezado de solicitud HTTP	Elimine el encabezado HTTP. http_request.header_delete: nombre de encabezado. http_request.header_delete: valor que se debe escribir.

- 3 Haga clic en **Solicitar reenvío > Agregar regla** para configurar las reglas de equilibrador de carga para el reenvío de solicitud HTTP.

Todos los valores de coincidencia aceptan expresiones regulares.

Condición de coincidencia compatible	Descripción
Método de solicitud HTTP	Coincide con un método de solicitud HTTP. http_request.method: valor que debe coincidir.
URI de solicitud HTTP	Coincide con un URI de solicitud HTTP. http_request.uri: valor que debe coincidir.
Versión de solicitud HTTP	Coincide con una versión de solicitud HTTP. http_request.version: valor que debe coincidir.
Encabezado de solicitud HTTP	Coincide con cualquier encabezado de solicitud HTTP. http_request.header_name: nombre de encabezado que debe coincidir. http_request.header_value: valor que debe coincidir.
Cookie de solicitud HTTP	Coincide con cualquier cookie de solicitud HTTP. http_request.cookie_value: valor que debe coincidir.
Cuerpo de solicitud HTTP	Coincide con el contenido del cuerpo de la solicitud HTTP. http_request.body_value: valor que debe coincidir.
SSL de cliente	Coincide con el identificador de perfil SSL del cliente. ssl_profile_id: valor que debe coincidir.
Puerto de encabezado TCP	Coincide con un puerto TCP de origen o destino. tcp_header.source_port: puerto de origen que debe coincidir. tcp_header.destination_port: puerto de destino que debe coincidir.

Condición de coincidencia compatible	Descripción
Origen de encabezado IP	<p>Coincide con una dirección IP de origen o destino.</p> <p>ip_header.source_address: dirección de origen que debe coincidir.</p> <p>ip_header.destination_address: dirección de destino que debe coincidir.</p>
Variable	Cree una variable y asigne un valor a la variable.
Distingue entre mayúsculas y minúsculas	Establezca una marca que distinga mayúsculas de minúsculas para la comparación de valores de encabezado HTTP.
Acción	Descripción
Rechazo de HTTP	<p>Rechaza una solicitud, por ejemplo, estableciendo el estado en 5xx.</p> <p>http_forward.reply_status: código de estado HTTP utilizado para el rechazo.</p> <p>http_forward.reply_message: mensaje de rechazo de HTTP.</p>
Redireccionamiento de HTTP	<p>Redirige una solicitud. El código de estado debe establecerse en 3xx.</p> <p>http_forward.redirect_status: código de estado HTTP de redirección.</p> <p>http_forward.redirect_url: URL de redirección de HTTP.</p>
Seleccionar grupo	<p>Fuerza la solicitud a un grupo de servidores específicos. El algoritmo configurado del miembro del grupo especificado (predictor) se utiliza para seleccionar un servidor del grupo de servidores.</p> <p>http_forward.select_pool: UUID de grupo de servidores.</p>
Activación de persistencia de variables	<p>Seleccione un perfil de persistencia genérico e introduzca un nombre de variable.</p> <p>También puede habilitar Variable hash. Si el valor de la variable es muy largo, la variable hash garantiza que se almacenará correctamente en la tabla de persistencia. Si no habilita Variable hash, solo se almacenará la parte fija del prefijo en la tabla de persistencia en caso de que el valor de la variable sea muy largo. En consecuencia, puede que se envíen dos solicitudes diferentes con valores de variables largas al mismo servidor de back-end (porque sus valores de variables tienen el mismo prefijo) cuando deberían enviarse a servidores de back-end distintos.</p>
Estado de respuesta	Muestra el estado de la respuesta.
Mensaje de respuesta	El servidor responde con un mensaje de respuesta que contiene la configuración y las direcciones confirmadas.

- Haga clic en **Reescritura de respuesta > Agregar regla** para configurar las reglas de equilibrador de carga para la reescritura de respuesta HTTP.

Todos los valores de coincidencia aceptan expresiones regulares.

Condición de coincidencia compatible	Descripción
Encabezado de respuesta HTTP	Coincide con cualquier encabezado de respuesta HTTP. http_response.header_name: nombre del encabezado que debe coincidir. http_response.header_value: valor que debe coincidir.
Método de respuesta HTTP	Coincide con un método de respuesta HTTP. http_response.method: valor que debe coincidir.
URI de respuesta HTTP	Coincide con un URI de respuesta HTTP. http_response.uri: valor que debe coincidir.
Argumentos de URI de respuesta HTTP	Coincide con los argumentos de un URI de respuesta HTTP. http_response.uri_args: valor que debe coincidir.
Versión de respuesta HTTP	Coincide con una versión de respuesta HTTP. http_response.version: valor que debe coincidir.
Cookie de respuesta HTTP	Coincide con cualquier cookie de respuesta HTTP. http_response.cookie_value: valor que debe coincidir.
SSL de cliente	Coincide con el identificador de perfil SSL del cliente. ssl_profile_id: valor que debe coincidir.
Puerto de encabezado TCP	Coincide con un puerto TCP de origen o destino. tcp_header.source_port: puerto de origen que debe coincidir. tcp_header.destination_port: puerto de destino que debe coincidir.
Origen de encabezado IP	Coincide con una dirección IP de origen o destino. ip_header.source_address: dirección de origen que debe coincidir. ip_header.destination_address: dirección de destino que debe coincidir.
Variable	Cree una variable y asigne un valor a la variable.
Distingue entre mayúsculas y minúsculas	Establezca una marca que distinga mayúsculas de minúsculas para la comparación de valores de encabezado HTTP.

Acción	Descripción
Reescritura de encabezado de respuesta HTTP	Modifica el valor del encabezado de una respuesta HTTP. http_response.header_name: nombre de encabezado. http_response.header_value: valor que se debe escribir.
Eliminación de encabezado de respuesta HTTP	Elimine el encabezado HTTP. http_request.header_delete: nombre de encabezado. http_request.header_delete: valor que se debe escribir.
Aprendizaje de persistencia de variables	Seleccione un perfil de persistencia genérico e introduzca un nombre de variable.

Acción	Descripción
	También puede habilitar Variable hash . Si el valor de la variable es muy largo, la variable hash garantiza que se almacenará correctamente en la tabla de persistencia. Si no habilita Variable hash , solo se almacenará la parte fija del prefijo en la tabla de persistencia en caso de que el valor de la variable sea muy largo. En consecuencia, puede que se envíen dos solicitudes diferentes con valores de variables largas al mismo servidor de back-end (porque sus valores de variables tienen el mismo prefijo) cuando deberían enviarse a servidores de back-end distintos.

Grupos creados para grupos de servidores y servidores virtuales

NSX Manager crea automáticamente grupos para puertos VIP y grupos de servidores del equilibrador de carga.

Los grupos creados para el equilibrador de carga se pueden ver en **Inventario > Grupos**.

Los conjuntos de grupos de servidores se crean con el nombre NLB.PoolLB.*Nombre_grupo Nombre_LB* y con las direcciones IP de los miembros del grupo asignadas:

- Grupo configurado sin LB-SNAT (transparente): 0.0.0.0/0
- Grupo configurado sin B-SNAT Automap: T1-Uplink IP 100.64.x.y y T1-ServiceInterface IP
- Grupo configurado sin LB-SNAT IP-Pool: LB-SNAT IP-Pool

Los grupos VIP se crean con el nombre NLB.VIP.*nombre del servidor virtual* y las direcciones IP de los miembros del grupo de VIP son VIP IP@.

Para los conjuntos de grupos de servidores, puede crear una regla de firewall distribuido para permitir tráfico desde el equilibrador de carga (NLB.PoolLB. *Nombre_grupo Nombre_LB*). Para el firewall de puerta de enlace de nivel 1, puede crear una regla para permitir el tráfico desde los clientes hasta LB VIP NLB.VIP.*nombre de servidor virtual*.

Directivas de reenvío

8

Esta función corresponde a NSX Cloud.

Las directivas de reenvío o reglas de enrutamiento basadas en directivas (Policy-Based Routing, PBR) establecen cómo procesa NSX-T el tráfico procedente de una máquina virtual administrada por NSX. Este tráfico se puede dirigir a la superposición de NSX-T o se puede enrutar a través de la red (subyacente) del proveedor de nube.

Nota Consulte [Capítulo 22 Uso de NSX Cloud](#) para obtener más información sobre cómo administrar las máquinas virtuales de carga de trabajo de nube pública con NSX-T Data Center.

Hay tres directivas de reenvío que se configuran de forma predeterminada después de que implemente una puerta de enlace de nube pública (Public Cloud Gateway, PCG) en una nube privada virtual (Virtual Private Cloud, VPC) o una red virtual (Virtual Network, VNet) de tránsito, o bien de que vincule una VPC o una VNet de equipo a una VPC o una VNet de tránsito.

- 1 Una **ruta hacia subyacente** para el todo el tráfico dentro de la VPC o VNet de tránsito o de equipo
- 2 Otra **ruta hacia la subyacente** para todo el tráfico dirigido a los servicios de metadatos de la nube pública.
- 3 Una **ruta hacia la subyacente**: para todo el tráfico, por ejemplo, el tráfico que se dirige fuera de la VPC o la VNet de tránsito o de equipo. Este tipo de tráfico se enruta a través del túnel de la superposición de NSX-T hacia la PCG y, posteriormente, hacia su destino.

Nota Tráfico dirigido a otra VPC o VNET administrada por la misma PCG: el tráfico se enruta desde la VPC o la VNet administrada por NSX de origen a través del túnel de la superposición de NSX-T hasta la PCG y, a continuación, se enruta hacia la VPC o la VNet de destino.

Tráfico dirigido a otra VPC o VNet administrada por otra PCG: el tráfico se enruta desde una VPC o una VNet administrada por NSX a través del túnel de la superposición de NSX hasta la PCG de la VPC o la VNet de origen y se reenvía a la PCG de la VPC o la VNet administrada por NSX de destino.

Si el tráfico se dirige a Internet, la PCG lo enruta hasta el destino de Internet.

Microsegmentación con la directiva Ruta hacia subordinación

La microsegmentación se aplica incluso en el caso de las máquinas virtuales de cargas de trabajo cuyo tráfico se enruta a través de la red subyacente.

Si hay conectividad directa desde una máquina virtual de carga de trabajo administrada por NSX hasta un destino situado fuera de la VPC o la VNet administrada y quiere omitir la PCG, configure una directiva de reenvío para enrutar el tráfico procedente de esta máquina virtual a través de la red subyacente.

Cuando el tráfico se enruta a través de la red subyacente, la PCG se omite y el tráfico evita el firewall de norte a sur. Sin embargo, deberá seguir gestionando las reglas para el firewall distribuido o de este a oeste (Distributed Firewall, DFW), ya que esas reglas se aplican en el nivel de la máquina virtual antes de que llegue a la PCG.

Directivas de reenvío admitidas y casos de uso comunes

Aunque puede consultar una lista de directivas de reenvío en el menú desplegable, solo se admiten las siguientes en esta versión:

- Ruta hacia subyacente
- Ruta desde subyacente
- Ruta hacia superposición

Estos son los casos comunes en los que las directivas de reenvío resultan útiles:

- **Ruta hacia la subordinación:** acceda a un servicio de la red subyacente desde una máquina virtual administrada por NSX. Por ejemplo, acceda al servicio S3 de Amazon Web Services (AWS) en la red subyacente de AWS.
- **Ruta hacia la subordinación:** acceda a un servicio alojado en una máquina virtual administrada por NSX desde la red subyacente. Por ejemplo, acceda a la máquina virtual administrada por NSX desde Elastic Load Balancing (ELB) de AWS.

Este capítulo incluye los siguientes temas:

- [Agregar o editar directivas de reenvío](#)

Agregar o editar directivas de reenvío

Puede editar las directivas de reenvío creadas automáticamente o agregar otras nuevas.

Por ejemplo, si desea utilizar los servicios que proporciona la nube pública (como S3 de AWS), puede crear manualmente una directiva que permita a un conjunto de direcciones IP acceder a este servicio a través del enrutamiento mediante subordinación.

Requisitos previos

Debe tener una VPC o una VNet en las que se implementó una instancia de PCG.

Procedimiento

- 1 Haga clic en **Agregar sección**. Asigne un nombre correcto a la sección (por ejemplo, **Servicios de AWS**).
- 2 Active la casilla que aparece junto a la sección y haga clic en **Agregar regla**. Asigne un nombre a la regla (por ejemplo, **Reglas de S3**).
- 3 En la pestaña **Orígenes**, seleccione la VPC o la VNet en la que se encuentren las máquinas virtuales de cargas de trabajo a las que desea proporcionar acceso al servicio (por ejemplo, la VPC de AWS). También puede crear un **Grupo** aquí para incluir varias máquinas virtuales que coincidan con uno o varios criterios.
- 4 En la pestaña **Destinos**, seleccione la VPC o la VNet en las que se aloja el servicio (por ejemplo, un **Grupo** que contiene la dirección IP del servicio S3 en AWS).
- 5 En la pestaña **Servicios**, seleccione el servicio del menú desplegable. Si el servicio no existe, puede agregarlo. También puede dejar **Cualquiera** seleccionado, ya que puede proporcionar los detalles de enrutamiento en **Destinos**.
- 6 En la pestaña **Acción**, seleccione cómo desea que se produzca el enrutamiento. Por ejemplo, seleccione **Ruta hacia subordinación** si configura esta directiva para el servicio S3 de AWS.
- 7 Haga clic en **Publicar** para finalizar la configuración de la directiva de reenvío.

Administración de direcciones IP (IP Address Management, IPAM)

9

Para administrar las direcciones IP, puede configurar los bloques de direcciones IP, el protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP), los grupos de direcciones IP y el sistema de nombres de dominio (Domain Name System, DNS).

Nota NSX Container Plug-in (NCP) utiliza los bloques de direcciones IP. Para obtener más información sobre NCP, consulte la *Guía de instalación y administración de NSX Container Plug-in para Kubernetes y Cloud Foundry*.

Este capítulo incluye los siguientes temas:

- [Agregar una zona de DNS](#)
- [Agregar un servicio de reenviador DNS](#)
- [Agregar un servidor DHCP](#)
- [Configurar un servidor de retransmisión DHCP para una puerta de enlace de nivel 0 o nivel 1](#)
- [Agregar un grupo de direcciones IP](#)
- [Agregar un bloque de direcciones IP](#)

Agregar una zona de DNS

Puede configurar zonas de DNS para el servicio de DNS. Una zona de DNS es una parte definida del espacio de nombres de dominio en DNS.

Cuando se configura una zona de DNS, se puede especificar una IP de origen para que la utilice un reenviador de DNS para reenviar las consultas de DNS a un servidor DNS ascendente. Si no especifica una IP de origen, la dirección IP de origen del paquete de consulta de DNS será la IP del agente de escucha del reenviador de DNS. Es necesario especificar una dirección IP de origen si la IP del agente de escucha es una dirección interna a la que no se puede acceder desde el servidor DNS ascendente externo. Para garantizar que los paquetes de respuesta de DNS vuelvan a enrutarse al reenviador, se necesita una dirección IP de origen dedicada. Como alternativa, puede configurar SNAT en el enrutador lógico para convertir la IP del agente de escucha en una dirección IP pública. En este caso, no es necesario especificar una dirección IP de origen.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Administración de direcciones IP > DNS**.
- 3 Haga clic en la pestaña **Zonas de DNS**.
- 4 Para agregar una zona predeterminada, seleccione **Agregar zona de DNS > Agregar zona predeterminada**.
 - a Introduzca un nombre y, si lo desea, una descripción.
 - b Introduzca la dirección IP de hasta tres servidores de DNS.
 - c (opcional) Introduzca una dirección IP en el campo **IP de origen**.
- 5 Para agregar una zona FQDN, seleccione **Agregar zona de DNS > Agregar zona de FQDN**.
 - a Introduzca un nombre y, si lo desea, una descripción.
 - b Introduzca un FQDN para el dominio.
 - c Introduzca la dirección IP de hasta tres servidores de DNS.
 - d (opcional) Introduzca una dirección IP en el campo **IP de origen**.
- 6 Haga clic en **Guardar**.

Agregar un servicio de reenviador DNS

Puede configurar un reenviador DNS para reenviar consultas de DNS a servidores DNS externos.

Antes de configurar un reenviador DNS, debe configurar una zona de DNS predeterminada. De forma opcional, puede configurar una o varias zonas DNS de FQDN. Cada zona DNS se asocia a un máximo de 3 servidores DNS. Cuando configure una zona DNS de FQDN, especifique uno o varios nombres de dominio. Un reenviador DNS se asocia a una zona DNS predeterminada y a un máximo de 5 zonas DNS de FQDN. Cuando se recibe una consulta de DNS, el reenviador DNS compara el nombre de dominio de la consulta con los nombres de dominio de las zonas DNS de FQDN. Si encuentra una coincidencia, la consulta se reenvía a los servidores DNS especificados en la zona DNS de FQDN. Si no encuentra una coincidencia, la consulta se reenvía a los servidores DNS especificados en la zona DNS predeterminada.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Administración de direcciones IP > DNS**.
- 3 Haga clic en **Agregar servicio de DNS**.
- 4 Introduzca un nombre y, si lo desea, una descripción.
- 5 Seleccione una puerta de enlace de nivel 0 o nivel 1.

6 Introduzca la dirección IP del servicio de DNS.

Los clientes envían consultas de DNS a esta dirección IP, que también se conoce como IP del agente de escucha del reenviador DNS.

7 Seleccione una zona de DNS predeterminada.

8 Seleccione un nivel de registro.

9 Seleccione hasta cinco zonas FQDN.

10 Haga clic en el botón de alternancia **Estado de administración** para habilitar o deshabilitar el servicio de DNS.

11 Haga clic en **Guardar**.

Agregar un servidor DHCP

El Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) permite a los clientes obtener de forma automática la configuración de la red, como direcciones IP, máscara de subred, puerta de enlace predeterminada y configuración de DNS desde un servidor DHCP. Puede crear servidores DHCP para gestionar las solicitudes DHCP.

Nota El servidor DHCP que se crea mediante este procedimiento no es compatible con un segmento respaldado por VLAN. Debe utilizar la función DHCP disponible en **Opciones avanzadas de redes y seguridad** para crear un servidor DHCP que sea compatible con un conmutador lógico respaldado por VLAN.

Procedimiento

1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

2 Seleccione **Redes > Administración de direcciones IP > DHCP**.

3 Haga clic en **Agregar servidor**.

4 Seleccione **Servidor DHCP** como tipo de servidor.

5 Introduzca un nombre para el servidor.

6 Introduzca la dirección IP del servidor en formato CIDR.

Este paso creará dos puertos lógicos (uno para una interfaz lógica y otro para el propio servidor DHCP) y conectará el servidor DHCP a un conmutador lógico de DHCP específico. Esta interfaz aparecerá en la puerta de enlace de nivel 0 o nivel 1 como una interfaz conectada, por lo que debe elegir una subred no superpuesta para la puerta de enlace de nivel 1 o nivel 0 a la que desea asignar el servidor DHCP. Para ello, puede especificar <Dirección IP>/30 para este propósito. El rango de subred utilizado aquí no se anuncia a la puerta de enlace de nivel 0 conectada, pero sí aparece en la tabla de reenvíos de la puerta de enlace de nivel 1.

7 Introduzca un tiempo de concesión.

- 8 Seleccione un clúster de NSX Edge.
- 9 Haga clic en **Guardar**.
- 10 Para asignar un servidor DHCP a una puerta de enlace de nivel 0 o nivel 1:
 - a Desplácese hasta **Redes > Puertas de enlace de nivel 0** o **Redes > Puertas de enlace de nivel 1**.
 - b Edite una puerta de enlace.
 - c En el campo **Administración de direcciones IP**, haga clic en **No hay asignaciones de IP**.
 - d Seleccione **Servidor local DHCP** en la lista desplegable Tipo.
 - e Seleccione un servidor DHCP.
 - f Haga clic en **Guardar**.
 - g Haga clic en **Guardar**.
- 11 Para asignar un servidor DHCP a un segmento:
 - a Desplácese hasta **Redes > Segmentos**.
 - b Añada o edite un segmento.

El segmento debe estar asociado a una puerta de enlace de nivel 0 o nivel 1.
 - c Haga clic en **Establecer subredes** si desea agregar un nuevo segmento o en el número debajo de **Subredes** si desea agregar o modificar una subred.
 - d Introduzca los rangos DHCP apropiados.
 - e Haga clic en **Aplicar**.
 - f Haga clic en **Guardar**.

Configurar un servidor de retransmisión DHCP para una puerta de enlace de nivel 0 o nivel 1

El Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) permite a los clientes obtener de forma automática la configuración de la red, como direcciones IP, máscara de subred, puerta de enlace predeterminada y configuración de DNS desde un servidor DHCP. Puede crear un servidor de retransmisión DHCP para retransmitir el tráfico DHCP a servidores DHCP externos.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Administración de direcciones IP > DHCP**.
- 3 Haga clic en **Agregar servidor**.
- 4 Seleccione **Retransmisión DHCP** como tipo de servidor.

- 5 Introduzca un nombre para el servidor de retransmisión.
- 6 Introduzca una o varias direcciones IP para el servidor.
- 7 Haga clic en **Guardar**.
- 8 Desplácese hasta **Redes > Puertas de enlace de nivel 0**, o bien **Redes > Puertas de enlace de nivel 1** para configurar un servidor de retransmisión DHCP para una puerta de enlace.
- 9 Edite la puerta de enlace correspondiente.
- 10 En el campo **Administración de direcciones IP**, haga clic en **No hay asignaciones de IP** para la puerta de enlace de nivel 0, o en **No hay asignaciones de IP establecidas** para la puerta de enlace de nivel 1.
- 11 En el campo **Tipo**, seleccione **Retransmisión de DHCP**.
- 12 En el campo **Retransmisión de DHCP**, seleccione el servidor de retransmisión DHCP que creó anteriormente.
- 13 Haga clic en **Guardar**.
- 14 Para que funcione la retransmisión, deberá especificar rangos de DHCP para cada segmento conectado a la puerta de enlace que utilizará este servicio de retransmisión de DHCP.
 - a Desplácese hasta **Redes > Segmentos**.
 - b Añada o edite un segmento.
 - c Haga clic en **Establecer subredes** si desea agregar un segmento o en el número debajo de **Subredes** si desea modificar una subred.
 - d Especifique uno o varios rangos de DHCP.

Este paso es necesario para que funcione la retransmisión.
 - e Haga clic en **Aplicar**.
 - f Haga clic en **Guardar**.

Agregar un grupo de direcciones IP

Puede configurar grupos de direcciones IP para utilizar con componentes, como DHCP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Administración de direcciones IP > Grupos de direcciones IP**.
- 3 Haga clic en **Agregar grupo de direcciones IP**.
- 4 Introduzca un nombre y, si lo desea, una descripción.
- 5 Haga clic en **Establecer** en la columna **Subredes** para agregar subredes.

- 6 Para especificar un bloque de direcciones, seleccione **Agregar subred > Bloque de direcciones IP**.
 - a Seleccione un bloque de direcciones IP.
 - b Especifique un tamaño.
 - c Haga clic en el botón de alternancia **Asignar puerta de enlace automáticamente** para habilitar o deshabilitar la asignación automática de la dirección IP de la puerta de enlace.
 - d Haga clic en **Agregar**.
- 7 Para especificar los rangos de direcciones IP, seleccione **Agregar subred > Rangos de IP**.
 - a Introduzca los rangos de IP IPv4 o IPv6.
 - b Introduzca los rangos de IP en formato CIDR.
 - c Introduzca una dirección para **IP de puerta de enlace**.
 - d Haga clic en **Agregar**.
- 8 Haga clic en **Guardar**.

Agregar un bloque de direcciones IP

Los bloques de direcciones IP se pueden configurar para que otros componentes puedan usarlos.

Nota Un bloque de direcciones IP también se puede agregar si se desplaza hasta **Opciones avanzadas de redes y seguridad > Redes > IPAM**.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Redes > Administración de direcciones IP > Grupos de direcciones IP**.
- 3 Haga clic en la pestaña **Bloques de direcciones IP**.
- 4 Haga clic en **Agregar bloque de direcciones IP**.
- 5 Introduzca un nombre y, si lo desea, una descripción.
- 6 Introduzca un bloque de IP en formato CIDR.
- 7 Haga clic en **Guardar**.

Los temas de esta sección tratan la seguridad de norte a sur y de este a oeste para reglas de firewall distribuido, firewall de identidad, introspección de red, firewall de puerta de enlace y directivas de protección de endpoints.

Este capítulo incluye los siguientes temas:

- Información general de la configuración de seguridad
- Terminología de seguridad
- Firewall de identidad
- Perfil de contexto de Capa 7
- Firewall distribuido
- Seguridad de red de este a oeste: cadena de servicios de terceros
- Configurar un firewall de puerta de enlace
- Seguridad de red de norte a sur: inserción de servicio de terceros
- Protección de endpoints
- Perfiles de seguridad

Información general de la configuración de seguridad

Configure las directivas de firewall de Este a Oeste y de Norte a Sur en categorías predefinidas para su entorno.

El firewall distribuido (de este a oeste) y el firewall de puerta de enlace (de norte a sur) ofrecen varios conjuntos de reglas configurables que se dividen en categorías. Puede configurar una lista de exclusión que contenga los conmutadores lógicos, los puertos lógicos o los grupos que se excluirán de la aplicación del firewall.

Las directivas de firewall se aplican de la siguiente manera:

- Las reglas se procesan en categorías, de izquierda a derecha.
- Las reglas se procesan siguiendo un orden de arriba a abajo.

- Cada paquete se compara con la regla principal de la tabla antes de bajar a las reglas subsiguientes de esa tabla.
- Se aplica la primera regla de la tabla que coincide con los parámetros de tráfico.

No se pueden aplicar las reglas subsiguientes, ya que la búsqueda en ese paquete finaliza. Debido a este comportamiento, se recomienda siempre colocar las directivas más pormenorizadas al principio de la tabla. Esto garantiza que se apliquen antes que otras reglas más específicas.

Terminología de seguridad

Los siguientes términos se utilizan en toda la referencia al firewall distribuido.

Tabla 10-1. Terminología relacionada con la seguridad

Término	Definición
Directiva	Una directiva de seguridad incluye diversos elementos de seguridad, incluidas las reglas de firewall y las configuraciones de servicio. La directiva anteriormente se denominaba sección de firewall.
Regla	Un conjunto de parámetros con los que se comparan los flujos y que definen las acciones que se llevarán a cabo tras una coincidencia. Las reglas incluyen parámetros, como el origen y el destino, el servicio, el perfil de contexto, el registro y etiquetas.
Grupo	Los grupos incluyen distintos objetos que se agregan tanto de forma estática como dinámica y pueden utilizarse como campo de origen y de destino de una regla de firewall. Los grupos se pueden configurar para que contengan una combinación de máquinas virtuales, conjuntos de direcciones IP, conjuntos de direcciones MAC, puertos lógicos, conmutadores lógicos, grupos de usuarios de AD y otros grupos anidados. La inclusión dinámica de grupos puede basarse en la etiqueta, el nombre del equipo, el nombre del sistema operativo o el nombre del equipo. Cuando crea un grupo, debe incluir un dominio al que pertenezca dicho grupo; este es el dominio predeterminado. Los grupos anteriormente se denominaban NSGroup o grupo de seguridad.
Servicio	Define una combinación o un puerto y protocolo. Se utiliza para clasificar el tráfico según el puerto y el protocolo. En las reglas de firewall, pueden utilizarse servicios predefinidos y definidos por el usuario.
Perfil de contexto	Define los atributos con reconocimiento de contexto, incluidos el nombre de dominio y la instancia de APP-ID. También incluye subatributos, como la versión de la aplicación o un conjunto de claves de cifrado. Las reglas de firewall pueden incluir un perfil de contexto para habilitar las reglas de firewall de Capa 7.

Firewall de identidad

Las funciones del firewall de identidad (IDFW) permiten al administrador de NSX crear reglas de firewall distribuido (DFW) basadas en el usuario.

El IDFW se puede usar en escritorios virtuales (VDI) o sesiones de escritorios remotos (soporte de RDSH), lo que permite los inicios de sesión simultáneos de varios usuarios, el acceso de aplicaciones de usuario según ciertos requisitos y la capacidad de mantener los entornos de usuarios independientes. Los sistemas de administración de infraestructura de escritorios virtuales

controlan qué usuarios tienen acceso a las máquinas virtuales de VDI. NSX-T controla el acceso a los servidores de destino de la máquina virtual de origen, que tiene el IDFW habilitado. Con los administradores de RDSH se crean grupos de seguridad con distintos usuarios en Active Directory (AD), y se permite o se deniega a dichos usuarios el acceso a un servidor de aplicaciones en función de su función. Por ejemplo, Recursos Humanos e Ingeniería pueden conectarse al mismo servidor RDSH y tener acceso a diferentes aplicaciones de ese servidor.

IDFW también se puede utilizar en máquinas virtuales con sistemas operativos compatibles. Consulte [Configuraciones admitidas del firewall de identidad](#).

Al preparar la infraestructura comienza una visión general de alto nivel del flujo de trabajo de la configuración de IDFW. Esto incluye que el administrador instale los componentes de preparación del host en cada clúster protegido y que establezca la sincronización de Active Directory de forma que NSX pueda aceptar usuarios y grupos de AD. A continuación, IDFW debe saber en qué escritorio inicia sesión un usuario de Active Directory para poder aplicar las reglas de IDFW. Cuando un usuario genera eventos de red, la instancia de Thin Agent instalada con VMware Tools en la máquina virtual recopila y reenvía la información, y la envía al motor de contexto. Esta información se utiliza para hacer que se cumpla el firewall distribuido.

IDFW procesa la identidad del usuario en el origen únicamente en las reglas de firewall distribuido. Los grupos basados en identidad no se pueden utilizar como destino en las reglas de DFW.

Nota IDFW se basa en la seguridad y la integridad del sistema operativo invitado. Existen varios métodos para que un administrador local malintencionado suplante su identidad para omitir las reglas de firewall. La información de identidad del usuario se proporciona en NSX Guest Introspection Thin Agent dentro de las máquinas virtuales invitadas. Los administradores de seguridad deben asegurarse de que el Thin Agent esté instalado y en ejecución en cada máquina virtual invitada. Los usuarios que iniciaron sesión no deben tener el privilegio para eliminar o detener el agente.

Para conocer las configuraciones de IDFW compatibles, consulte [Configuraciones admitidas del firewall de identidad](#).

Flujo de trabajo de IDFW:

- 1 Un usuario inicia sesión en una máquina virtual e inicia una conexión de red al abrir Skype o Outlook.
- 2 Thin Agent, que recopila información de conexión e información de identidad y la envía al motor de contexto, detecta un evento de inicio de sesión de usuario.
- 3 El motor de contexto reenvía la información de conexión y de identidad al muro del firewall distribuido para hacer cumplir las reglas aplicables.

Flujo de trabajo del firewall de identidad

IDFW mejora el firewall tradicional al permitir reglas de firewall basadas en la identidad del usuario. Por ejemplo, los administradores pueden permitir o prohibir al personal de soporte

técnico del cliente que acceda a una base de datos de Recursos Humanos con una sola directiva de firewall.

Las reglas del firewall basadas en identidad están determinadas por la pertenencia a un grupo Active Directory (AD). Consulte [Configuraciones admitidas del firewall de identidad](#).

IDFW procesa la identidad del usuario en el origen únicamente en las reglas de firewall distribuido. Los grupos basados en identidad no se pueden utilizar como destino en las reglas de DFW.

Nota Para aplicar la regla del firewall de identidad, el servicio hora de Windows debe estar **activado** para todas las máquinas virtuales que utilicen Active Directory. De esta forma, se asegurará de que la fecha y la hora de Active Directory y de las máquinas virtuales estén sincronizadas. Los cambios en la pertenencia al grupo de AD (incluida la habilitación y eliminación de usuarios) no se aplican inmediatamente a los usuarios que hayan iniciado sesión. Para que los cambios se apliquen, los usuarios deben cerrar sesión y volver a iniciarla. Los administradores de AD deben forzar el cierre de sesión cuando se modifique la pertenencia al grupo. Este comportamiento es una limitación de Active Directory.

Requisitos previos

Si el inicio de sesión automático de Windows está habilitado en las máquinas virtuales, vaya a **Directiva de equipo local > Configuración del equipo > Plantillas administrativas > Sistema > Inicio de sesión** y habilite **Esperar siempre a que se inicialice la red en el inicio del equipo y el inicio de sesión**.

Para ver las configuraciones de IDFW admitidas, consulte [Configuraciones admitidas del firewall de identidad](#).

Procedimiento

- 1 Habilite el controlador de introspección de archivos de NSX y el controlador de introspección de red de NSX. La instalación completa de VMware Tools se agrega de forma predeterminada.
- 2 Habilite IDFW en clúster o en un host independiente: [Habilitar firewall de identidad](#).
- 3 Configure el dominio de Active Directory: [Agregar una instancia de Active Directory](#).
- 4 Configure las operaciones de sincronización de Active Directory: [Sincronizar Active Directory](#).
- 5 Cree grupos de seguridad (Security Groups, SG) con los miembros del grupo de Active Directory: [Agregar un grupo](#).
- 6 Asigne SG con miembros del grupo de AD a una regla de firewall distribuido: [Agregar un firewall distribuido](#).

Habilitar firewall de identidad

El firewall de identidad se debe habilitar para que las reglas de firewall de IDFW surtan efecto.

Procedimiento

- 1 Seleccione **Seguridad > Firewall distribuido**.
- 2 En la esquina izquierda, haga clic en **Acciones > Configuración general**.
- 3 Active el botón de estado para habilitar IDFW.
El firewall distribuido también debe estar habilitado para que funcione IDFW.
- 4 Para habilitar IDFW en clústeres o hosts independientes, seleccione la pestaña **Configuración del firewall de identidad**.
- 5 Active o desactive la barra **Habilitar** y seleccione los hosts independientes o seleccione el clúster en el que se debe habilitar el host de IDFW.
- 6 Haga clic en **Guardar**.

Prácticas recomendadas del firewall de identidad

Las siguientes prácticas recomendadas le ayudan a maximizar el resultado de las reglas del firewall de identidad.

- IDFW es compatible con los siguientes protocolos:
 - Soporte para casos prácticos de usuario único (servidor VDI o que no es RDSH): TCP, UDP, ICMP
 - Soporte para casos prácticos de varios usuarios (RDSH): TCP, UDP
- Un único grupo basado en identidad se puede utilizar como origen solo dentro de una regla de firewall distribuido. Si necesita utilizar grupos basados en identificadores y direcciones IP en el origen, cree dos reglas de firewall independientes.
- Todos los cambios que realice en un dominio, incluida la modificación del nombre de dominio, activará una sincronización completa con Active Directory. Como una sincronización completa puede tardar mucho tiempo en completarse, le recomendamos que realice la sincronización fuera de las horas punta o cuando la empresa esté cerrada.
- Para los controladores de dominio locales, los puertos 389 y 636 predeterminados del servidor LDAP se utilizan en la sincronización de Active Directory, y no se deben modificar los valores predeterminados.

Configuraciones admitidas del firewall de identidad

Las siguientes configuraciones son compatibles con IDFW en máquinas virtuales. No se admiten IDFW para dispositivos físicos.

Sistemas operativos invitados	Tipo de implementación
Windows 8	Escritorio: compatible con el caso práctico de usuarios de escritorio
Windows 10	Escritorio: compatible con el caso práctico de usuarios de escritorio
Windows 2012	Servidor: compatible con el caso práctico de usuarios de servidor
Windows 2012R2	Servidor: compatible con el caso práctico de usuarios de servidor
Windows 2016	Servidor: compatible con el caso práctico de usuarios de servidor
Windows 2012R2	RDSH: admite el host de sesión de escritorio remoto
Windows 2016	RDSH: admite el host de sesión de escritorio remoto

Controladores de dominio de Active Directory:

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

Sistema operativo del host: ESXi

VMware Tools: versión 11

- Controlador VMCI
- Controlador de introspección de archivos de NSX
- Controlador de introspección de redes de NSX

Perfil de contexto de Capa 7

Los identificadores de la aplicación de Capa 7 están configurados como parte de un perfil de contexto.

Un perfil de contexto puede especificar uno o más [Atributos](#), y también puede incluir subatributos para usarlos en las reglas de firewall distribuido (DFW) y las reglas de firewall de puerta de enlace. Cuando se define un subatributo, como TLS versión 1.2, no se admiten varios atributos de identidad de aplicación. Además de los atributos, DFW también admite un nombre de dominio completo (FQDN) o una URL que se pueden especificar en un perfil de contexto para la lista blanca o negra de FQDN. Actualmente se admite una lista predefinida de dominios. FQDN se puede configurar con un atributo en un perfil de contexto, o cada uno se puede configurar en distintos perfiles de contexto. Cuando se haya definido un perfil de contexto, este se podrá aplicar a una o varias reglas de firewall distribuido.

Actualmente se admite una lista predefinida de dominios. Puede ver la lista de FQDN cuando agrega un nuevo perfil de contexto del tipo de atributo *Nombre de dominio (FQDN)*. También puede ver una lista de FQDN ejecutando la llamada API `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`.

Nota

- No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace en perfiles de contexto.
- Los perfiles de contexto no se admiten en la directiva de firewall de puerta de enlace de nivel 0. No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace.

Cuando se haya usado un perfil de contexto en una regla, todo el tráfico que provenga de una máquina virtual se comparará con la tabla de reglas basada en cinco tuplas. Si la regla coincide con el flujo, también incluye un perfil de contexto de Capa 7, ese paquete se redireccionará a un componente de espacio de usuario denominado el motor vDPI. Se envía una pequeña cantidad de paquetes posteriores a ese motor vDPI para cada flujo y, una vez que se determina el identificador de aplicación, esta información se almacena en la tabla de contexto del kernel. Cuando entra el siguiente paquete del flujo, la información de la tabla de contexto se compara con la tabla de reglas de nuevo y se hace coincidir con las cinco tuplas y el identificador de aplicación de Capa 7. Se lleva a cabo la acción adecuada que se define en la regla que coincide completamente y, en el caso de una regla de permiso, todos los paquetes posteriores para el flujo se procesan en el kernel y se comparan con la tabla de conexión. Para la regla de colocación de coincidencia completa, se genera un paquete de rechazo. Los registros que genera el firewall incluirán el identificador de aplicación de Capa 7 si ese flujo se envió a DPI.

Procesamiento de reglas para un paquete entrante:

- 1 Al especificar un filtro de puerta de enlace o DFW, se buscan los paquetes en la tabla de flujos basados en cinco tuplas.
- 2 Si no se encuentran flujos ni estados, el flujo coincide con la tabla de reglas basadas en cinco tuplas y se crea una entrada en la tabla de flujos.
- 3 Si el flujo coincide con una regla con un objeto de servicio de Capa 7, el estado de la tabla de flujos se marca como "DPI en curso".
- 4 El tráfico se envía al motor de DPI. El motor de DPI determina el identificador de aplicación.
- 5 Una vez que se determina el identificador de aplicación, el motor de DPI envía el atributo que se inserta en la tabla de contexto para este flujo. Se elimina la marca "DPI en curso" y el tráfico ya no se envía al motor de DPI.
- 6 El flujo (ahora con identificador de aplicación) se vuelve a evaluar con todas las reglas que coincidan con este identificador, a partir de la regla original con la que coincidió basada en cinco tuplas, y se elige la primera regla de Capa 4 o 7 que coincida completamente. Se lleva a cabo la acción apropiada (permitir/denegar/rechazar) y la entrada de la tabla de flujos se actualiza según corresponda.

Flujo de trabajo de reglas de firewall de Capa 7

Los identificadores de aplicaciones de Capa 7 se utilizan para crear perfiles de contexto que se utilizan en reglas de firewall distribuido o de firewall de puerta de enlace. El cumplimiento de reglas basado en atributos permite a los usuarios permitir o denegar que las aplicaciones se ejecuten en cualquier puerto.

NSX-T proporciona [Atributos](#) integrada para las aplicaciones de infraestructura y empresariales más comunes. Los identificadores de aplicaciones incluyen las versiones (SSL/TLS y CIFS/SMB) y el conjunto de claves de cifrado (SSL/TLS). Para un firewall distribuido, los identificadores de aplicaciones se utilizan en las reglas a través de perfiles de contexto, y se pueden combinar con listas blancas y negras de FQDN. Los identificadores de aplicaciones son compatibles con los hosts ESXi y KVM.

Nota

- No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace en perfiles de contexto.
- Los perfiles de contexto no se admiten en la directiva de firewall de puerta de enlace de nivel 0. No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace.

Identificadores de aplicación y FQDN compatibles:

- Para el FQDN, los usuarios deben configurar una regla de prioridad alta con un identificador de aplicación de DNS para los servidores DNS especificados en el puerto 53.
- Los identificadores de aplicación de ALG (FTP, ORACLE, DCERPC y TFTP) requieren el servicio de ALG correspondiente para la regla de firewall.
- El identificador de aplicación de SYSLOG solo se detecta en puertos estándar.

Identificadores de aplicación y FQDN de KVM compatibles:

- Los subatributos no se admiten en KVM.
- Los identificadores de aplicación TFTP y FTP de ALG son compatibles con KVM.

Tenga en cuenta que si utiliza una combinación de Capa 7 y ICMP, o cualquier otro protocolo, deberá colocar las reglas de firewall de capa 7 en último lugar. Las reglas situadas por encima de la regla cualquiera/cualquiera de Capa 7 no se ejecutarán.

Procedimiento

- 1 Cree un perfil de contexto personalizado: [Agregar un perfil de contexto](#).

- 2 Utilice el perfil de contexto en una regla de firewall distribuido o una regla de firewall de puerta de enlace: [Agregar un firewall distribuido](#) o [Agregar una regla y una directiva de firewall de puerta de enlace](#).

Se pueden utilizar varios perfiles de contexto de identificador de aplicación en una regla de firewall con servicios establecidos en **Cualquiera**. Para los perfiles ALG (FTP, ORACLE, DCERPC, TFTP), se admite un perfil de contexto por regla.

Atributos

Los atributos de Capa 7 (identificadores de aplicación) identifican qué aplicación genera un paquete o un flujo específicos, independientemente del puerto que se esté utilizando.

Gracias al cumplimiento en función de los identificadores de aplicación, los usuarios pueden permitir o denegar que las aplicaciones se ejecuten en cualquier puerto, o bien forzar que las aplicaciones se ejecuten en su puerto estándar. El motor vDPI permite comparar la carga útil de paquetes con patrones definidos, comúnmente conocidos como firmas. Con el cumplimiento y la identificación basada en firmas, los clientes no solo pueden hacer coincidir con el protocolo o la aplicación particular a la que pertenece un flujo, sino también la versión de ese protocolo; por ejemplo, TLS versión 1.0, TLS versión 1.2 o diferentes versiones del tráfico de CIFS. De este modo, los clientes obtienen visibilidad en el uso (o lo restringen) de los protocolos que tienen vulnerabilidades conocidas para todas las aplicaciones implementadas y sus flujos de este-oeste dentro del centro de datos.

Los identificadores de aplicación de Capa 7 se utilizan en perfiles de contexto de reglas de firewall distribuido y de firewall de puerta de enlace. Además, son compatibles con los hosts ESXi y de KVM.

Nota La versión 4 de NFS no es un atributo compatible.

Nota

- No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace en perfiles de contexto.
 - Los perfiles de contexto no se admiten en la directiva de firewall de puerta de enlace de nivel 0. No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace.
-

Identificadores de aplicación y FQDN compatibles:

- Para el FQDN, los usuarios deben configurar una regla de prioridad alta con un identificador de aplicación de DNS para los servidores DNS especificados en el puerto 53.
- Los identificadores de aplicación de ALG (FTP, ORACLE, DCERPC y TFTP) requieren el servicio de ALG correspondiente para la regla de firewall.
- El identificador de aplicación de SYSLOG solo se detecta en puertos estándar.

Identificadores de aplicación y FQDN de KVM compatibles:

- Los subatributos no se admiten en KVM.
- Los identificadores de aplicación TFTP y FTP de ALG son compatibles con KVM.

Atributo (identificador de aplicación)	Descripción	Tipo
360ANTIV	360 Safeguard es un programa desarrollado por Qihoo 360, una empresa de TI con sede en China.	Servicios Web
ACTIVDIR	Active Directory de Microsoft	Redes
AMQP	Advanced Messaging Queueing Protocol es un protocolo de capa de aplicación que admite la comunicación a través de mensajes comerciales entre aplicaciones u organizaciones.	Redes
AVAST	Tráfico generado al navegar por Avast.com, el sitio web oficial de Avast! Descargas de antivirus	Servicios Web
AVG	Descarga de software de antivirus/seguridad AVG y sus actualizaciones.	Transferencia de archivos
AVIRA	Descarga de software de antivirus/seguridad Avira y sus actualizaciones.	Transferencia de archivos
BLAST	Un protocolo de acceso remoto que comprime, cifra y codifica experiencias de computación en un centro de datos y las transmite a través de cualquier red IP estándar para escritorios VMware Horizon.	Acceso remoto
BDEFENDER	Descarga de software de antivirus/seguridad BitDefender y sus actualizaciones.	Transferencia de archivos
CA_CERT	La entidad de certificación (CA) emite certificados digitales que certifican la propiedad de una clave pública para el cifrado de mensajes.	Redes
CIFS	El sistema CIFS (Common Internet File System) se utiliza para proporcionar acceso compartido a directorios, archivos, impresoras, puertos serie y diversos tipos de comunicaciones entre los nodos de una red.	Transferencia de archivos
CLDAP	El protocolo ligero de acceso a directorios sin conexión es un protocolo de aplicaciones que se utiliza para acceder a los servicios de información de directorios distribuidos y mantenerlos a través de una red de protocolos de Internet (IP) mediante UDP.	Redes
CTRXCGP	El protocolo común de puerta de enlace de Citrix es un protocolo de aplicaciones que se utiliza para acceder a los servicios de información de directorios distribuidos y mantenerlos a través de una red de protocolos de Internet (IP) mediante UDP.	Base de datos
CTRKGOTO	Alojamiento de Citrix GoToMeeting o sesiones similares basadas en la plataforma GoToMeeting. Incluye las funciones de administración de vídeo, voz y limitación de usuarios.	Colaboración
CTRICA	ICA (Independent Computing Architecture) es un protocolo registrado de un sistema de servidor de aplicaciones diseñado por Citrix Systems.	Acceso remoto

Atributo (identificador de aplicación)	Descripción	Tipo
DCERPC	DCE/RPC es el sistema de llamadas a procedimientos remotos desarrollado para entornos de computación distribuida (DCE).	Redes
DIAMETER	Protocolo de autenticación, autorización y cuentas para redes informáticas.	Redes
DHCP	El protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) es un protocolo que utiliza la administración para distribuir direcciones IP dentro de una red.	Redes
DNS	Consultar un servidor DNS a través de TCP o UDP	Redes
EPIC	EMR Epic es una aplicación de registros médicos electrónicos que ofrece información sobre la salud y el cuidado del paciente.	Servidor de cliente
ESET	Descarga de software de antivirus/seguridad Eset y sus actualizaciones.	Transferencia de archivos
FPROT	Descarga de software de antivirus/seguridad F-Prot y sus actualizaciones.	Transferencia de archivos
FTP	El protocolo FTP (File Transfer Protocol) se utiliza para transferir archivos de un servidor de archivos a una máquina local.	Transferencia de archivos
GITHUB	Git basado en web o repositorio de control de versión y el servicio de hospedaje en Internet.	Colaboración
HTTP	El protocolo HTTP (HyperText Transfer Protocol) es el protocolo de transporte principal de Internet.	Servicios Web
HTTP2	Tráfico generado al navegar por sitios Web compatibles con el protocolo HTTP 2.0.	Servicios Web
IMAP	El protocolo IMAP (Internet Message Access Protocol) es un protocolo estándar de Internet para acceder al correo electrónico en un servidor remoto.	Correo
KASPRSKY	Descarga de software de antivirus/seguridad Kaspersky y sus actualizaciones.	Transferencia de archivos
KERBEROS	Kerberos es un protocolo de autenticación de red diseñado para proporcionar una autenticación segura para las aplicaciones cliente/servidor usando criptografía de clave secreta.	Redes
LDAP	El protocolo LDAP (Lightweight Directory Access Protocol) es un protocolo para leer y modificar los directorios a través de una red IP.	Base de datos
MAXDB	Las consultas y las conexiones de SQL realizadas a un servidor SQL MaxDB.	Base de datos
MCAFEE	Descarga de software de antivirus/seguridad McAfee y sus actualizaciones.	Transferencia de archivos
MSSQL	Microsoft SQL Server es una base de datos relacional.	Base de datos

Atributo (identificador de aplicación)	Descripción	Tipo
NFS	Permite que un usuario en un equipo cliente acceda a archivos a través de una red de forma similar a cómo accedería a un almacenamiento local. Nota La versión 4 de NFS no es un atributo compatible.	Transferencia de archivos
NNTP	Un protocolo de aplicaciones de Internet se utiliza para transportar artículos de noticias en Usenet (netnews) entre servidores de noticias y para que las aplicaciones cliente de usuarios finales puedan leer y publicar artículos.	Transferencia de archivos
NTBIOSNS	Servicio de nombres de NetBIOS. Para poder iniciar las sesiones o distribuir datagramas, una aplicación debe registrar su nombre de NetBIOS mediante el servicio de nombres.	Redes
NTP	El protocolo NTP (Network Time Protocol) se utiliza para sincronizar los relojes de los sistemas informáticos a través de la red.	Redes
OCSP	Respondedor OCSP que verifica que la clave privada de un usuario no se comprometió ni revocó.	Redes
ORACLE	El sistema de gestión de bases de datos objeto-relacional (ORDBMS) diseñada y comercializada por Oracle Corporation.	Base de datos
PANDA	Descarga de software de antivirus/seguridad Panda y sus actualizaciones.	Transferencia de archivos
PCOIP	Un protocolo de acceso remoto que comprime, cifra y codifica experiencias de computación en un centro de datos y las transmite a través de cualquier red IP estándar.	Acceso remoto
POP2	El protocolo POP (Post Office Protocol) es un protocolo utilizado por los clientes de correo electrónico local para recuperar el correo electrónico de un servidor remoto.	Correo
POP3	Implementación de Microsoft del servicio de nombres de NetBIOS (NBNS), un servicio y servidor de nombres para equipos NetBIOS.	Correo
RADIUS	Proporciona gestión centralizada de AAA (autenticación, autorización y contabilidad) para que los equipos se conecten y utilicen un servicio de red.	Redes
RDP	El protocolo RDP (Remote Desktop Protocol) proporciona a los usuarios una interfaz gráfica a otro equipo.	Acceso remoto
RTCP	El protocolo RTCP (Real-Time Transport Control Protocol) es un protocolo del mismo tipo que el protocolo RTP (Real-time Transport Protocol). RTCP proporciona información de control de fuera de banda para un flujo de RTP.	Transmisión multimedia
RTP	El protocolo RTP (Real-Time Transport Protocol) se utiliza principalmente para ofrecer vídeo y audio en tiempo real.	Transmisión multimedia
RTSP	El protocolo RTSP (Real Time Streaming Protocol) se utiliza para establecer y controlar sesiones de medio entre terminales.	Transmisión multimedia

Atributo (identificador de aplicación)	Descripción	Tipo
SIP	El protocolo SIP (Session Initiation Protocol) es un protocolo de control común para configurar y controlar llamadas de voz o vídeo.	Transmisión multimedia
SMTP	El protocolo SMTP (Simple Mail Transfer Protocol) es un estándar de Internet para la transmisión de correo electrónico a través de redes de protocolo de Internet (IP).	Correo
SNMP	El protocolo SNMP (Simple Network Management Protocol) es un protocolo de Internet estándar para gestionar dispositivos en redes IP.	Supervisión de redes
SSH	SSH (Secure Shell) es un protocolo de red que permite que se intercambien datos mediante un canal seguro entre dos dispositivos de la red.	Acceso remoto
SSL	SSL (Secure Sockets Layer) es un protocolo criptográfico que ofrece seguridad a través de Internet.	Servicios Web
SYMUPDAT	Tráfico de Symantec LiveUpdate. Incluye definiciones de programas espía, reglas de firewall, archivos de firmas antivirus y actualizaciones de software.	Transferencia de archivos
SYSLOG	SYSLOG es un protocolo que permite que los dispositivos de red envíen mensajes de eventos a un servidor de registro.	Supervisión de redes
TELNET	Protocolo de red utilizado en las redes de área local o de Internet para proporcionar una instalación de comunicaciones orientadas a texto interactivas o bidireccionales mediante una conexión a un terminal virtual.	Acceso remoto
TFTP	El protocolo TFTP (Trivial File Transfer Protocol) se utiliza para enumerar, descargar y cargar archivos a un servidor TFTP como SolarWinds TFTP Server usando un cliente como WinAgents TFTP.	Transferencia de archivos
VNC	Tráfico de computación virtual de red.	Acceso remoto
WINS	Implementación de Microsoft del servicio de nombres de NetBIOS (NBNS), un servicio y servidor de nombres para equipos NetBIOS.	Redes

Firewall distribuido

El firewall distribuido incluye categorías predefinidas para las reglas de firewall. Las reglas se evalúan de arriba hacia abajo y de izquierda a derecha.

Tabla 10-2. Categorías de reglas de firewall distribuido

Categoría	Descripción
Ethernet	Se utiliza para las reglas basadas en la Capa 2
Emergencia	Se utiliza para la cuarentena y reglas de permiso

Tabla 10-2. Categorías de reglas de firewall distribuido (continuación)

Categoría	Descripción
Infraestructura	Define el acceso a los servicios compartidos. Reglas globales: AD, DNS, NTP, DHCP, copia de seguridad, servidores de administración
Entorno	Reglas entre zonas: producción frente a desarrollo, reglas entre unidades de negocio
Aplicación	Reglas entre aplicaciones, niveles de aplicación o las reglas entre microservicios

Borradores de firewall

Un borrador es una configuración de firewall distribuido completa con reglas y secciones de directivas. Los borradores se pueden guardar automática o manualmente, y pueden publicarse o guardarse inmediatamente para publicarlos más adelante.

Para guardar una configuración de firewall de borrador manual, vaya a la esquina superior derecha de la pantalla Firewall distribuido y haga clic en **Acciones > Guardar**. Para ver la configuración después de guardarla, seleccione **Acciones > Ver**. Los borradores automáticos están habilitados de forma predeterminada. Para deshabilitar los borradores automáticos, vaya a **Acciones > Configuración general**. Si los borradores automáticos están habilitados, cualquier cambio que se realice en una configuración de firewall hará que el sistema genere un borrador automático. Se puede guardar un máximo de 100 borradores automáticos y 10 borradores manuales. Los borradores automáticos se pueden editar y guardar como borradores manuales y se pueden publicar ahora o más adelante. Para evitar que varios usuarios abran y editen un borrador, los borradores manuales se pueden bloquear. Cuando se publica un borrador, la configuración actual se reemplaza por la configuración del borrador.

Guardar o ver el borrador del firewall

Un borrador es una configuración de firewall distribuido publicada o guardada para su publicación posterior. Los borradores se crean automáticamente y de forma manual.

Los borradores manuales se pueden editar y guardar. Los borradores automáticos se pueden clonar y guardar como borradores manuales y, a continuación, editarse. Como máximo se pueden guardar 100 borradores automáticos y 10 borradores manuales.

Procedimiento

- 1 Haga clic en **Seguridad > Firewall distribuido**.
- 2 Para guardar una configuración de firewall manualmente, vaya a **Acciones > Guardar**.
Se puede guardar un borrador manual, editarlo y, a continuación, guardarlo. Después de guardar, puede revertir a la configuración original.
- 3 **Asigne un nombre** a la configuración.

- 4 Para evitar que varios usuarios abran y editen un borrador, seleccione **Bloquear** para bloquear la configuración y agregue un comentario.
- 5 Haga clic en **Guardar**.
- 6 Para ver la configuración guardada, haga clic en **Acciones > Ver**.

Se abre una escala de tiempo donde se muestran todas las configuraciones guardadas. Para ver detalles como el nombre del borrador, la fecha, la hora y quién lo guardó, coloque el cursor en el icono de punto o de estrella de cualquier borrador. Las configuraciones guardadas se pueden filtrar por tiempo para mostrar los borradores creados en el último día, la última semana, los últimos 30 días o los últimos 3 meses. Se pueden filtrar por borrador automático y guardado por mí. También se pueden filtrar por nombre mediante la herramienta de búsqueda situada en la parte superior derecha.

- 7 Coloque el cursor sobre un borrador para ver su nombre y la fecha y hora en las que se guardó la configuración. Haga clic en el nombre para ver los detalles del borrador.

La vista de borrador detallada muestra los cambios que se deben realizar en la configuración del firewall actual para sincronizarse con este borrador. Si este borrador está publicado, todos los cambios visibles en esta vista se aplicarán a la configuración actual.

Al hacer clic en la flecha hacia abajo, se expande cada sección y se muestran los cambios agregados, modificados y eliminados en cada sección. La comparación muestra las reglas agregadas con una barra verde en el lado izquierdo del cuadro, los elementos modificados (como un cambio de nombre) con una barra amarilla, y los elementos eliminados con una barra roja.

- 8 Para editar el nombre o la descripción de un borrador seleccionado, haga clic en el icono de menú (tres puntos) de la ventana **Ver detalles del borrador** y seleccione **Editar**.

Los borradores manuales se pueden bloquear. Si lo bloquea, deberá introducir un comentario para el borrador.

Algunas funciones, como el administrador empresarial, tienen credenciales de acceso completo y no se pueden bloquear. Consulte [Control de acceso basado en funciones](#).

- 9 Los borradores automáticos y los borradores manuales también se pueden clonar y guardar haciendo clic en **Clonar**.

En la ventana Configuraciones guardadas, puede aceptar el nombre predeterminado o editarlo. También puede bloquear la configuración. Si lo bloquea, deberá introducir un comentario para el borrador.

- 10 Para guardar la versión clonada de la configuración del borrador, haga clic en **Guardar**. El borrador ahora está disponible en la sección Configuraciones guardadas.

Pasos siguientes

Después de ver un borrador, puede cargarlo y publicarlo. A continuación, este pasará a ser la configuración del firewall activo.

Publicar o revertir un borrador de firewall

Tanto los borradores automáticos como los borradores manuales guardados pueden cargarse y publicarse para convertirse en la configuración activa.

Durante la publicación, se crea un nuevo borrador automático. Este borrador automático se puede publicar para volver a la configuración anterior.

Procedimiento

- 1 Para ver la configuración guardada, haga clic en **Acciones > Ver**.

Se abre una escala de tiempo donde se muestran todas las configuraciones guardadas. Para ver detalles como el nombre del borrador, la fecha, la hora y quién lo guardó, coloque el cursor en el icono de punto de cualquier borrador. Las configuraciones guardadas se filtran por hora, mostrando todos los borradores creados en un periodo de 1 día, 1 semana, 30 días o 3 meses.

- 2 Si hace clic en el nombre de un borrador, se abrirá la ventana Ver detalles del borrador.
- 3 Haga clic en **Cargar**. La nueva configuración del firewall se muestra en la ventana principal.

Nota No se puede cargar un borrador si se están utilizando filtros de firewall o si hay cambios sin guardar en la configuración actual.

- 4 Para confirmar la configuración del borrador y activarla, haga clic en **Publicar**. Para volver a la configuración publicada anterior, haga clic en **Revertir**.

Después de publicarlo, los cambios del borrador se aplicarán a la configuración activa.

- 5 Para editar el contenido del borrador seleccionado antes de publicarlo, edite la configuración después de hacer clic en **Cargar**.
- 6 Para guardar la versión editada de la configuración del borrador, haga clic en **Acciones > Guardar**.

Los borradores manuales se pueden guardar como una nueva configuración o una actualización de la configuración actual. Los borradores automáticos solo se pueden guardar como una nueva configuración.

- 7 Rellene el campo **Nombre** y, de forma opcional, el campo **Descripción**. También puede **Bloquear** el borrador. Si lo bloquea, deberá introducir un comentario para el borrador.
- 8 Haga clic en **Guardar**.
- 9 Para confirmar la configuración del borrador y activarla, haga clic en **Publicar**. En cambio, si desea volver a la configuración anterior, haga clic en **Revertir**.

Agregar un firewall distribuido

El firewall distribuido (DWF) supervisa todo el tráfico de este a oeste en las máquinas virtuales.

Requisitos previos

Para que las máquinas virtuales invitadas estén protegidas por DFW, deben estar conectadas a un conmutador lógico de N-VDS asociado a una zona de transporte.

Si se dispone a crear reglas para el firewall de identidad, primero cree un grupo con miembros de Active Directory. IDFW solo admite reglas de firewall basadas en TCP.

Nota Para aplicar la regla del firewall de identidad, el servicio hora de Windows debe estar **activado** para todas las máquinas virtuales que utilicen Active Directory. De esta forma, se asegurará de que la fecha y la hora de Active Directory y de las máquinas virtuales estén sincronizadas. Los cambios en la pertenencia al grupo de AD (incluida la habilitación y eliminación de usuarios) no se aplican inmediatamente a los usuarios que hayan iniciado sesión. Para que los cambios se apliquen, los usuarios deben cerrar sesión y volver a iniciarla. Los administradores de AD deben forzar el cierre de sesión cuando se modifique la pertenencia al grupo. Este comportamiento es una limitación de Active Directory.

Tenga en cuenta que si utiliza una combinación de Capa 7 y ICMP, o cualquier otro protocolo, deberá colocar las reglas de firewall de capa 7 en último lugar. Las reglas situadas por encima de la regla cualquiera/cualquiera de Capa 7 no se ejecutarán.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Seguridad > Firewall distribuido** en el panel de navegación.
- 3 Habilite el firewall distribuido. Para ello, seleccione **Acciones > Configuración general** y active el Estado de Firewall distribuido. Haga clic en **Guardar**.
- 4 Compruebe que se encuentra en la categoría predefinida correcta y haga clic en **Agregar directiva**. Para obtener más información sobre las categorías, consulte [Firewall distribuido](#).
- 5 En **Nombre**, escriba un nombre para la nueva sección de directiva.

- 6 (opcional) Para configurar los siguientes ajustes de directiva, haga clic en el icono de rueda dentada:

Opción	Descripción
TCP estricto	<p>Una conexión TCP comienza con un protocolo de enlace de tres vías (SYN, SYN-ACK y ACK) y, por lo general, termina con un intercambio de dos vías (FIN y ACK). En determinadas circunstancias, es posible que el firewall distribuido (Distributed firewall, DFW) no vea el protocolo de enlace de tres vías para un flujo concreto (por ejemplo, porque el tráfico asimétrico o el firewall distribuido están habilitados mientras existe un flujo). De forma predeterminada, el DFW no exige ver un protocolo de enlace de tres vías y recoge sesiones que ya están establecidas. TCP estricto se puede habilitar en cada sección para desactivar la recogida de sesiones medias y exigir el requisito de un protocolo de enlace de tres vías.</p> <p>Cuando se habilita el modo TCP estricto para una determinada directiva de DFW y se utiliza una regla de bloqueo ANY-ANY predeterminada, se descartan los paquetes que no cumplan todos los requisitos de conexión de protocolo de tres vías y que coincidan con una regla basada en TCP de esta sección. El modo TCP estricto solo se aplica a las reglas de TCP con estado y se habilita en el nivel de la sección de firewall distribuido. TCP estricto no se aplica a los paquetes que coinciden con el permiso ANY-ANY predeterminado, sin especificar ningún servicio TCP.</p>
Con estado	<p>Un firewall con estado supervisa el estado de las conexiones activas y utiliza esta información para determinar a qué paquetes se les permite atravesar el firewall.</p>
Bloqueado	<p>La directiva se puede bloquear para impedir que varios usuarios editen las mismas secciones. Cuando bloquea una sección, debe incluir un comentario.</p> <p>Algunas funciones, como administrador empresarial, tienen credenciales de acceso completo y no se pueden bloquear. Consulte Control de acceso basado en funciones.</p>

- 7 Haga clic en **Publicar**. Se pueden agregar varias directivas y, a continuación, publicarlas al mismo tiempo.

La nueva directiva se muestra en la pantalla.

- 8 Seleccione una sección de directiva y haga clic en **Agregar regla**.
- 9 Introduzca un nombre para la regla.

- 10 En la columna **Orígenes**, haga clic en el icono de edición y seleccione el origen de la regla. Para el campo de origen de una regla de IDFW, se pueden usar grupos con miembros de Active Directory. Consulte [Agregar un grupo](#) para obtener más información.

Se admiten direcciones IPv4, IPv6 y de multidifusión.

Nota: El firewall IPv6 debe tener habilitada la detección de direcciones IP para IPv6 en un segmento conectado. Para obtener más información, consulte [Información sobre el perfil de segmentos de detección de direcciones IP](#).

- 11 En la columna **Destinos**, haga clic en el icono de edición y seleccione el destino de la regla. Si no está definido, el destino coincidirá con **Cualquiera**. Consulte [Agregar un grupo](#) para obtener más información. Se admiten direcciones IPv4, IPv6 y de multidifusión.
- 12 En la columna **Servicios**, haga clic en el icono de edición y seleccione los servicios. Si no está definido, el servicio coincidirá con **cualquiera**.
- 13 La columna **Perfiles** no está disponible cuando se agrega una regla a la categoría Ethernet. Para todas las demás categorías de regla, en la columna **Perfiles**, haga clic en el icono de edición y seleccione un perfil de contexto, o bien haga clic en **Agregar nuevo perfil de contexto**. Consulte [Agregar un perfil de contexto](#).

Los perfiles de contexto usan atributos de identificador de aplicación de Capa 7 para emplearlos en reglas de firewall distribuido y reglas de firewall de puerta de enlace. Se pueden utilizar varios perfiles de contexto de identificador de aplicación en una regla de firewall con servicios establecidos en **Cualquiera**. Para los perfiles ALG (FTP y TFTP), se admite un perfil de contexto por regla.

- 14 Haga clic en **Aplicar** para hacer efectivo el perfil de contexto en la regla.
- 15 De forma predeterminada, la columna **Se aplica a** se establece como DFW y la regla se aplica en todas las cargas de trabajo. También puede aplicar la regla o la política a grupos seleccionados. **Se aplica a** define el alcance de la implementación por regla, y se utiliza principalmente para la optimización o los recursos en hosts ESXi y KVM. Esto ayuda a definir una directiva dirigida para zonas y tenants específicos sin interferir con otra directiva definida para otros tenants y zonas.

Los grupos que constan únicamente de direcciones IP, direcciones MAC o grupos de Active Directory no se pueden utilizar en el cuadro de texto **Se aplica a**.

- 16 En la columna **Acción**, seleccione una acción.

Opción	Descripción
Permitir	Permite el acceso directo de todo el tráfico de Capa 3 y Capa 2 con el origen, destino y protocolo especificados a través del contexto de firewall presente. Los paquetes que coincidan con la regla y se acepten atraviesan el sistema como si el firewall no estuviese presente.
Quitar	Descarta paquetes con el origen, destino y protocolo especificados. Descartar un paquete es una acción silenciosa que no envía ninguna notificación a los sistemas de origen y de destino. Al descartar el paquete, se intentará recuperar la conexión hasta que se alcance el umbral de reintentos.
Rechazar	Rechaza paquetes con el origen, destino y protocolo especificados. Rechazar un paquete es una manera más estable para denegarlo, ya que envía un mensaje de destino no alcanzable al remitente. Si el protocolo es TCP, se envía un mensaje TCP RST. Se envían mensajes ICMP con código prohibido de forma administrativa para conexiones UDP, ICMP y otras conexiones IP. Una ventaja de utilizar la opción Rechazar es que la aplicación que envía el mensaje recibe una notificación después de que se produzca un único intento de establecer conexión sin éxito.

- 17 Haga clic en el botón de alternancia de estado para habilitar o deshabilitar la regla.
- 18 (opcional) Haga clic en el icono de engranaje para configurar las siguientes opciones de regla:

Opción	Descripción
Registro	El registro se desactiva de forma predeterminada. Los registros se almacenan en el archivo /var/log/dfwpktlogs.log en los hosts ESXi y KVM.
Dirección	Hace referencia a la dirección del tráfico desde el punto de vista del objeto de destino. ENTRADA significa que solo se comprueba el tráfico que entra al objeto, SALIDA significa que solo se comprueba el tráfico que sale del objeto y Entrada/salida significa que se comprueba el tráfico en ambas direcciones.
Protocolo IP	Aplique la regla basada en IPv4, IPv6 o tanto en IPv4 como en IPv6.
Etiqueta de registro	La etiqueta de registro se incluye en el registro del firewall cuando el registro está habilitado.

- 19 Haga clic en **Publicar**. Se pueden agregar varias reglas y, a continuación, publicarlas al mismo tiempo.
- 20 En cada regla, haga clic en el icono de **información** para ver el número de identificador de regla y dónde se aplica.

Este icono aparecerá atenuado hasta que publique la regla. También puede especificar un identificador de regla al hacer clic en el icono de filtro para mostrar solo las directivas y las reglas que cumplan los criterios de filtro.

- 21 La API del estado de realización se ha mejorado en lo que respecta a las directivas de seguridad para proporcionar información adicional sobre el estado de realización. Para conseguirlo, especifique el parámetro de consulta *include_enforced_status=true* junto con *intent_path*. Haga la siguiente llamada API.

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/
infra/domains/default/security-policies/<security-policy-
id>&include_enforced_status=true
```

Registros de paquetes de firewall distribuido

Si se habilita el registro de reglas de firewall, puede consultar los registros de paquetes de firewall para solucionar los problemas.

El archivo de registro es `/var/log/dfwpktlogs.log` para los hosts ESXi y de KVM.

A continuación se muestra un ejemplo de registro regular para las reglas de firewall distribuido:

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainrs/1024 IN 52 TCP 192.168.4.3/49627-
>192.168.4.4/49153 SEW

2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainrs/1024 OUT 52 TCP 192.168.4.3/49676-
>192.168.4.4/135 SEW

2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1

2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP
fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:1:2/547
```

Los elementos de un formato de archivo de registro de DFW incluyen los siguientes (separados por un espacio):

- marca de tiempo:
- últimos ocho dígitos del identificador de VIF de la interfaz
- Tipo de INET (v4 o v6)
- motivo (coincidencia)
- acción (PASS, DROP, REJECT)
- nombre de conjunto de reglas/ID de regla
- dirección del paquete (IN/OUT)
- tamaño del paquete
- protocolo (TCP, UDP o PROTO #)
- dirección de SVM para el acierto de regla de NETX
- dirección IP de origen/puerto de origen>dirección IP de destino/puerto de destino
- marcas TCP (SEW)

Para los paquetes TCP pasados, hay un registro de terminación cuando finaliza la sesión:

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

Los elementos de un registro de terminación de TCP incluyen los siguientes (separados por un espacio):

- marca de tiempo:
- últimos 8 dígitos del identificador de VIF de la interfaz
- Tipo de INET (v4 o v6)
- acción (TERM)
- nombre de conjunto de reglas/ID de regla
- dirección del paquete (IN/OUT)
- protocolo (TCP, UDP o PROTO #)
- marca RST de TCP
- dirección de SVM para el acierto de regla de NETX
- dirección IP de origen/puerto de origen>dirección IP de destino/puerto de destino
- número de paquetes de salida o entrada (todos acumulados)
- tamaño de paquete de salida o de entrada

A continuación se muestra un ejemplo de archivo de registro de FQDN para las reglas de firewall distribuido:

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

Los elementos de un registro de FQDN incluyen los siguientes (separados por un espacio):

- marca de tiempo:
- últimos ocho dígitos del identificador de VIF de la interfaz
- Tipo de INET (v4 o v6)
- motivo (coincidencia)
- acción (PASS, DROP, REJECT)
- nombre de conjunto de reglas/ID de regla
- dirección del paquete (IN/OUT)
- tamaño del paquete
- protocolo (TCP, UDP o PROTO #)
- dirección IP de origen/puerto de origen>dirección IP de destino/puerto de destino

- nombre de dominio/UUID donde UUID es la representación interna binaria del nombre de dominio

A continuación se muestra un ejemplo de archivo de registro de capa 7 para las reglas de firewall distribuido:

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

Los elementos de un registro de capa 7 incluyen los siguientes (separados por un espacio):

- marca de tiempo:
- últimos ocho dígitos del identificador de VIF de la interfaz
- Tipo de INET (v4 o v6)
- motivo (coincidencia)
- acción (PASS, DROP, REJECT)
- nombre de conjunto de reglas/ID de regla
- dirección del paquete (IN/OUT)
- tamaño del paquete
- protocolo (TCP, UDP o PROTO #)
- dirección IP de origen/puerto de origen>dirección IP de destino/puerto de destino
- APP_XXX es la aplicación detectada

Seleccionar una estrategia de conectividad predeterminada

Es posible seleccionar una estrategia de conectividad predeterminada para aplicar el modelo de seguridad.

La estrategia de conectividad predeterminada crea una directiva de firewall en la que se permite todo (lista negra) o una en la que se deniega todo (lista blanca) que prevalecen sobre las otras reglas de firewall que cree, en lugar de tener que modificar reglas individuales. Para establecer una estrategia de conectividad predeterminada, vaya a **Firewall distribuido**. En la parte superior de la página, haga clic en el estado de conectividad para seleccionar otra opción.

Las reglas y la directiva de firewall ya se deben haber creado para cambiar la estrategia de conectividad seleccionada predeterminada y hacer que se aplique inmediatamente. Si no se crea ninguna directiva ni regla, la estrategia de conectividad predeterminada permanecerá hasta que se creen una directiva y reglas.

Las siguientes opciones están disponibles:

- **Lista negra (con o sin registro):** esta es la opción predeterminada y crea una regla en la que se permite todo en el DFW.

- **Lista blanca (con o sin registro):** crea una regla de firewall de denegación de todo el tráfico. Solo se permite la comunicación de sitios o aplicaciones que se hayan definido en reglas de firewall, y se deniega el acceso a las demás comunicaciones, incluido el tráfico DHCP.
- **Ninguna:** seleccione esta opción para deshabilitar tanto las listas negras como las listas blancas de las reglas de firewall. Esta opción resulta útil si tiene un conjunto de reglas ya configuradas que usan versiones anteriores de NSX-T Data Center.

Administrar una lista de exclusión de firewall

Las listas de exclusión de firewall se componen de grupos que se pueden excluir de una regla de firewall basada en la pertenencia a grupos.

Los grupos se pueden excluir de las reglas de firewall, pudiendo incluir en la lista un máximo de 100 grupos. Los conjuntos de direcciones IP, los conjuntos de direcciones MAC y los grupos de AD no se pueden incluir como miembros de un grupo que se utiliza en una lista de exclusión de firewall.

Nota NSX-T Data Center agrega automáticamente las máquinas virtuales del nodo de NSX Manager y NSX Edge a la lista de exclusión del firewall.

Procedimiento

- 1 Desplácese hasta **Seguridad > Firewall distribuido > Acciones > Lista de exclusión**.
Aparece una ventana con una lista de los grupos disponibles.
- 2 Para agregar un grupo a la lista de exclusión, haga clic en la casilla de verificación situada junto a cualquier grupo. A continuación, haga clic en **Aplicar**.
- 3 Para crear un grupo, haga clic en **Agregar grupo**. Consulte [Agregar un grupo](#).
- 4 Para editar un grupo, haga clic en el menú de tres puntos situado junto a un grupo y seleccione **Editar**.
- 5 Para eliminar un grupo, haga clic en el menú de tres puntos y seleccione **Eliminar**.
- 6 Para mostrar los detalles del grupo, haga clic en **Expandir todo**.

Filtrar dominios específicos (FQDN/URL)

Configure una regla de firewall distribuido para filtrar dominios específicos identificados con FQDN o URL (por ejemplo, **.office365.com*).

Actualmente se admite una lista predefinida de dominios. Puede ver la lista de FQDN cuando agrega un nuevo perfil de contexto del tipo de atributo *Nombre de dominio (FQDN)*. También puede ver una lista de FQDN ejecutando la llamada API `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`.

Primero debe configurar una regla DNS y, a continuación, la regla de adición a la lista de permitidos o no permitidos de FQDN debajo de ella. NSX-T Data Center usa el tiempo de vida (TTL) en la respuesta de DNS (que proviene del servidor DNS a la máquina virtual) para mantener la entrada de memoria caché de asignación de DNS a IP para la máquina virtual. Para anular el TTL de DNS mediante un perfil de seguridad de DNS, consulte [Configurar la seguridad de DNS](#). Para que el filtrado de FQDN sea efectivo, las máquinas virtuales deben utilizar un servidor DNS para la resolución de dominio (sin entradas de DNS estáticas) y también deben respetar el TTL recibido en la respuesta de DNS. NSX-T Data Center utiliza la intromisión de DNS para obtener una asignación entre la dirección IP y el FQDN. SpoofGuard debe habilitarse en todo el conmutador de todos los puertos lógicos para protegerse frente al riesgo de ataques de suplantación de DNS. Un ataque de suplantación de DNS consiste en que una máquina virtual malintencionada inyecta respuestas de DNS falsas para redireccionar el tráfico a endpoints malintencionados o evitar el firewall. Para obtener más información sobre SpoofGuard, consulte [Información sobre el perfil de segmentos de Spoofguard](#).

Esta función opera en la capa 7 y no incluye ICMP. Si un usuario crea una regla de lista de denegación para todos los servicios de `example.com`, la función está operando de la manera prevista si el ping `example.com` responde, pero `curl example.com` no.

Una práctica recomendada es seleccionar un FQDN comodín, ya que incluye subdominios. Por ejemplo, si selecciona `*example.com`, se incluirán subdominios, como `americas.example.com` y `emea.example.com`. Si usa `example.com`, no se incluirá ningún subdominio.

Las reglas basadas en FQDN se conservan durante vMotion para los hosts ESXi.

Nota Se admiten los hosts ESXi y KVM. Los hosts de KVM solo admiten la lista de permitidos de FQDN. El filtrado de FQDN solo está disponible con el tráfico TCP y UDP.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Vaya a **Seguridad > Firewall distribuido**.
- 3 Agregue una sección de directiva de firewall siguiendo los pasos que se describen en [Agregar un firewall distribuido](#). También se puede utilizar una sección de directiva de firewall existente.
- 4 Elija la sección de directiva de firewall nueva o una ya existente, y haga clic en **Agregar regla** para crear primero la regla de firewall DNS.

- 5 Proporcione un nombre para la regla de firewall, como **Regla DNS**, y proporcione los siguientes detalles:

Opción	Descripción
Servicios	Haga clic en el icono de edición y seleccione el servicio de DNS o DNS-UDP según corresponda en su entorno.
Perfil	Haga clic en el icono de edición y seleccione el perfil de contexto de DNS. Este se crea previamente y está disponible en la implementación de forma predeterminada.
Se aplica a	Seleccione un grupo según corresponda.
Acción	Seleccione Permitir .

- 6 Vuelva a hacer clic en **Agregar regla** para configurar la regla de adición a la lista de permitidos o no permitidos de FQDN.
- 7 Asigne un nombre correcto a la regla, como **Lista de permitidos de FQDN/URL**. Arrastre la regla debajo de la regla DNS en esta sección de directiva.
- 8 Proporcione los siguientes detalles:

Opción	Descripción
Servicios	Haga clic en el icono de edición y seleccione el servicio que desea asociar con esta regla (por ejemplo, HTTP).
Perfil	Haga clic en el icono de edición y en Agregar nuevo perfil de contexto . Haga clic en la columna denominada Atributo y seleccione Nombre de dominio (FQDN) . Seleccione la lista de nombres o valores de atributos de la lista predefinida. Haga clic en Agregar . Consulte Agregar un perfil de contexto para obtener detalles.
Se aplica a	Seleccione DFW o un grupo según corresponda.
Acción	Seleccione Permitir , Anular o Rechazar .

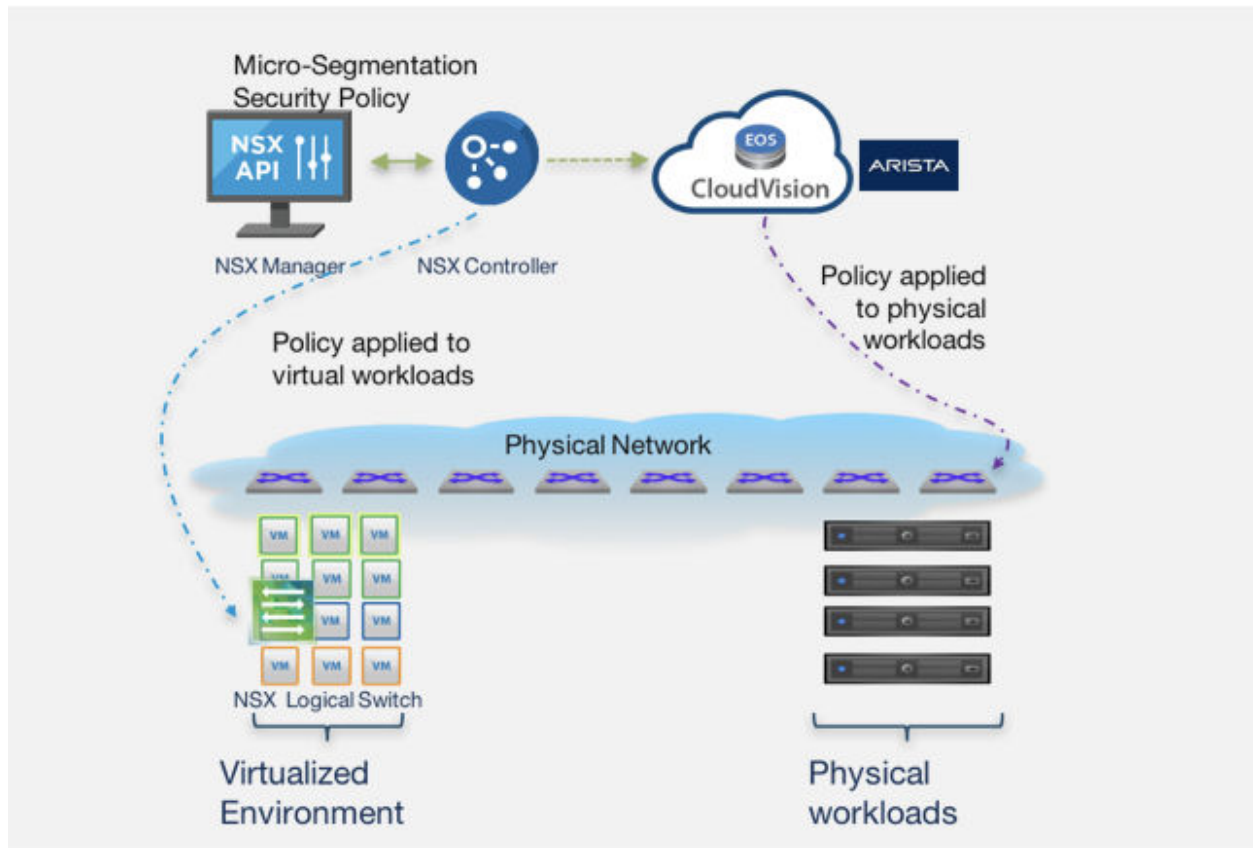
- 9 Haga clic en **Publicar**.

Ampliar las directivas de seguridad a las cargas de trabajo físicas

NSX-T Data Center puede actuar como un único punto de administración para las cargas de trabajo virtuales y físicas.

A partir de NSX-T Data Center 2.5.1, se admite la integración con Arista CloudVision eXchange (CVX). Esta integración facilita los servicios de redes y seguridad coherentes en las cargas de trabajo virtuales y físicas, independientemente de los marcos de aplicaciones o de la infraestructura de red física. NSX-T Data Center no programa directamente el conmutador de red física ni el enrutador, sino que se integra en el nivel del controlador de SDN física, lo que permite conservar la autonomía de los administradores de seguridad y de la red física.

A partir de NSX-T Data Center 2.5.1, se admite la integración con Arista EOS 4.22.1FX-PCS y versiones posteriores.



Limitaciones

- Los conmutadores Arista requieren que el tráfico ARP exista antes de que se apliquen las reglas de firewall a un host final que esté conectado a un conmutador Arista. Por lo tanto, los paquetes pueden pasar a través del conmutador antes de que las reglas de firewall estén configuradas para bloquear el tráfico.
- El tráfico permitido no se reanuda cuando un conmutador se bloquea o se vuelve a cargar. Es necesario volver a rellenar las tablas de ARP una vez que se enciende el conmutador para que se apliquen las reglas de firewall en el conmutador.
- No se pueden aplicar reglas de firewall en el conmutador físico Arista para clientes FTP pasivos que se conectan al servidor FTP conectado al conmutador físico Arista.
- En la configuración de CVX HA que utiliza una IP virtual para el clúster de CVX, el modo promiscuo de DVPD de la máquina virtual de CVX y las transmisiones falsificadas deben estar configuradas para aceptarse. En caso de que se establezcan en valores predeterminados (Rechazar), no se podrá acceder a la IP virtual de CVX HA desde NSX Manager.

Configurar Arista CVX para que interactúe con NSX-T Manager

Después de configurar NSX-T Data Center, complete el procedimiento de configuración en Arista CloudVision eXchange (CVX) para permitir que CVX interactúe con NSX-T Data Center.

Requisitos previos

NSX-T Data Center registró CVX como punto de implementación.

Procedimiento

- 1 Inicie sesión en NSX Manager como usuario root y ejecute el siguiente comando para crear una huella digital que permita que CVX se comuniquen con NSX Manager:

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

Resultados de muestra:

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 Ejecute el siguiente comando desde la CLI de CVX:

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 Ejecute el siguiente comando desde la CLI de CVX para comprobar la configuración:

```
show running-config
```

Resultado de muestra:

```
cvx
    no shutdown
    source-interface Management1
    !
    service hsc
        no shutdown
    !
    service pcs
        no shutdown
        controller 192.168.2.80
```

```
username admin
password 7 046D26110E33491F482F2800131909556B
enforcement-point cvx-default-ep
pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
notification-id a0286cb6-de4d-41de-99a0-294465345b80
```

- Configure tag en la interfaz Ethernet del conmutador físico que se conecta al servidor físico. Ejecute los siguientes comandos en el conmutador físico administrado por CVX.

```
configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.
```

- Ejecute el siguiente comando para comprobar la configuración de etiquetas del conmutador:

```
show running-config section tag
```

Resultados de muestra:

```
interface Ethernet4
description connected-to-7150s-3
switchport trunk allowed vlan 1-4093
switchport mode trunk
tag sx4_app_server
```

Las direcciones IP que se obtienen en las interfaces etiquetadas mediante ARP se comparten con NSX-T Data Center.

- Inicie sesión en NSX Manager para crear y publicar reglas de firewall para las cargas de trabajo físicas administradas por CVX. Consulte [Capítulo 10 Seguridad](#) para obtener más información sobre la creación de reglas. Por ejemplo:

+ AGREGAR DIRECTIVA + AGREGAR REGLA CLONAR DESHACER ELIMINAR ...								
	Nombre	Orígenes	Destinos	Servicios	Perfiles	Se aplica a	Acción	
⋮	Firewall_Services	(2)	Se aplica a	DFW			● Activo	ⓘ ⚙
⋮	vm_to_phy_server	① 55 vm	55 phy_server	Cualquiera	Ninguno	DFW	● Permitir	ⓘ ⚙
⋮	phy_server_to_vm	① 55 phy_server	55 vm	Cualquiera	Ninguno	DFW	● Permitir	ⓘ ⚙

Las directivas y reglas de NSX-T Data Center publicadas en NSX-T Data Center aparecen como ACL dinámicas en el conmutador físico administrado por CVX.

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
    10 permit ip host 71.1.1.3 host 27.1.1.11

IP Access List et4.v4.out [dynamic]
    10 permit ip host 27.1.1.11 host 71.1.1.3
```

Para obtener más información, consulte [Configuración de HA de CVX](#), [Configuración de IP virtual de HA de CVX](#) y [Configuración de Mlag del conmutador físico](#)

Configurar NSX-T Data Center para que interactúe con arista CVX

Complete el procedimiento de configuración en NSX-T Data Center para que CVX se pueda agregar como punto de implementación en NSX-T Data Center y NSX-T Data Center pueda interactuar con CVX.

Requisitos previos

Obtenga la dirección IP virtual del clúster de Arista CVX.

Procedimiento

- 1 Inicie sesión en NSX Manager como usuario root y ejecute el siguiente comando para recuperar la huella digital de CVX:

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

Resultados de muestra:

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 Edite la huella digital recuperada para utilizar solo caracteres en minúscula y excluir los dos puntos de la huella digital.

Muestra de la huella digital editada para CVX:

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 Llame a la API PATCH** /policy/api/v1/infra/sites/default/enforcement-points y use la huella digital de CVX para crear un endpoint de aplicación para CVX. Por ejemplo:

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 Llame a la API GET** /policy/api/v1/infra/sites/default/enforcement-points para recuperar la información del endpoint. Por ejemplo:

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "admin",
    "password": "1q2w3e4rT",
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
  }
}
```

Resultados de muestra:

```
{
  "connection_info": {
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
    "enforcement_point_address": "192.168.2.198",
    "resource_type": "CvxConnectionInfo"
  },
  "auto_enforce": false,
  "resource_type": "EnforcementPoint",
  "id": "cvx-default-ep",
  "display_name": "cvx-default-ep",
  "path": "/infra/sites/default/enforcement-points/cvx-default-ep",
  "relative_path": "cvx-default-ep",
  "parent_path": "/infra/sites/default",
  "marked_for_delete": false,
  "_system_owned": false,
  "_create_user": "admin",
  "_create_time": 1564036461953,
  "_last_modified_user": "admin",
}
```

```
{
  "_last_modified_time": 1564036461953,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

- 5 Llame a la API POST /api/v1/notification-watchers/ y utilice la huella digital de CVX para crear un identificador de notificación. Por ejemplo:

```
POST https://<nsx-manager>/api/v1/notification-watchers/
{
  "server": "<virtual IP address of CVX cluster>",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin",
    "password": "1q2w3e4rT"
  }
}
```

- 6 Llame a GET /api/v1/notification-watchers/ para recuperar el identificador de notificación.

Resultados de muestra:

```
{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
  "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
  "_create_user": "admin",
  "_create_time": 1564038044780,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564038044780,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```


- 7 Llame a la API `PATCH /policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap` para crear un mapa de implementación de dominio de CVX. Por ejemplo:

```
PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap
{

  "display_name": "cvx-deployment-map",

  "id": "cvx-default-dmap",

  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"

}
```

- 8 Llame a la API `GET /policy/api/v1/infra/domains/default/domain-deployment-maps` para recuperar la información del mapa de implementación.

Conjuntos de direcciones compartidas

Los grupos de seguridad basados en objetos dinámicos o lógicos pueden crearse y utilizarse en el cuadro de texto **Se aplica a** de las reglas de firewall distribuido.

Debido a que los conjuntos de direcciones se rellenan de forma dinámica según el nombre de la máquina virtual o las etiquetas y se deben actualizar en cada filtro, pueden agotar la memoria de pila disponible en los hosts para almacenar las reglas de DFW y los conjuntos de direcciones IP.

En NSX-T Data Center 2.5 y versiones posteriores, una función denominada conjuntos de direcciones compartidas o globales hace que los conjuntos de direcciones se compartan entre todos los filtros. Aunque cada filtro puede tener diferentes reglas según la configuración de **Se aplica a**, los miembros de los conjuntos de direcciones son constantes en todos los filtros. Esta función está habilitada de forma predeterminada, lo que reduce el uso de la memoria de pila. No se puede deshabilitar.

En NSX-T Data Center 2.4 y versiones anteriores, los conjuntos de direcciones globales o compartidas están deshabilitados, y los entornos con una gran cantidad de reglas de firewall distribuido pueden experimentar un agotamiento de pila de VSIP.

Seguridad de red de este a oeste: cadena de servicios de terceros

Después de que los partners registran servicios de red —como el sistema de detección de intrusiones o el sistema de protección contra intrusiones (Intrusion Detection System/Intrusion Protection System, IDS/IPS)— en NSX-T Data Center, como administrador puede configurar los servicios de red para realizar la introspección del tráfico de este a oeste que circula entre las máquinas virtuales en un centro de datos local.

Requisitos previos

- Los partners deben registrar los servicios con NSX-T Data Center.
- Los hosts ESXi deben estar preparados como nodos de transporte de NSX-T Data Center usando perfiles de nodo de transporte.

Nota

- Las máquinas virtuales de servicio solo se admiten en hosts ESXi y no en hosts KVM.
 - NSX-T Data Center solo protege las máquinas virtuales invitadas que se ejecutan en hosts ESXi.
 - NSX-T Data Center no protege las máquinas virtuales invitadas que se ejecutan en hosts KVM.
-

Conceptos clave de la protección de red de Este a Oeste

El tráfico que circula entre las máquinas virtuales invitadas en un centro de datos local está protegido por los servicios de terceros que proporcionan los partners. Hay algunos conceptos que le permitirán comprender mejor el flujo de trabajo.

- Servicio: los partners registran los servicios con NSX-T Data Center. Un servicio representa la funcionalidad de seguridad proporcionada por el partner, incluidos los detalles de implementación del servicio, como la dirección URL de OVF de las máquinas virtuales de servicio, el punto para asociar el servicio y el estado del servicio.
- Plantilla de proveedor: consiste en la funcionalidad que puede realizar un servicio en el tráfico de red. Los partners definen las plantillas de proveedor. Por ejemplo, una plantilla de proveedor puede ofrecer un servicio de operación de red, como proporcionar un túnel con el servicio IPSec.
- Perfil de servicio: es una instancia de una plantilla de proveedor. Un administrador de NSX-T Data Center puede crear un perfil de servicio que consumirán las máquinas virtuales de servicio.
- Máquina virtual invitada: el origen o el destino del tráfico en la red. El tráfico entrante o saliente se inspecciona internamente mediante una cadena de servicios definida para una regla que ejecuta servicios de red de este a oeste.
- Máquina virtual de servicio: una máquina virtual que ejecuta el dispositivo OVA u OVF especificado por un servicio. Se conecta a través del plano de servicios para recibir el tráfico redireccionado.
- Instancia de servicio: se crea al implementar un servicio en un host. Cada instancia de servicio tiene su correspondiente máquina virtual de servicio.
- Segmento de servicio: un segmento de un plano de servicio que está asociado a una zona de transporte. Cada conexión del servicio se separa de otras conexiones de servicios y de los segmentos de red normales de Capa 2 o Capa 3 proporcionados por NSX-T. El plano de servicio administra las conexiones de servicios.

- **Service Manager:** es el administrador de servicios de partners que apunta a un conjunto de servicios.
- **Cadena de servicios:** es una secuencia lógica de perfiles de servicio definidos por un administrador. Los perfiles de servicio realizan la introspección del tráfico de red en el orden definido en la cadena de servicios. Por ejemplo, el primer perfil de servicio es el firewall, el segundo es el monitor, etc. Las cadenas de servicios pueden especificar una secuencia de perfiles de servicio diferente para distintas direcciones de tráfico (de salida o de entrada).
- **Directiva de redireccionamiento:** garantiza que el tráfico clasificado para una cadena de servicios específica se redirija a esa cadena de servicios. Se basa en los patrones de tráfico que coinciden con una cadena de servicios y el grupo de seguridad de NSX-T Data Center. Todo el tráfico que coincida con el patrón se redireccionará hacia la cadena de servicios.
- **Ruta de acceso de servicio:** es una secuencia de las máquinas virtuales de servicio que implementan los perfiles de servicio de una cadena de servicios. Un administrador define la cadena de servicios, que consiste en un orden predefinido de perfiles de servicio. NSX-T Data Center genera varias rutas de acceso de servicio a partir de una cadena de servicios en función del número y de las ubicaciones de las máquinas virtuales invitadas y las máquinas virtuales de servicio. Selecciona la ruta de acceso de servicio óptima para la introspección interna del flujo de tráfico. Cada ruta de acceso de servicio se identifica mediante un índice de ruta de acceso de servicio (Service Path Index, SPI) y cada salto en una ruta de acceso tiene un índice de servicio (Service Index, SI) único.

Requisitos de NSX-T Data Center para el tráfico de este a oeste

En la implementación de NSX-T Data Center, debe asegurarse de que exista una zona de transporte superpuesta y conmutadores lógicos respaldados por superposición.

La inserción de servicios de este a oeste se aplica a una implementación de NSX-T completa. No se puede implementar el servicio a nivel de clúster o de host.

Todos los nodos de transporte deben ser del tipo superpuesto, ya que el servicio envía tráfico en GENEVE o conmutadores lógicos respaldados por superposición. Un conmutador lógico respaldado por superposición (respaldado por GENEVE) se aprovisiona internamente y no se muestra en la interfaz de usuario.

Aunque planifique una implementación con solo conmutadores lógicos respaldados por VLAN, el tráfico de este a oeste pasará por las zonas de transporte superpuestas y los conmutadores lógicos respaldados por superposición. Por lo tanto, asegúrese de crear una zona de transporte superpuesta y conmutadores lógicos respaldados por GENEVE. Sin estos requisitos, durante una operación de vMotion, la guestVM de un host no se podrá migrar a otro nodo de transporte. La guestVM entrará en estado Desconectado, lo que provocará errores de configuración en el servicio de este a oeste.

Tareas de alto nivel para la seguridad de red de Este a Oeste

Siga estos pasos para configurar la seguridad de red del tráfico de Este a Oeste.

Tabla 10-3. Lista de tareas para configurar la introspección de red de Este a Oeste

Tareas de flujo de trabajo	Persona	Implementación
Registrar servicio	Partner	Solo API
Registre plantilla de proveedor	Partner	Solo API
Registrar instancia de Service Manager	Partner	Solo API
Implementar un servicio de introspección de tráfico de este a oeste	Administrador	API e interfaz de usuario de NSX Manager
Agregar un perfil de servicio	Administrador	API e interfaz de usuario de NSX Manager
Agregar una cadena de servicios	Administrador	API e interfaz de usuario de NSX Manager
Agregar reglas de redirección para el tráfico de este a oeste	Administrador	API e interfaz de usuario de NSX Manager

Implementar un servicio de introspección de tráfico de este a oeste

Después de que los partners registran los servicios, deberá, como administrador, implementar una instancia del servicio en los hosts que forman parte de un clúster.

Implemente máquinas virtuales de servicio de partners que ejecuten el motor de seguridad de partner en todos los hosts de NSX-T Data Center de un clúster. Después de implementar las SVM, puede crear reglas de directiva utilizadas por las SVM para proteger las máquinas virtuales invitadas.

Requisitos previos

- Todos los hosts se administran mediante vCenter Server.
- Los servicios de partners deben estar registrados en NSX-T Data Center y listos para la implementación.
- Los administradores de NSX-T Data Center pueden acceder a los servicios de partners y las plantillas de proveedor.
- La máquina virtual de servicio y la instancia de Service Manager de partners (consola) deben poder comunicarse entre sí en el nivel de la red de administración.
- Implementación de servicio basado en host: antes de implementar las máquinas virtuales de servicio en cada host, configure cada host del clúster con NSX-T Data Center aplicando un perfil de nodo de transporte.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

- 2 Seleccione **Sistema > Implementaciones de servicio > Implementación > Implementar servicio**.
- 3 En el campo Servicio de partners, seleccione el servicio de partners.
- 4 Introduzca el nombre de implementación del servicio.
- 5 En el campo Administrador de equipo, seleccione la instancia de vCenter Server para implementar el servicio.
- 6 En el campo Clúster, seleccione el clúster donde deben implementarse los servicios.
- 7 En el menú desplegable Almacén de datos, seleccione un almacén de datos como repositorio para la máquina virtual de servicio.
- 8 En la columna Red, haga clic en **Establecer** e introduzca la interfaz de la red de administración seleccionando el tipo DHCP o dirección IP estática y la red de datos.
- 9 En el campo Segmentos de servicio, seleccione un segmento de servicio de la lista o haga clic en el icono de acción para agregar o editar un segmento de servicio. Las máquinas virtuales invitadas conectadas a un segmento de servicio se proporcionan con protección del tráfico de red de este a oeste.
- 10 En el campo Tipo de implementación, seleccione una de las siguientes opciones. En función de los servicios registrados por el partner, se pueden implementar varios servicios como parte de una máquina virtual de un solo servicio.
 - En clúster: implementa el servicio en un host o hosts que pertenecen a un clúster dedicado a las máquinas virtuales del servicio de host.
 - Basado en host: implementa el servicio en todos los hosts de un clúster.
- 11 En el campo Plantilla de implementación, seleccione la plantilla que proporciona atributos para proteger la carga de trabajo que desee ejecutar en los grupos de máquinas virtuales invitadas.
- 12 (Solo en implementaciones basadas en clúster) En la opción Recuento de implementación agrupada en clúster, introduzca el número de máquinas virtuales de servicio que se implementarán en el clúster. vCenter Server decide en qué host se implementarán las máquinas virtuales de servicio.
- 13 Haga clic en **Guardar**.

Resultados

Tras implementar el servicio, se notifica a la instancia de Service Manager de partners sobre la actualización.

Pasos siguientes

Conozca los detalles de implementación y el estado de mantenimiento de las instancias de servicio implementadas en los hosts. Consulte [Agregar un perfil de servicio](#).

Agregar un perfil de servicio

Un perfil de servicio es una instancia de una plantilla de proveedor de partner. Los administradores pueden personalizar los atributos de una plantilla de proveedor para crear una instancia de la plantilla.

Nota Puede crear varios perfiles de servicio para un único proveedor. Por ejemplo, el perfil de servicio establecido para la ruta de reenvío proporciona protección IDS, mientras que el perfil de servicio establecido para la ruta inversa es compatible con la protección IPS. Sin embargo, puede establecer un solo perfil de servicio para los dos tipos de rutas.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Seguridad > Seguridad de este y oeste > Introspección de red > Perfiles de servicio**.
- 3 Seleccione un servicio en el campo desplegable Servicio de partners. Puede crear un perfil de servicio para el servicio seleccionado.
- 4 Introduzca el nombre del perfil de servicio y seleccione la plantilla de proveedor.
- 5 El campo Acción de redireccionamiento hereda la funcionalidad de la plantilla del proveedor. Por ejemplo, si la funcionalidad que proporciona la plantilla del proveedor es COPIAR, la acción de redireccionamiento predeterminada cuando cree un perfil de servicio será COPIAR.
- 6 (Opcional) Establezca alguna etiqueta para filtrar y administrar los perfiles de servicio.
- 7 Haga clic en **Guardar**.

Resultados

Se creará un nuevo perfil de servicio para el servicio de partners.

Pasos siguientes

Agregue una cadena de servicios. Consulte [Agregar una cadena de servicios](#).

Agregar una cadena de servicios

Una cadena de servicios es una secuencia lógica de perfiles de servicio definidos por el administrador de red.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Seguridad > Seguridad de este y oeste > Introspección de red > Cadena de servicios > Agregar cadena**.

- 3 Introduzca el nombre de la cadena de servicios.
- 4 En el campo Segmentos de servicio, seleccione el segmento de servicio al que desea aplicar la cadena de servicios. Un segmento de servicio es un segmento de plano de servicio que se conecta a varias máquinas virtuales de servicio correspondientes a una zona de transporte superpuesta. Cada máquina virtual de servicio en la cadena de servicios es independiente de otra máquina virtual de servicio, y los segmentos de red de Capa 2 y Capa 3 se ejecutan mediante NSX-T Data Center. El plano de servicio controla el acceso a las máquinas virtuales de servicio.
- 5 Para establecer la ruta de reenvío, haga clic en el campo **Establecer ruta de reenvío** y haga clic en **Agregar perfil en secuencia**.
- 6 Seleccione el primer perfil de la cadena de servicios y haga clic en **Agregar**.
- 7 Para especificar el perfil de servicio siguiente, haga clic en **Agregar perfil en secuencia** e introduzca los detalles. También puede cambiar la disposición del perfil mediante el uso de los iconos de flecha hacia arriba y hacia abajo.
- 8 Haga clic en **Guardar** para terminar de agregar una ruta de reenvío para la cadena de servicios.
- 9 En la columna Ruta inversa, seleccione **Ruta de acceso directa inversa** para utilizar el perfil de servicio que estableció para la ruta de reenvío en el plano de servicio.
- 10 Si quiere establecer un perfil de servicio nuevo para la ruta inversa, haga clic en **Establecer ruta de acceso inversa** y agregue un perfil de servicio.
- 11 Haga clic en **Guardar** para terminar de agregar una ruta inversa para la cadena de servicios.
- 12 En el campo Directiva de error:
 - Seleccione **Permitir** para enviar tráfico a la máquina virtual de destino cuando se produce un error en la máquina virtual de servicio. Se detectó un error de la máquina virtual de servicio mediante el mecanismo de detección de ejecución que solo los partners pueden habilitar.
 - Seleccione **Bloquear** para no enviar tráfico a la máquina virtual de destino cuando se produce un error en la máquina virtual de servicio.
- 13 Haga clic en **Guardar**.

Resultados

Después de agregar una cadena de servicios, se notifica a la instancia de Service Manager de partners acerca de la actualización.

Pasos siguientes

Cree una regla de redirección para realizar la introspección del tráfico de red de este a oeste. Consulte [Agregar reglas de redirección para el tráfico de este a oeste](#).

Agregar reglas de redirección para el tráfico de este a oeste

Agregue reglas a fin de redirigir un tráfico de este a oeste para introspección de red.

Las reglas se definen en una directiva. Una directiva como concepto es similar al concepto de secciones en los firewalls. Al agregar una directiva, seleccione la cadena de servicios para redirigir el tráfico de introspección mediante los perfiles de servicio de la cadena de servicios.


La definición de una regla consiste en el origen y el destino del tráfico, el servicio de introspección, el objeto NSX-T Data Center al cual se aplica la regla y la directiva de redirección de tráfico. Después de publicar la regla, NSX Manager activa la regla cuando se encuentra un patrón de tráfico que coincide. La regla comienza a realizar la introspección del tráfico. Por ejemplo, cuando NSX Manager clasifica un flujo de tráfico que se debe someter a introspección, no lo reenvía al firewall distribuido regular, sino que redirige ese tráfico por la cadena de servicios especificada en la directiva. Los perfiles de servicio definidos en la cadena de servicios realizan la introspección del tráfico para los servicios de red que ofrece el partner. Si un perfil de servicio finaliza la introspección sin detectar problemas de seguridad en el tráfico, el tráfico se reenvía al perfil de servicio siguiente en la cadena de servicios. Al final de la cadena de servicios, el tráfico se reenvía al destino.

Todas las notificaciones se envían a la instancia de Service Manager de partners y a NSX-T Data Center.

Requisitos previos

Una cadena de servicios está disponible para redirigir el tráfico en una introspección de red.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 **Seguridad > Seguridad de este y oeste > Introspección de red > Reglas > Agregar directiva.**
Una sección de directiva es similar a una sección de firewall donde se definen las reglas que determinan cómo fluye el tráfico.
- 3 Seleccione una cadena de servicios.
- 4 Para agregar una directiva, haga clic en **Publicar**.
- 5 Haga clic en los  tres puntos verticales en una sección y haga clic en **Agregar regla**.

- 6 Edite el campo **Origen** para agregar un grupo mediante la definición de criterios de pertenencia, miembros estáticos, direcciones IP/MAC o grupos de Active Directory.
 - a Establezca los criterios de pertenencia mediante una de estas entidades:
 - Máquina virtual
 - Conmutador lógico
 - Puerto lógico
 - Conjunto de direcciones IP
 - b Especifique la lista de miembros estáticos mediante una de estas entidades:
 - Grupo
 - Segmento
 - Puerto de segmento
 - Interfaz de red virtual
 - Máquina virtual
- 7 Haga clic en **Guardar**.
- 8 Para agregar un grupo de destino, edite el campo **Destino**.
- 9 En el campo Se aplica a, elija una de las siguientes opciones:
 - Seleccione **DFW** para aplicar la regla a todas las NIC virtuales conectadas al conmutador lógico.
 - Seleccione **Grupos de máquinas virtuales** para aplicar la regla en las NIC virtuales de las máquinas virtuales que pertenecen al grupo. Los miembros se pueden seleccionar de una lista estática o en función de criterios dinámicos. Los objetos de NSX-T Data Center compatibles son: máquina virtual, conmutador lógico, puerto lógico, conjunto de direcciones IP, etc.
- 10 En el campo Acción, seleccione **Redirigir** para redirigir el tráfico por la cadena de servicios o **No redirigir** para que no se aplique introspección de red en el tráfico.
- 11 Haga clic en **Publicar**.
- 12 Para revertir una regla publicada, seleccione una regla y haga clic en **Revertir**.
- 13 Para agregar una directiva, haga clic en **+ Agregar directiva**.
- 14 Para clonar una directiva o una regla, seleccione la directiva o la regla y haga clic en **Clonar**.
- 15 Para habilitar una regla, active el icono Habilitar/deshabilitar, o bien seleccione la regla y, en el menú, haga clic en **Habilitar > Habilitar regla**.
- 16 Después de habilitar o deshabilitar una regla, haga clic en **Publicar** para aplicar la regla.

Resultados

El tráfico que circula hacia el origen se redirige a la cadena de servicios para introspección de red. Después de que los perfiles de servicio de la cadena realizan la introspección del tráfico, este se envía al destino.

Durante la implementación, es posible que cambie la pertenencia de un grupo de máquinas virtuales para una directiva específica. NSX-T Data Center notifica a la instancia de Service Manager de partners sobre estas actualizaciones.

Configurar un firewall de puerta de enlace

El firewall de puerta de enlace representa reglas que se aplican en el firewall perimetral.

Hay categorías predefinidas en la vista **Todas las reglas compartidas**, donde son visibles las reglas en todas las puertas de enlace. Las reglas se evalúan de arriba hacia abajo y de izquierda a derecha. Los nombres de las categorías se pueden cambiar mediante la API.

Tabla 10-4. Categorías de reglas de firewall de puerta de enlace

Categoría de regla	Propósito
Emergencia	Se utiliza para poner en cuarentena. También puede utilizarse para permitir reglas.
Sistema	Estas reglas se generan automáticamente mediante NSX-T Data Center y son específicas del tráfico del plano de control interno, por ejemplo, reglas BFD, VPN, etc. Nota No edite las reglas del sistema.
Reglas previas compartidas	Estas reglas se aplican globalmente en todas las puertas de enlace.
Puerta de enlace local	Estas reglas son específicas de una puerta de enlace en particular.
Reglas de autoservicio	Estas son reglas asociadas automáticamente que se aplican al plano de datos. Puede editar estas reglas según sea necesario.
Predeterminado	Estas reglas definen el comportamiento predeterminado del firewall de puerta de enlace.

Agregar una regla y una directiva de firewall de puerta de enlace

Para implementar reglas de firewall de puerta de enlace, agregue las reglas en una sección de directiva de firewall que pertenezca a una categoría predefinida.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Seguridad > Seguridad de Norte y Sur > Firewall de puerta de enlace**.

- 3 Para habilitar el firewall de puerta de enlace, seleccione **Acciones > Configuración general** y alterne el botón de estado. Haga clic en **Guardar**.
- 4 Haga clic en **Agregar directiva**. Para obtener más información sobre las categorías, consulte [Configurar un firewall de puerta de enlace](#).
- 5 En **Nombre**, escriba un nombre para la nueva sección de directiva.
- 6 En **Destino**, seleccione el destino de la directiva.
- 7 Haga clic en el icono de engranaje para establecer la siguiente configuración de directiva:

Configuración	Descripción
TCP estricto	Una conexión TCP comienza con un protocolo de enlace de tres vías (SYN, SYN-ACK y ACK) y, por lo general, termina con un intercambio de dos vías (FIN y ACK). En determinadas circunstancias, es posible que el firewall no vea el protocolo de enlace de tres vías para un flujo concreto (por ejemplo, debido al tráfico asimétrico). De forma predeterminada, el firewall obliga a un protocolo de enlace de tres vías y realizará sesiones de recogida que ya estén establecidas. Se puede habilitar el modo TCP estricto en cada sección para desactivar la recogida de sesiones medias y exigir el requisito de un protocolo de enlace de tres vías. Cuando se habilita el modo TCP estricto para una determinada directiva y se utiliza una regla de bloqueo ANY-ANY predeterminada, se descartan los paquetes que no cumplan todos los requisitos de conexión de protocolo de tres vías y que coincidan con una regla basada en TCP de esta sección. El modo TCP estricto solo se aplica a las reglas de TCP con estado y se habilita en el nivel de la sección de firewall de puerta de enlace. TCP estricto no se aplica a los paquetes que coinciden con el permiso ANY-ANY predeterminado, sin especificar ningún servicio TCP.
Con estado	Un firewall con estado supervisa el estado de las conexiones activas y utiliza esta información para determinar a qué paquetes se les permite atravesar el firewall.
Bloqueado	La directiva se puede bloquear para impedir que varios usuarios realicen cambios en las mismas secciones. Cuando bloquea una sección, debe incluir un comentario.

- 8 Haga clic en **Publicar**. Se pueden agregar varias directivas y, a continuación, publicarlas al mismo tiempo.
La nueva directiva se muestra en la pantalla.
- 9 Seleccione una sección de directiva y haga clic en **Agregar regla**.
- 10 Introduzca un nombre para la regla. Se admiten direcciones IPv4, IPv6 y de multidifusión.

- 11 En la columna **Orígenes**, haga clic en el icono de edición y seleccione el origen de la regla. Consulte [Agregar un grupo](#) para obtener más información.
- 12 En la columna **Destinos**, haga clic en el icono de edición y seleccione el destino de la regla. Si no está definido, el destino coincidirá con cualquiera. Consulte [Agregar un grupo](#) para obtener más información.
- 13 En la columna **Servicios**, haga clic en el icono de lápiz y seleccione los servicios. Si no está definido, el servicio coincidirá con cualquiera.
- 14 En la columna **Perfiles**, haga clic en el icono de edición y seleccione un perfil de contexto, o bien haga clic en **Agregar nuevo perfil de contexto**. Consulte [Agregar un perfil de contexto](#).
 - Los perfiles de contexto no se admiten en la directiva de firewall de puerta de enlace de nivel 0.
 - No se pueden utilizar perfiles de contexto con atributos de FQDN u otros subatributos en las reglas de firewall de puerta de enlace.

Los perfiles de contexto usan atributos de identificador de aplicación de Capa 7 para emplearlos en reglas de firewall distribuido y reglas de firewall de puerta de enlace. Se pueden utilizar varios perfiles de contexto de identificador de aplicación en una regla de firewall con servicios establecidos en **Cualquiera**. Para perfiles de ALG (FTP y TFTP), se admite un perfil de contexto por regla.

- 15 Haga clic en **Aplicar**.
- 16 La columna **Se aplica a** define el ámbito de aplicación por regla y permite a los usuarios aplicar reglas de forma selectiva a una o varias interfaces de vínculo superior o interfaces de servicio. De forma predeterminada, las reglas de firewall de puerta de enlace se aplican a todos los vínculos superiores e interfaces de servicio disponibles en una puerta de enlace seleccionada.
- 17 En la columna **Acción**, seleccione una acción.

Opción	Descripción
Permitir	Permite todo el tráfico con el origen, destino y protocolo especificados a través del contexto de firewall presente. Los paquetes que coincidan con la regla y se acepten atraviesan el sistema como si el firewall no estuviese presente.
Quitar	Descarta paquetes con el origen, destino y protocolo especificados. Descartar un paquete es una acción silenciosa que no envía ninguna notificación a los sistemas de origen y de destino. Al descartar el paquete, se intentará recuperar la conexión hasta que se alcance el umbral de reintentos.
Rechazar	Rechaza paquetes con el origen, destino y protocolo especificados. Al rechazar un paquete, se envía al remitente un mensaje de destino inaccesible. Si el protocolo es TCP, se envía un mensaje TCP RST. Se envían mensajes ICMP con código prohibido de forma administrativa para conexiones UDP, ICMP y otras conexiones IP. Después de un intento, se envía una notificación a la aplicación de envío para indicarle que no se puede establecer conexión.

- 18 Haga clic en el botón de alternancia de estado para habilitar o deshabilitar la regla.
- 19 Haga clic en el icono de engranaje para establecer el registro, la dirección, el protocolo IP, las etiquetas y las notas.

Opción	Descripción
Registro	Se puede activar o desactivar el registro. Los registros se almacenan en /var/log/syslog en la instancia de Edge.
Dirección	Las opciones son Entrada , Salida y Entrada/salida . El valor predeterminado es Entrada/salida . Este campo hace referencia a la dirección del tráfico desde el punto de vista del objeto de destino. Entrada significa que solo se comprueba el tráfico que entra al objeto, Salida significa que solo se comprueba el tráfico que sale del objeto y Entrada/salida significa que se comprueba el tráfico en ambas direcciones.
Protocolo IP	Las opciones son IPv4 , IPv6 e IPv4_IPv6 . El valor predeterminado es IPv4_IPv6 .
Etiqueta	Las etiquetas que se han agregado a la regla.

Nota Haga clic en el icono de gráfico para ver las estadísticas de flujo de la regla de firewall. Puede ver información como la cantidad de bytes, el recuento de paquetes y las sesiones.

- 20 Haga clic en **Publicar**. Se pueden agregar varias reglas y, a continuación, publicirlas al mismo tiempo.
- 21 En cada sección de la directiva, haga clic en el icono de **información** para ver el estado actual de las reglas de firewall de Edge que se envían a los nodos de Edge. También se muestran las alarmas generadas cuando se insertan las reglas en los nodos de Edge.
- 22 Para ver el estado consolidado de las reglas de directiva que se aplican a los nodos de Edge, realice la llamada API.

```
GET https://<policy-mgr>/policy/api/v1/infra/
realized-state/status?intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

Seguridad de red de norte a sur: inserción de servicio de terceros

NSX-T Data Center proporciona la función para insertar servicios de terceros en un enrutador de nivel 0 o 1 en el centro de datos para redireccionar el tráfico al servicio de terceros para la introspección. Solo se admiten hosts ESXi para implementar máquinas virtuales de servicios de Norte a Sur. No se admiten hosts KVM.

Tareas de alto nivel para la seguridad de red de Norte a Sur

Siga estos pasos para configurar la seguridad de red del tráfico de Norte a Sur.

Tabla 10-5. Lista de tareas para configurar la introspección de red de Norte a Sur

Tareas de flujo de trabajo	Persona	Implementación
Registrar servicio con NSX-T Data Center	Partner	Solo API
Implementar un servicio de introspección de tráfico de norte a sur	Administrador	API e interfaz de usuario de NSX Manager
Configurar el redireccionamiento de tráfico	Administrador	API e interfaz de usuario de NSX Manager

Implementar un servicio de introspección de tráfico de norte a sur

Después de registrar un servicio, debe implementar una instancia del servicio para iniciar el procesamiento del tráfico de red.

Implemente la máquina virtual de servicio de partners en el enrutador lógico de nivel 0 o nivel 1 que actúa como puerta de enlace entre el mundo físico y la red lógica en vCenter Server. Después de implementar la SVM como una instancia de servicio independiente o una instancia de servicio activo-en espera, puede crear reglas de redireccionamiento a fin de redirigir el tráfico a la SVM para la introspección de red.

Requisitos previos

- Todos los hosts se administran mediante vCenter Server.
- Los servicios de partners están registrados con NSX-T Data Center y listos para la implementación.
- Los administradores de NSX-T Data Center pueden acceder a los servicios de partners.
- El modo de alta disponibilidad para el enrutador lógico debe estar en modo activo-en espera.
- Active la utilidad Distributed Resource Scheduler.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Servicios de partners > Instancias de servicio > Catálogo**.
- 3 La pestaña Catálogo muestra los servicios registrados.
- 4 Seleccione el servicio que se muestra en formato OVF y haga clic en **Implementar** para comenzar la implementación de la instancia de servicio.
- 5 En la ventana Inserción de servicios de partners, haga clic en **Continuar**.

- 6 En la ventana Servicio de partners, introduzca los detalles.

Tabla 10-6. Detalles del servicio de partners

Campo	Descripción
Nombre de instancia	Escriba un nombre para identificar la instancia de servicio.
Descripción	Descripción de la instancia de servicio.
Servicio de partners	Seleccione el servicio de partners registrado con NSX-T Data Center.
Especificación de implementación	Seleccione el formato para implementar.
Enrutador lógico	Seleccione el enrutador lógico de nivel 0 donde se debe implementar la instancia de servicio.

- 7 Haga clic en **Siguiente**.

- 8 En la ventana Configuración de la instancia, introduzca los detalles.

Tabla 10-7. Detalles de la instancia de servicio

Campo	Descripción
Modo de implementación	Seleccione Independiente para implementar una sola instancia de servicio en el enrutador lógico de nivel 0. Seleccione Alta disponibilidad para implementar un par de instancias de servicio en modo activo-en espera en el enrutador lógico de nivel 0.
Directiva de error	Seleccione Permitir o Bloquear .
Dirección IP de la instancia de servicio	Introduzca la dirección IP que utilizará la instancia de servicio.
Puerta de enlace	Introduzca la dirección de puerta de enlace.
Máscara de subred	Introduzca la máscara de subred.
Id. de red	Introduzca el identificador de red del conmutador lógico donde desea conectar la red de administración.
Administrador de equipo	Seleccione la instancia de vCenter Server registrada.
Grupo de recursos	Seleccione el grupo de recursos que proporciona recursos para implementar la instancia de servicio.
Almacén de datos	Seleccione el repositorio para almacenar datos de la instancia de servicio.

- 9 Haga clic en **Siguiente**.

10 En la ventana Configuración avanzada, introduzca los detalles.

Tabla 10-8.

Campo	Descripción
Plantilla de implementación	Seleccione la plantilla que se usará durante la implementación de la instancia de servicio.
Licencia	Introduzca la licencia de la plantilla.

11 Haga clic en **Finalizar**.

Resultados

La pestaña Instancias de servicio muestra el progreso de la implementación. La tarea podría tardar algunos minutos en completarse. Compruebe el estado de implementación para asegurarse de que la instancia de servicio se implemente correctamente en el enrutador lógico de nivel 0.

Si lo prefiere, vaya a vCenter Server y compruebe el estado de la implementación.

Pasos siguientes

Configure reglas para redirigir el tráfico a la instancia de servicio implementada en el enrutador de nivel 0. Consulte [Configurar el redireccionamiento de tráfico](#)

Configurar el redireccionamiento de tráfico

Después de implementar una instancia de servicio, configure el tipo de tráfico que el enrutador redirige al servicio. Configurar el redireccionamiento de tráfico es similar a configurar un firewall.

Para obtener más información sobre cómo configurar un firewall, consulte [Secciones y reglas de firewall](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Servicios de partners > Instancias de servicio**.
- 3 Haga clic en la instancia de servicio.
- 4 Haga clic en la pestaña **Redireccionamiento de tráfico**.
- 5 Para agregar una sección, seleccione una existente y haga clic en **Agregar sección**.
 - ◆ En el menú, seleccione **Agregar sección encima** o **Agregar sección debajo**.

Se creará una sección. El tipo de tráfico que se redirige se establece como **Redireccionamiento de Capa 3**, el tipo de servicio es **Sin estado** y el campo **Se aplica a** se asocia a un enrutador lógico de nivel 0 que se configura en el host. Después de establecer las reglas, el campo **Reglas** se rellena automáticamente.

- 6 Haga clic en **Publicar** para que se aplique la información de configuración de la sección.
- 7 Para agregar una regla a esa sección, seleccione la sección y haga clic en **Agregar regla**.
- 8 Introduzca la siguiente información en la fila de la regla:
 - a Introduzca el nombre de la regla.
 - b Introduzca el origen y el destino del tráfico de Capa 3. La máquina virtual del servicio de partners realiza la introspección del tráfico procedente del origen antes de redirigirlo a la máquina virtual de destino.
 - c En el campo **Se aplica a**, seleccione el enlace ascendente del enrutador de nivel 0.
 - d En el campo **Acción**, seleccione **Redirigir** si necesita que las máquinas de servicio realicen la introspección del tráfico, o bien seleccione **No redirigir** si no se debe realizar la introspección del tráfico de norte a sur.
- 9 Puede habilitar cada regla de forma individual. Una vez que la habilite, se aplicará al tráfico que coincida con la regla.
- 10 Haga clic en Configuración avanzada para configurar la dirección del tráfico y habilitar el registro.
- 11 Al final de una sección que contenga reglas, haga clic en **Publicar** para que se apliquen las reglas de la sección, o bien haga clic en **Revertir** para cancelar la operación.

Resultados

El tráfico se envía a las reglas de introspección de la red donde se aplican las reglas de la directiva al tráfico.

Pasos siguientes

Consulte [Agregar reglas de redireccionamiento para el tráfico de norte a sur](#).

Agregar reglas de redireccionamiento para el tráfico de norte a sur

Configure reglas de redireccionamiento de norte a sur con la interfaz de usuario de **Opciones avanzadas de redes y seguridad**. El tráfico solo se redirige en el caso de los servicios insertados en el enrutador de nivel 0.

Siga las instrucciones que se indican en [Configurar el redireccionamiento de tráfico](#).

Requisitos previos


- Registrar e implementar los servicios de terceros en NSX-T.
- Configurar el enrutador de nivel 0.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

2 Seguridad > Firewall de norte y sur > Introspección de red (N-S) > Agregar directiva.

Una sección de directiva es similar a una sección de firewall donde se definen las reglas que determinan cómo fluye el tráfico.

- 3 En **Redireccionamiento a**, establezca la instancia de servicio registrada en NSX-T para que realice la introspección de red del tráfico que fluye entre las entidades de origen y destino.
- 4 Para agregar una directiva, haga clic en **Publicar**.
- 5 Haga clic en los  tres puntos verticales en una sección y haga clic en **Agregar regla**.
- 6 Edite el campo **Origen** para agregar un grupo mediante la definición de criterios de pertenencia, miembros estáticos, direcciones IP/MAC o grupos de Active Directory. Los criterios de pertenencia pueden definirse a partir de uno de estos tipos: máquina virtual, conmutador lógico, puerto lógico y conjunto de direcciones IP. Puede seleccionar miembros estáticos de una de estas categorías: grupo, segmento, puerto de segmento, interfaz de red virtual o máquina virtual.
- 7 Haga clic en **Guardar**.
- 8 Para agregar un grupo de destino, edite el campo **Destino**.
- 9 En el campo Se aplica a, elija una de las siguientes opciones:
 - Seleccione **DFW** para aplicar la regla a todas las NIC virtuales conectadas al conmutador lógico.
 - Seleccione **Grupos de máquinas virtuales** para aplicar la regla en las NIC virtuales de las máquinas virtuales que pertenecen al grupo. Los miembros se pueden seleccionar de una lista estática o en función de criterios dinámicos. Los objetos de NSX-T Data Center compatibles son: máquina virtual, conmutador lógico, puerto lógico, conjunto de direcciones IP, etc.
- 10 En el campo Acción, seleccione **Redirigir** para redirigir el tráfico por la instancia de servicio o **No redirigir** para que no se aplique introspección de red en el tráfico.
- 11 Haga clic en **Publicar**.
- 12 Para revertir una regla publicada, seleccione una regla y haga clic en **Revertir**.
- 13 Para agregar una directiva, haga clic en **+ Agregar directiva**.
- 14 Para clonar una directiva o una regla, seleccione la directiva o la regla y haga clic en **Clonar**.
- 15 Para habilitar una regla, active el icono Habilitar/deshabilitar, o bien seleccione la regla y, en el menú, haga clic en **Habilitar > Habilitar regla**.
- 16 Después de habilitar o deshabilitar una regla, haga clic en **Publicar** para aplicar la regla.

Resultados

En función de las acciones establecidas, el tráfico de norte a sur se redirigirá a la instancia de servicio para la introspección de red.

Supervisar el redireccionamiento de tráfico

Después de implementar una instancia de servicio y configurar el redireccionamiento de tráfico, puede supervisar la cantidad de tráfico que entra y sale de la instancia de servicio.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Servicios de partners > Instancias de servicio**.
- 3 Haga clic en el nombre de una instancia de servicio.

La pestaña **Información general** muestra la configuración y el estado de la instancia de servicio.
- 4 Haga clic en la pestaña **Estadísticas**.

Se muestra información sobre la cantidad de paquetes y la cantidad de datos que entran a la instancia de servicio y salen de esta.
- 5 Haga clic en **Actualizar** para actualizar las estadísticas.

Protección de endpoints

NSX-T Data Center permite insertar servicios de partners de terceros como una máquina virtual de servicio independiente que proporciona servicios de protección de endpoints. Una máquina virtual de servicio de partners procesa los eventos de archivos, procesos y registros de la máquina virtual invitada en función de las reglas de directiva de protección de endpoints aplicadas por el administrador de NSX-T Data Center.

Protección de endpoints

Conozca los casos prácticos, el flujo de trabajo y los conceptos clave de la protección de endpoints.

Caso práctico de protección de endpoints

En un entorno virtual, utilice la plataforma Guest Introspection para proporcionar protección antivirus y antimalware a las máquinas virtuales invitadas.

Como administrador de NSX, implemente una solución antivirus y antimalware que se distribuye como una máquina virtual de servicio (Service Virtual Machine, SVM) para supervisar la actividad de un archivo, una red o un proceso en una máquina virtual invitada. Cuando se accede a un archivo (por ejemplo, cuando se intenta abrir un archivo), la máquina virtual de servicio antimalware recibe una notificación del evento. A continuación, la máquina virtual de servicio determina cómo responder al evento. Por ejemplo, inspeccionar el archivo en busca de firmas de virus.

- Si la máquina virtual de servicio determina que el archivo no contiene ningún virus, permitirá que la operación de apertura del archivo se realice correctamente.
- Si la máquina virtual de servicio detecta un virus en el archivo, solicita al Thin Agent de la máquina virtual invitada que actúe de una de las siguientes maneras:
 - Eliminar el archivo infectado o denegar el acceso al archivo.
 - NSX puede asignar una etiqueta a las máquinas virtuales infectadas. Además, puede definir una regla que mueva automáticamente dichas máquinas virtuales invitadas etiquetadas a un grupo de seguridad que ponga en cuarentena la máquina virtual infectada como medida adicional de exploración y aislamiento en la red hasta que la infección se elimine por completo.

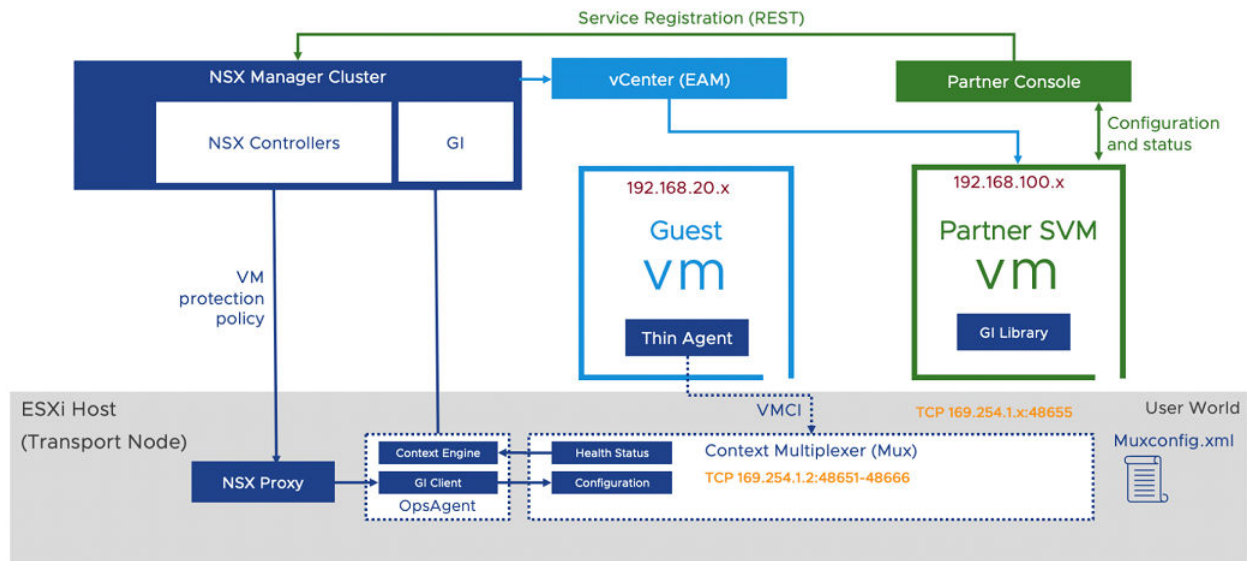
Las ventajas de usar la plataforma Guest Introspection para proteger los endpoints de la máquina virtual invitada son:

- Consumo reducido de recursos informáticos: Guest Introspection descarga las firmas de virus y la lógica de exploración de seguridad de cada endpoint de un host en una máquina virtual de servicio de partner de terceros en el host. Como la detección de virus se produce solo en la máquina virtual de servicio, no es necesario gastar recursos informáticos detectando virus en las máquinas virtuales invitadas.
- Mejor administración: a medida que se descargan las exploraciones de virus en una máquina virtual de servicio, las firmas de virus deben actualizarse a un solo objeto por host. Un mecanismo de este tipo funciona mejor que la solución basada en agentes, donde las mismas firmas de virus necesitan actualizaciones en todas las máquinas virtuales invitadas.
- Protección antivirus y antimalware continua: como la máquina virtual de servicio se ejecuta continuamente, no se permite que las máquinas virtuales invitadas ejecuten las firmas de virus más recientes. Por ejemplo, una máquina virtual de instantáneas puede ejecutar alguna versión anterior de la firma de virus, lo que hace que sea vulnerable con la forma tradicional de proteger los endpoints. Con la plataforma Guest Introspection, la máquina virtual de servicio ejecuta continuamente las firmas de virus y malware más recientes, lo que garantiza que cualquier máquina virtual recién agregada también esté protegida con las firmas de virus más recientes.
- Las firmas de virus se descargan en una máquina virtual de servicio: el ciclo de vida de la base de datos de virus está fuera del ciclo de vida de la máquina virtual invitada, por lo que la máquina virtual no se ve afectada por interrupciones.

Arquitectura de Guest Introspection

Conozca la arquitectura de los componentes de inserción de servicios e introspección de invitado en NSX-T Data Center.

Figura 10-1. Arquitectura de Guest Introspection



Conceptos clave:

- **Consola de partners:** es la aplicación web que proporciona el proveedor de seguridad para trabajar con la plataforma Guest Introspection.
- **NSX Manager:** es el dispositivo del plano de administración de NSX que proporciona una API y una interfaz gráfica de usuario a los clientes y los partners para la configuración de directivas de redes y seguridad. Para Guest Introspection, NSX Manager también proporciona una API y una GUI para implementar y administrar dispositivos de partners.
- **SDK de Guest Introspection:** biblioteca proporcionada por VMware para el proveedor de seguridad.
- **Máquina virtual de servicio:** es la máquina virtual proporcionada por el proveedor de seguridad para el SDK de Guest Introspection proporcionado por VMware. Contiene la lógica para analizar los eventos de archivo o de proceso para detectar virus o malware en el invitado. Después de examinar una solicitud, devuelve un veredicto o una notificación sobre la acción emprendida por la máquina virtual invitada en la solicitud.
- **Guest Introspection Agent (multiplexor de contexto):** procesa la configuración de las directivas de protección de endpoints. También multiplexa y reenvía los mensajes de las máquinas virtuales protegidas a la máquina virtual de servicio. Notifica el estado de mantenimiento de la plataforma de Guest Introspection y mantiene registros de la configuración de la máquina virtual del servicio en el archivo `muxconfig.xml`.

- Ops Agent (motor de contexto y cliente de Guest Introspection): reenvía la configuración de Guest Introspection al agente de host de Guest Introspection (multiplexor de contexto). También transmite el estado de la solución a NSX Manager.
- EAM: NSX Manager utiliza ESXi Agent Manager para implementar una máquina virtual de servicio de partners en cada host del clúster configurado para protección.
- Thin Agent: es el agente de introspección de redes o archivos que se ejecuta en las máquinas virtuales invitadas. También intercepta las actividades de redes y archivos que se reenvían a la máquina virtual de servicio a través del agente de host. Este agente forma parte de VMware Tools. Reemplaza al agente tradicional proporcionado por los proveedores de seguridad antivirus o antimalware. Se trata de un agente genérico y ligero que facilita la descarga de archivos y procesos para la exploración en la máquina virtual de servicio proporcionada por el proveedor.

Conceptos clave de la protección de endpoints

El flujo de trabajo de protección de endpoints necesita que los partners registren sus servicios con NSX-T Data Center y que un administrador consuma estos servicios. Hay algunos conceptos que le permitirán comprender mejor el flujo de trabajo.

- Definición de servicio: los partners definen servicios con los atributos nombre, descripción, factores de forma compatibles, atributos de implementación que incluyen interfaces de red y la ubicación del paquete OVF del dispositivo que utilizará la SVM.
- Inserción de servicios: NSX proporciona el marco de inserción de servicios que permite a los partners integrar soluciones de redes y seguridad con la plataforma de NSX. La solución Guest Introspection es una de estas formas de inserción de servicios.
- Perfiles de servicio y plantillas de proveedor: los partners registran plantillas de proveedor que exponen los niveles de protección de las directivas. Por ejemplo, los niveles de protección pueden clasificarse como Gold, Silver o Platinum. Los perfiles de servicio se pueden crear a partir de plantillas de proveedor, lo que permite a los administradores de NSX asignar un nombre a las plantillas de proveedor según su preferencia. En el caso de los servicios que no sean de Guest Introspection, los perfiles de servicio permiten una personalización adicional mediante atributos. A continuación, los perfiles de servicio se pueden utilizar en las reglas de directiva de protección de endpoints para configurar la protección de los grupos de máquinas virtuales definidos en NSX. Como administrador, puede crear grupos según el nombre, las etiquetas o los identificadores de la máquina virtual. De forma opcional, se pueden crear varios perfiles de servicio a partir de una única plantilla de proveedor.
- Directiva de protección de endpoints: una directiva es una recopilación de reglas. Cuando disponga de varias directivas, organícelas en el orden que desea ejecutarlas. Lo mismo ocurre con las reglas definidas en una directiva. Por ejemplo, la directiva A tiene tres reglas y la directiva B tiene cuatro, y se organizan en secuencia, de manera que la directiva A precede a la directiva B. Cuando Guest Introspection comienza a ejecutar directivas, las reglas de la directiva A se ejecutan antes que las de la directiva B.

- **Regla de protección de endpoints:** como administrador de NSX, puede crear reglas que especifiquen los grupos de máquinas virtuales que se van a proteger y, a continuación, seleccionar el nivel de protección para esos grupos especificando el perfil de servicio para cada regla.
- **Instancia de servicio:** hace referencia a la máquina virtual de servicio en un host. VCenter considera las máquinas virtuales de servicio como máquinas virtuales especiales, y estas se inician antes de que las máquinas virtuales invitadas se enciendan y se detengan después de que todas las máquinas virtuales invitadas estén apagadas. Hay una instancia de servicio por servicio por host.

Importante El número de instancias de servicio es igual al número de hosts en los que el servicio ejecuta el host. Por ejemplo, si tiene ocho hosts en un clúster y el servicio de partners se implementó en dos clústeres, el número total de instancias de servicio en ejecución será 16 SVM.

- **Implementación del servicio:** como usuario admin, implemente las máquinas virtuales del servicio de partners a través de NSX-T en cada clúster. Las implementaciones se administran a nivel de clúster, de modo que, cuando se agrega un host al clúster, EAM implementa automáticamente la máquina virtual de servicio en ellos.

La implementación automática de la SVM es importante porque si el servicio Distributed Resource Scheduler (DRS) está configurado en un clúster de vCenter, vCenter puede volver a equilibrar o distribuir las máquinas virtuales existentes en cualquier host que se haya agregado al clúster después de que la SVM y se haya implementado e iniciado en el nuevo host. Dado que las máquinas virtuales del servicio de partners necesitan la plataforma NSX-T para proporcionar seguridad a las máquinas virtuales invitadas, el host debe estar preparado como nodo de transporte.

Importante Una implementación de servicio hace referencia a un clúster en vCenter Server que se administra para implementar y configurar un servicio de partners.

- **Controlador de introspección de archivo:** instalado en la máquina virtual invitada, intercepta la actividad del archivo en la máquina virtual invitada.
- **Controlador de introspección de red:** instalado en la máquina virtual invitada, intercepta el tráfico de red, el proceso y la actividad del usuario en la máquina virtual invitada.

Tareas de alto nivel para la protección de endpoints

Los servicios de partners de terceros que contienen lógica de análisis de seguridad se registran con NSX-T Data Center para la protección de las máquinas virtuales invitadas. El servicio de partners se aplica cuando el administrador de NSX implementa los servicios registrados y aplica las directivas de protección de endpoint a los grupos de máquinas virtuales invitadas.

El flujo de trabajo de introspección de invitado para el caso práctico de protección del endpoint es el siguiente:

Figura 10-2. Flujo de trabajo de protección de endpoints

Tareas de flujo de trabajo	Rol/persona	Implementación
Registrar un servicio con NSX-T Data Center	Administrador de partners	Consola de partners
Registrar un servicio con NSX-T Data Center	Administrador de partners	Consola de partners
Registrar un servicio con NSX-T Data Center	Administrador de partners	Consola de partners
Implementar un servicio	Administrador de NSX	API e interfaz de usuario de NSX Manager
Ver detalles de la instancia de servicio	Administrador de NSX	API e interfaz de usuario de NSX Manager
Activar instancia de servicio	Administrador de NSX	API e interfaz de usuario de NSX Manager
Agregar un perfil de servicio	Administrador de NSX	API e interfaz de usuario de NSX Manager
Consumir la directiva de Guest Introspection	Administrador de NSX	API e interfaz de usuario de NSX Manager
Agregar y publicar reglas de protección de endpoints	Administrador de NSX	API e interfaz de usuario de NSX Manager
Supervisar el estado de la protección de endpoints	Administrador de NSX	API e interfaz de usuario de NSX Manager

Configurar la protección de endpoints

Proteja las máquinas virtuales invitadas que se ejecutan en un entorno de NSX-T Data Center mediante servicios de seguridad de partners de terceros.

Pasos de alto nivel para configurar las directivas de protección de endpoints:

- 1 Asegúrese de que se cumplan [Requisitos previos para configurar la protección de endpoints](#) antes de configurar la protección de endpoints en las máquinas virtuales invitadas.
- 2 Software compatible. Consulte [Software compatible](#).
- 3 Instale el controlador de introspección de archivos para máquinas virtuales Linux. Consulte [Instalar Thin Agent de Guest Introspection en máquinas virtuales Linux](#).
- 4 Instale el controlador de introspección de archivos para máquinas virtuales Windows. Consulte [Instalar Thin Agent de Guest Introspection en máquinas virtuales Linux](#).
- 5 Instale el controlador de introspección de redes para máquinas virtuales Linux. Consulte [Instalar el Thin Agent de Linux para introspección de red](#).
- 6 Cree un usuario con la función de administrador de partners de Guest Introspection. Consulte [Crear un usuario con la función de usuario admin de partners de Guest Introspection](#).

- 7 Registre el servicio de partners con NSX-T Data Center. Consulte la documentación sobre partners.
- 8 Implementar un servicio. Consulte [Implementar un servicio](#).
- 9 Consuma la directiva de Guest Introspection. Consulte [Consumir la directiva de Guest Introspection](#).
- 10 Agregue y publique reglas de protección de endpoints. Consulte [Agregar y publicar reglas de protección de endpoints](#).
- 11 Supervise las reglas de protección de endpoints. Consulte [Supervisar el estado de la protección de endpoints](#).

Requisitos previos para configurar la protección de endpoints

Antes de configurar la protección de endpoints en las máquinas virtuales invitadas, asegúrese de que se cumplan los requisitos previos.

Requisitos previos

- NSX Manager está instalado en todos los hosts.
- Prepare y configure el clúster de NSX-T Data Center como nodos de transporte aplicando perfiles de nodo de transporte. Una vez que el host está configurado como el nodo de transporte, se instalan los componentes de la introspección de invitado. Consulte la *Guía de instalación de NSX-T Data Center*.
- La consola de partners se instala y se configura para registrar servicios con NSX-T Data Center.
- Asegúrese de que las máquinas virtuales invitadas ejecuten la versión 9 del archivo VM Hardware Configuration o una versión posterior.
- Configure VMware Tools e instale las instancias de Thin Agent.
 - Consulte [Instalar Thin Agent de Guest Introspection en máquinas virtuales Linux](#).
 - Consulte [Instalar Thin Agent de Guest Introspection en máquinas virtuales de Windows](#).
 - Consulte [Instalar el Thin Agent de Linux para introspección de red](#).

Instalar Thin Agent de Guest Introspection en máquinas virtuales Linux

Guest Introspection es compatible con la introspección de archivos en Linux solo para antivirus. Para proteger las máquinas virtuales Linux con una solución de seguridad de Guest Introspection, debe instalar Thin Agent de Guest Introspection.

La instancia de Thin Agent de Linux está disponible como parte de los paquetes específicos del sistema operativo (OSP). Los paquetes se alojan en el portal de paquetes de VMware. El Administrador de Enterprise o Seguridad (Administrador no de NSX) puede instalar el agente en las máquinas virtuales invitadas fuera de NSX.

No es necesario instalar VMware Tools.

Según su sistema operativo Linux, realice los siguientes pasos con privilegios de raíz:

Requisitos previos

- Asegúrese de que la máquina virtual invitada tenga una versión compatible de Linux instalada:
 - Red Hat Enterprise Linux (RHEL) 7.4 (64 bits) GA
 - SUSE Linux Enterprise Server (SLES) 12 (64 bits) GA
 - Ubuntu 16.04.5 LTS (64 bits) GA
 - CentOS 7.4 GA
- Compruebe que GLib 2.0 esté instalado en la máquina virtual Linux.

Procedimiento

1 Para sistemas Ubuntu

- a Obtenga e importe las clave públicas de empaquetado de VMware mediante los siguientes comandos.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-  
RSA-KEY.pub  
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Cree un archivo llamado `vmware.list` en `/etc/apt/sources.list.d`
- c Edite el archivo con el siguiente contenido:

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- d Instale el paquete.

```
apt-get update  
apt-get install vmware-nsx-gi-file
```

2 Para sistemas RHEL7

- a Obtenga e importe las clave públicas de empaquetado de VMware mediante los siguientes comandos.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Cree un archivo llamado `vmware.repo` en `/etc/yum.repos.d`.
- c Edite el archivo con el siguiente contenido:

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

3 Instale el paquete.

```
yum install vmware-nsx-gi-file
```

4 Para sistemas SLES

- a Obtenga e importe las clave públicas de empaquetado de VMware mediante los siguientes comandos.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Agregue el siguiente repositorio:

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c Instale el paquete.

```
zypper install vmware-nsx-gi-file
```

5 Para sistemas CentOS

- a Obtenga e importe las clave públicas de empaquetado de VMware mediante los siguientes comandos.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Cree un archivo llamado `vmware.repo` en `/etc/yum.repos.d`.
- c Edite el archivo con el siguiente contenido:

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

Pasos siguientes

Compruebe que se esté ejecutando la instancia de Thin Agent utilizando el comando `vsepd status` de servicio con privilegios administrativos. El estado se debe estar ejecutando.

Instalar el Thin Agent de Linux para introspección de red

Instale el Thin Agent de Linux para realizar la introspección del tráfico de red.

Importante Para proteger las máquinas virtuales invitadas contra antivirus, no es necesario instalar Thin Agent de Linux para introspección de red.

El controlador de Thin Agent de Linux que se utiliza para realizar la introspección del tráfico de red depende de un controlador de código abierto.

Requisitos previos

Instale los siguientes paquetes:

- glib2
- libnetfilter-conntrack3/ libnetfilter-conntrack
- libnetfilter-queue1/ libnetfilter-queue
- iptables

Procedimiento

- 1 Para instalar el controlador de código abierto proporcionado por la introspección de invitado.

- a Agregue la siguiente URL como la dirección URL base de su sistema operativo.

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

- b Importe la clave de empaquetado de VMware.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c Actualice el repositorio e instale el controlador de código abierto.

```
apt-get install Guest-Introspection-for-VMware-NSX
```

- 2 Para instalar el Thin Agent de Linux que se utiliza para realizar la introspección del tráfico o de archivos.

- Para instalar paquetes de introspección de red y archivos, seleccione el paquete `vmware-nsx-gi` en el paso C.
- Para instalar paquetes de introspección de red, seleccione el paquete `vmware-nsx-gi-net` en el paso C.

- a Agregue la siguiente URL como la dirección URL base de su sistema operativo.

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

- b Importe la clave de empaquetado de VMware.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c Instale uno de los controladores.

```
vmware-nsx-gi
vmware-nsx-gi-net
```

Instalar Thin Agent de Guest Introspection en máquinas virtuales de Windows

Para proteger las máquinas virtuales mediante una solución de seguridad de Guest Introspection, debe instalar en ellas Thin Agent de Guest Introspection, también conocido como controladores de Guest Introspection. Los controladores de Guest Introspection se incluyen con VMware Tools para Windows, pero no forman parte de la instalación predeterminada. Para instalar Guest Introspection en una máquina virtual Windows, debe realizar una instalación personalizada y seleccionar los controladores.

Las máquinas virtuales de Windows con controladores de Guest Introspection instalados quedan automáticamente protegidas cuando se inician en un host ESXi con la solución de seguridad instalada. Las máquinas virtuales protegidas mantienen la protección de seguridad durante los apagados y reinicios e incluso después del traslado de vMotion a otro host ESXi con la solución de seguridad instalada.

- Si utiliza vSphere 6.0, consulte las instrucciones para instalar VMware Tools en [Instalar o actualizar manualmente VMware Tools en una máquina virtual Windows](#).
- Si utiliza vSphere 6.5, consulte estas instrucciones para instalar VMware Tools: <https://www.vmware.com/support/pubs/vmware-tools-pubs.html>.

Requisitos previos

Asegúrese de que una máquina virtual invitada tenga una versión compatible de Windows instalada. Los sistemas operativos de Windows siguientes son compatibles con NSX Guest Introspection:

- Windows XP SP3 y posteriores (32 bit)
- Windows Vista (32 bit)
- Windows 7 (32/64 bit)
- Windows 8 (32/64 bit)
- Windows 8.1 (32/64) (vSphere 6.0 y versiones posteriores)
- Windows 10
- Windows 2003 SP2 y posteriores (32/64 bit)
- Windows 2003 R2 (32/64 bit)
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (64 bit)
- Win2012 (64)
- Win2012 R2 (64) (vSphere 6.0 y versiones posteriores)
- Windows Server 2016
- Windows Server 2019

Procedimiento

- 1 Comience la instalación de VMware Tools y siga las instrucciones de su versión de vSphere. Seleccione **Instalación personalizada**.
- 2 Expanda la sección Controlador VMCI.

Las opciones disponibles varían en función de la versión de VMware Tools.

3 Seleccione el controlador que se instalará en la máquina virtual.

Controlador	Descripción
Controladores de vShield Endpoint	Instala los controladores de introspección de archivos (<code>vsepflt</code>) e introspección de red (<code>vnetflt</code>).
Controladores de Guest Introspection	Instala los controladores de introspección de archivos (<code>vsepflt</code>) e introspección de red (<code>vnetflt</code>).
Controlador de introspección de archivos de NSX y controlador de introspección de red de NSX	<p>Seleccione el controlador de introspección de archivos de NSX para instalar <code>vsepflt</code>.</p> <p>También puede seleccionar el controlador de introspección de red de NSX para instalar <code>vnetflt</code> (<code>vnetWFP</code> en Windows 10 o versiones posteriores).</p> <p>Nota Seleccione el controlador de introspección de red de NSX solo si utiliza las funciones de firewall de identidad o supervisión de endpoints.</p>

4 En el menú desplegable situado junto a los controladores que desea agregar, seleccione Esta función se instalará en el disco duro local.

5 Siga los pasos restantes del procedimiento.

Pasos siguientes

Compruebe que se esté ejecutando la instancia de Thin Agent utilizando el comando `fltmc` con privilegios administrativos. La columna Nombre de filtro de la salida enumera la instancia de Thin Agent con una entrada `vsepflt`.

Software compatible

Guest Introspection es interoperable con versiones específicas de software.

VMware Tools

VMware Tool 10.3.10 es compatible.

Compruebe la interoperabilidad entre VMware Tools y NSX-T. Consulte [Matrices de interoperabilidad de productos de VMware](#).

Sistema operativo compatible

- Windows 7
- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server
- CentOS 7.4 GA
- RHEL 7.4 GA

- Ubuntu 16.04.5 LTS (64 bits)
- SLES 12 GA

Hosts compatibles

Para los hosts ESXi admitidos, consulte [Matrices de interoperabilidad de productos de VMware](#).

Crear un usuario con la función de usuario admin de partners de Guest Introspection

Asigne un usuario con la función de usuario admin de partners de Guest Introspection disponible en NSX-T Data Center.

Nota: Se recomienda registrar los servicios de partner mediante un usuario que esté asociado a la función de usuario admin de partners de Guest Introspection para evitar problemas de seguridad.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema** → **Usuario** → **Asignaciones de funciones**.
- 3 Haga clic en **Agregar**.
- 4 Seleccione el usuario y asígnele la función **Administrador de partners de GI**.

Pasos siguientes

Registre los servicios con NSX-T Data Center. Consulte [Registrar un servicio con NSX-T Data Center](#).

Registrar un servicio con NSX-T Data Center

Registre los servicios de seguridad de terceros con NSX-T Data Center.

Requisitos previos

- Asegúrese de que se cumplan los requisitos previos. Consulte [Requisitos previos para configurar la protección de endpoints](#).
- Asegúrese de que se asigne la función Usuario admin de partners de GI a un usuario de vIDM. Esta función se utiliza para registrar servicios con NSX-T Data Center.

Procedimiento

- 1 Inicie sesión con privilegios de Usuario admin de partners de GI en la consola de partners.
- 2 Registre un servicio y una plantilla de proveedor, y configure la solución de partners con NSX-T Data Center. Consulte la documentación para partners.

Pasos siguientes

Consulte el catálogo de los servicios de partners. Consulte [Vista de catálogo de los servicios de partners](#).

Vista de catálogo de los servicios de partners

La página Catálogo muestra todos los partners y los servicios que están registrados en NSX-T Data Center.

Requisitos previos

- Los partners registran los servicios con NSX-T Data Center.
- Los servicios se implementan en un clúster.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Implementaciones de servicio > Catálogo**.
- 3 Haga clic en **Ver** en un servicio. La página Implementación muestra los detalles acerca del servicio, como el estado de implementación, los detalles de red, los detalles del clúster, etc.

Pasos siguientes

Actualice una máquina virtual de servicio de partners.

Implementar un servicio

Después de registrar un servicio, debe implementar una instancia del servicio para iniciar el procesamiento del tráfico de red.

Implemente máquinas virtuales de servicio de partners que ejecuten el motor de seguridad de partner en todos los hosts de NSX-T Data Center de un clúster. El servicio ESX Agency Manager (EAM) de vSphere se utiliza para implementar las máquinas virtuales del servicio de partners en cada host. Después de implementar las SVM, puede crear reglas de directiva utilizadas por las SVM para proteger las máquinas virtuales invitadas.

Requisitos previos

- Todos los hosts se administran mediante vCenter Server.
- Los servicios de partners están registrados con NSX-T Data Center y listos para la implementación.
- Los administradores de NSX-T Data Center pueden acceder a los servicios de partners y las plantillas de proveedor.
- La máquina virtual de servicio y la instancia de Service Manager de partners (consola) deben poder comunicarse entre sí en el nivel de la red de administración.

- Prepare los hosts como nodos de transporte de NSX-T Data Center:
 - Cree una zona de transporte.
 - Cree un grupo de direcciones IP para direcciones IP de endpoints de túneles.
 - Cree un perfil de vínculo superior.
 - Agregue un perfil de nodo de transporte a fin de preparar un clúster para la implementación automática de los nodos de transporte de NSX-T Data Center.
 - Configure un host administrado o independiente.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Vaya a la pestaña **Sistema** y haga clic en **Implementación del servicio**.
- 3 En el menú desplegable Servicio de partners, seleccione el servicio que desea implementar.
- 4 Haga clic en **Implementación** y en **Implementar servicio**.
- 5 Introduzca el nombre de implementación del servicio.
- 6 En el campo Administrador de equipo, seleccione el recurso informático en la instancia de vCenter Server para implementar el servicio.
- 7 En el campo Clúster, seleccione el clúster donde deben implementarse los servicios.
- 8 En el menú desplegable Almacén de datos, puede hacer lo siguiente:
 - a Seleccione un almacén de datos como repositorio para la máquina virtual de servicio.
 - b Seleccione **Especificado en el host**. Esta opción significa que no es necesario seleccionar un almacén de datos y un grupo de puertos en este asistente. Puede configurar los ajustes del agente directamente en EAM en vCenter Server para que apunte a un almacén de datos específico y a un grupo de puertos que se utilizará para la implementación del servicio.

Para saber cómo configurar EAM, consulte la documentación de vSphere.

- 9 En la columna Red, haga clic en **Establecer**.
- 10 Establezca la interfaz de red de administración en **Especificado en el host** o **DVPG**.
- 11 Establezca el tipo de red en DHCP o Grupo de direcciones IP estáticas. Si establece el tipo de red en Grupo de direcciones IP estáticas, seleccione en la lista de grupos de direcciones IP disponibles.
- 12 En el campo Especificación de implementación, seleccione la implementación basada en host para implementar el servicio en todos los hosts. En función de los servicios registrados por el partner, se pueden implementar varios servicios como parte de una máquina virtual de un solo servicio.
- 13 En el campo Plantilla de implementación, seleccione la plantilla de implementación registrada.

14 Haga clic en **Guardar**.

Resultados

Cuando se agrega un nuevo host al clúster, EAM implementa automáticamente el servicio de la máquina virtual en el nuevo host. El proceso de implementación puede tardar algún tiempo, según la implementación del proveedor. Puede ver el estado en la interfaz de usuario de NSX Manager. El servicio está implementado correctamente en el host cuando el estado pasa a ser `Deployment Successful`.

Para quitar el host de un clúster, en primer lugar debe colocarlo en modo de mantenimiento. A continuación, seleccione la opción para migrar las máquinas virtuales invitadas a otro host y, así, completar la migración.

Pasos siguientes

Conozca los detalles de implementación y el estado de mantenimiento de las instancias de servicio implementadas en los hosts. Consulte [Ver detalles de la instancia de servicio](#).

Ver detalles de la instancia de servicio

Conozca los detalles de implementación y el estado de mantenimiento de la instancia de servicio implementada en los hosts miembro de un clúster.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Implementaciones de servicio > Instancias de servicio**.
- 3 En el menú desplegable Servicio de partners, seleccione el servicio de partners para ver los detalles relacionados con las instancias de servicio.

Tabla 10-9.

Campo	Descripción
Nombre de instancia de servicio	Un identificador único que identifica la instancia de servicio en un host determinado.
Nombre de la implementación de servicio	El nombre que introdujo al implementar el servicio.
Implementado en	Dirección IP de host o FQDN
Modo de implementación	Clúster o Independiente.

Tabla 10-9. (continuación)

Campo	Descripción
Estado de implementación	El estado activo para determinar una implementación correcta.
Estado de mantenimiento	<p>Cuando se implementa la instancia de servicio, el estado de mantenimiento es <code>Listo</code>. Para cambiar el estado de <code>Listo</code> a <code>Activo</code>, realice los cambios de configuración necesarios. Consulte Activar instancia de servicio.</p> <p>Una vez que NSX-T Data Center haya aplicado correctamente los siguientes parámetros, el estado cambiará de <code>Listo</code> a <code>Activo</code>.</p> <ul style="list-style-type: none"> ■ Estado de solución: <code>Activo</code> ■ Conectividad entre NSX-T Data Center Guest Introspection Agent y NSX-T Data Center Ops Agent: <code>Activo</code> ■ Estado recibido el: <Día, Fecha, Hora>

Pasos siguientes

Abrir instancia de servicio. Consulte [Activar instancia de servicio](#).

Activar instancia de servicio

Después de implementar la instancia de servicio, deben realizarse ciertos parámetros en NSX-T Data Center para que el estado de mantenimiento sea activo.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Implementaciones de servicio > Instancias de servicio**.
- 3 En el menú desplegable Servicio de partners, seleccione el servicio de partners para ver los detalles relacionados con las instancias de servicio.
- 4 La columna Estado de mantenimiento muestra el estado de la instancia de servicio como `Listo`. Indica que la instancia de servicio está lista para configurarse con reglas de directiva de protección de endpoints para proteger las máquinas virtuales.
- 5 Los siguientes parámetros se deben aplicar en NSX-T Data Center para que el estado de mantenimiento cambie a `Activo`.
 - Las máquinas virtuales invitadas deben estar disponibles en el host.
 - Las máquinas virtuales invitadas deben estar encendidas.
 - Las reglas de protección de endpoints deben aplicarse a las máquinas virtuales invitadas.
 - Las máquinas virtuales invitadas deben estar configuradas con la versión compatible de VMTools y los controladores de introspección de archivos.

Pasos siguientes

Agregue un perfil de servicio. Consulte [Agregar un perfil de servicio](#).

Agregar un perfil de servicio

Las directivas de Guest Introspection pueden implementarse únicamente cuando un perfil de servicio está disponible en NSX-T Data Center. Los perfiles de servicio se crean a partir de una plantilla proporcionada por el partner. Los perfiles de servicio son una forma en la que el administrador puede elegir los niveles de protección (niveles de directiva Gold, Silver, Platinum) para una máquina virtual mediante la selección de las plantillas de proveedor proporcionadas por el proveedor.

Por ejemplo, un proveedor puede ofrecer los niveles de directiva Gold, Platinum y Silver. Cada perfil creado puede servir para un tipo diferente de carga de trabajo. Un perfil de servicio Gold proporciona un servicio antimalware completo a una carga de trabajo de tipo PCI, mientras que un perfil de servicio Silver solo proporciona protección antimalware básica a una carga de trabajo normal.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Seguridad > Protección de endpoints > Reglas de protección de endpoints > Perfiles de servicio**.
- 3 En el campo Servicio de partners, seleccione el servicio para el que desea crear un perfil de servicio.
- 4 Haga clic en **Agregar perfil de servicio**.
- 5 Introduzca el nombre del perfil de servicio y seleccione la plantilla de proveedor. Si lo desea, puede agregar etiquetas y una descripción.
- 6 Haga clic en **Guardar**.

El identificador de plantilla de proveedor que se utiliza para crear el perfil de servicio se pasa a la consola del partner. Los partners almacenan el identificador de proveedor para realizar un seguimiento del uso de aquellas máquinas virtuales invitadas que están protegidas por esta plantilla de proveedor.

Resultados

Después de crear el perfil de servicio, un usuario admin de NSX crea reglas para asociar un perfil de servicio a un grupo de máquinas virtuales antes de publicar la regla de directiva.

Pasos siguientes

Aplique la directiva de protección de endpoints en los grupos de máquinas virtuales invitadas que deben protegerse contra malware. Consulte [Consumir la directiva de Guest Introspection](#).

Consumir la directiva de Guest Introspection

Se puede aplicar una directiva en los grupos de máquinas virtuales mediante la creación de reglas que asocien los perfiles de servicio con grupos de máquinas virtuales. La protección se inicia inmediatamente después de que las reglas se aplican a un grupo de máquinas virtuales.

La directiva de protección de endpoints es un servicio de protección ofrecido por los partners para proteger a las máquinas virtuales invitadas contra el malware mediante la implementación de perfiles de servicio en máquinas virtuales invitadas. Una vez aplicada una regla a un grupo de máquinas virtuales, todas las máquinas virtuales invitadas dentro de ese grupo están protegidas por ese perfil de servicio. Cuando se produce un evento de acceso a archivos en una máquina virtual invitada, la instancia de Thin Agent de Guest Introspection (que se ejecuta en cada máquina virtual invitada) recopila el contexto del archivo (atributos de archivo, identificador de archivo y otros detalles de contexto) y notifica el evento a SVM. Si SVM desea examinar el contenido del archivo, solicita detalles mediante la biblioteca de API de EPSec. Tras un veredicto claro de SVM, la instancia de Thin Agent de Guest Introspection permite al usuario acceder al archivo. En caso de que SVM informe que el archivo está infectado, la instancia de Thin Agent de Guest Introspection deniega el acceso del usuario al archivo.

Para ejecutar un servicio de seguridad en un grupo de máquinas virtuales, debe realizar lo siguiente:

Procedimiento

- 1 Defina directivas y reglas.
- 2 Defina los criterios de pertenencia a un grupo de máquinas virtuales.
- 3 Defina las reglas para los grupos de máquinas virtuales.
- 4 Publique la regla.

Agregar y publicar reglas de protección de endpoints

Publicar reglas de directiva para grupos de máquinas virtuales significa asociar grupos de máquinas virtuales que deben protegerse con un perfil de servicio específico.

Procedimiento

- 1 En la sección Directivas, seleccione una directiva.
- 2 Haga clic en **Agregar** -> **Agregar regla**.
- 3 Introduzca el nombre de la regla nueva.
- 4 En el grupo Seleccionar grupos, haga clic en el icono de edición.
- 5 En la ventana Establecer grupos, seleccione el grupo de la lista de grupos existente o agregue uno nuevo.
 - a Para agregar un grupo, haga clic en **Agregar grupo**, introduzca los detalles y haga clic en **Guardar**.

Consulte [Agregar un grupo](#).

- 6 En la columna Grupo, seleccione el grupo de máquinas virtuales.
- 7 En la columna Perfiles de servicio, seleccione el perfil de servicio que proporciona el nivel de protección deseado a las máquinas virtuales invitadas en el grupo.
 - a Para agregar un perfil de servicio nuevo, haga clic en **Agregar perfil de servicio**, introduzca los detalles y haga clic en **Guardar**.
 Consulte [Agregar un perfil de servicio](#).
- 8 Haga clic en **Publicar**.

Resultados

Las directivas de protección de endpoints protegen los grupos de máquinas virtuales.

Pasos siguientes

Es posible que desee cambiar la secuencia de las reglas según el tipo de protección necesario para diferentes grupos de máquinas virtuales. Consulte [¿Cómo ejecuta Guest Introspection la directiva de protección de endpoints?](#)

Supervisar el estado de la protección de endpoints

Supervise el estado de configuración de las máquinas virtuales protegidas y sin protección, los problemas con el agente de host y las máquinas virtuales de servicio, y las máquinas virtuales configuradas con el controlador de introspección de archivos instalado como parte de VMTools.

Puede ver lo siguiente:

- Ver el estado de implementación de servicio.
- Ver el estado de la configuración de protección de endpoints.
- Ver el estado de capacidad establecido para la protección de endpoints.

Ver el estado de implementación de servicio

Consulte los detalles de implementación del servicio en el panel de control de supervisión.

Consulte el estado de la directiva EPP en todo el sistema.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Acceda a **Inicio > Supervisión - Paneles de control**.
- 3 En el menú desplegable, haga clic en **Supervisión - Sistema**.
- 4 Para ver el estado de la implementación en los clústeres del sistema, desplácese hasta el widget protección de endpoints y haga clic en el gráfico de anillos para ver las implementaciones correctas o incorrectas.

La página Implementaciones de servicio muestra los detalles de implementación.

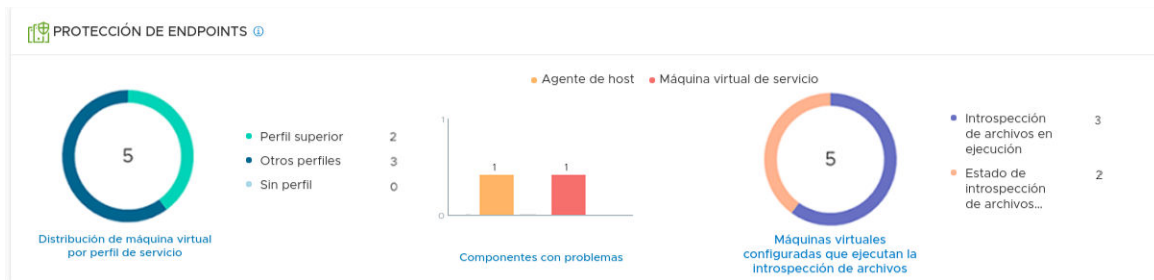
Ver el estado de la configuración de protección de endpoints

Consulte el estado de la configuración del servicio de protección de endpoints.

Consulte el estado de la directiva EPP en todo el sistema.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Acceda a **Inicio > Seguridad > Información general de seguridad**.
- 3 Para ver el estado de EPP en los clústeres, haga clic en el widget Seguridad.
- 4 En el panel Información general de seguridad, haga clic en **Configuración**.



- 5 En la sección Protección de endpoints, consulte:
 - a El widget Distribución de máquina virtual por perfil de servicio muestra:
 - 1 El número de máquinas virtuales protegidas por perfil superior. El perfil superior representa un perfil que protege el número máximo de máquinas virtuales en un clúster.
 - 2 Máquinas virtuales protegidas por perfiles de servicio restantes categorizadas en Otros perfiles.
 - 3 Máquinas virtuales no protegidas categorizadas en Sin perfil.

La página Reglas de protección de endpoints muestra las máquinas virtuales protegidas por directivas de protección de endpoints.

- b El widget Componentes con problemas muestra:
 - 1 Host: Problemas relacionados con el multiplexor de contexto.
 - 2 SVM: Problemas relacionados con las máquinas virtuales de servicio. Por ejemplo, el estado de SVM es inactivo, la conexión de SVM con la máquina virtual invitada está inactiva.

La columna Estado de la página implementación muestra problemas de estado.

- c El widget Máquinas virtuales configuradas que ejecutan la introspección de archivos muestra:
 - 1 Máquinas virtuales protegidas por el controlador de Introspección de archivos.

- 2 Máquinas virtuales en las que el estado del controlador de introspección de archivos es desconocido.

ESXi Agency Manager (EAM) intenta resolver algunos problemas relacionados con los hosts, las SVM y errores de configuración. Consulte [Solucionar problemas de servicios de partners](#).

Ver el estado de capacidad establecido para la protección de endpoints

Consulte el estado de capacidad del servicio de protección de endpoints.

Consulte el estado de capacidad de la directiva EPP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Acceda a **Inicio > Supervisión - Paneles de control**.
- 3 En el menú desplegable, haga clic en **Supervisión - Redes y seguridad**.
- 4 Para ver el estado de EPP en los clústeres, haga clic en el widget Seguridad.
- 5 En la página Información general de seguridad, haga clic en **Capacidad** y consulte el estado de capacidad de estos parámetros.

Límite	Capacidad máxima	Inventario actual (realizado)	Alerta de advertencia	Alerta crítica
Reglas de firewall distribuido	100.000	2	0%	70%
Secciones de firewall de todo el sistema	10.000	5	0,05%	70%

- a **Hosts con protección de endpoints en todo el sistema habilitada:** Si el número de host protegidos alcanza el límite de umbral, NSX Manager notificará una alerta de advertencia o una alerta crítica cuando se alcancen los límites de umbral correspondientes.
- b **Máquinas virtuales con protección de endpoints en todo el sistema habilitada:** Si el número de máquinas virtuales protegidas alcanza el límite de umbral, NSX Manager notificará una alerta de advertencia o una alerta crítica cuando se alcancen los límites de umbral correspondientes.

Nota Puede establecer límites de umbral para estos parámetros, ver el estado y recibir alertas cuando estos parámetros alcancen el límite de umbral establecido.

Administrar la protección de endpoints

Resuelva los conflictos entre directivas y los problemas de mantenimiento con las máquinas virtuales de servicio, y aprenda cómo funciona la directiva de protección de endpoints.

Solucionar problemas de servicios de partners

Si la máquina virtual del servicio de partners no es funcional, las máquinas virtuales invitadas no estarán protegidas contra malware.

En cada host, verifique que los siguientes servicios o procesos estén activos y en ejecución:

- El servicio ESXi Agency Manager (EAM) debe estar activo y en ejecución. Para comprobarlo, debe poder acceder a la siguiente URL.

```
https://<vCenter_Server_IP_Address>/eam/mob
```

Compruebe que ESXi Agency Manager esté conectado.

```
root> service-control --status vmware-eam
```

- No se deben eliminar los grupos de puertos de las SVM porque estos grupos de puertos son necesarios para garantizar que SVM siga protegiendo las máquinas virtuales invitadas.

```
https://<vCenter_Server_IP_Address>/ui
```

- En vCenter Server, vaya a la máquina virtual, haga clic en la pestaña **Redes** y compruebe si aparece **vmervice-vshield-pg**.
- El servicio de multiplexor de contexto (MUX) está activo y en ejecución. Compruebe que el VIB `nsx-context-mux` esté activo y en ejecución en el host.
- La interfaz de administración en la que NSX-T Data Center se comunica con la consola del servicio de partners debe estar activa.
- La interfaz de control que habilita la comunicación entre MUX y SVM debe estar activa. Se debe crear el grupo de puertos que conecta MUX con SVM. Tanto el grupo de puertos como la interfaz son necesarios para que el servicio de partners funcione.

Problemas de ESXi Agency Manager

En la tabla, se enumeran los problemas de ESXi Agency Manager que pueden resolverse mediante el botón Resolver en la interfaz de usuario de NSX Manager. Notifica a NSX Manager con detalles del error.

Tabla 10-10. Problemas de ESXi Agency Manager

Problema	Categoría	Descripción	Resolución
No se puede acceder al OVF de agente	Máquina virtual no implementada	Se espera implementar una máquina virtual de agente en un host, pero no es posible hacerlo porque ESXi Agency Manager no puede acceder al paquete OVF del agente. Puede suceder porque el servidor web que proporciona el paquete OVF está inactivo. El servidor web a menudo está integrado en la solución que creó Agency Manager.	El servicio ESXi Agency Manager (EAM) vuelve a intentar la descarga de OVF. Compruebe el estado de la consola de administración de partners. Haga clic en Resolver .
Versión de host no compatible	Máquina virtual no implementada	Se espera que se implemente una máquina virtual de agente en un host. Sin embargo, debido a problemas de compatibilidad, el agente no se implementó en el host.	Actualice el host o la solución para que el agente sea compatible con el host. Compruebe la compatibilidad de la SVM. Haga clic en Resolver .
Recursos insuficientes	Máquina virtual no implementada	Se espera que se implemente una máquina virtual de agente en un host. Sin embargo, el servicio ESXi Agency Manager (EAM) no implementó la máquina virtual del agente debido a que el host tiene menos recursos de CPU o de memoria.	El servicio ESXi Agency Manager (EAM) intenta volver a implementar la máquina virtual. Asegúrese de que los recursos de CPU y memoria estén disponibles. Compruebe el host y libere recursos. Haga clic en Resolver .
Espacio insuficiente	Máquina virtual no implementada	Se espera que se implemente una máquina virtual de agente en un host. Sin embargo, la máquina virtual del agente no se implementó porque el almacén de datos del agente en el host no tenía suficiente espacio libre.	El servicio ESXi Agency Manager (EAM) intenta volver a implementar la máquina virtual. Libere espacio en el almacén de datos. Haga clic en Resolver .
Red de la máquina virtual de agente faltante	Máquina virtual no implementada	Se espera implementar una máquina virtual de agente en un host, pero no es posible hacerlo porque no se configuró la red de agente en el host.	Agregue al host una de las redes especificadas en customAgentVmNetwork. El problema se resuelve automáticamente una vez que el almacén de datos esté disponible.

Tabla 10-10. Problemas de ESXi Agency Manager (continuación)

Formato de OVF no válido	Máquina virtual no implementada	Se espera aprovisionar una máquina virtual de agente en un host, pero no es posible hacerlo porque ocurre un error en el aprovisionamiento del paquete OVF. Es probable que el aprovisionamiento no funcione hasta que la solución que proporciona el paquete OVF se haya actualizado o revisado a fin de proporcionar un paquete OVF válido para la máquina virtual de agente.	El servicio ESXi Agency Manager (EAM) intenta volver a implementar la SVM. Consulte la documentación de la solución de partners o actualice la solución de partners para obtener el paquete de OVF válido. Haga clic en Resolver .
Grupo de IP de agente faltante	Máquina virtual apagada	Se espera que haya una máquina virtual de agente encendida, pero está apagada porque no hay direcciones IP definidas en la red de la máquina virtual del agente.	Defina la dirección IP en la red de la máquina virtual. Haga clic en Resolver .
Almacén de datos de la máquina virtual de agente faltante	Máquina virtual apagada	Se espera implementar una máquina virtual de agente en un host, pero no es posible hacerlo porque no se configuró el almacén de datos del agente en el host.	Agregue al host uno de los almacenes de datos especificados en customAgentVmDatastore. El problema se resuelve automáticamente una vez que el almacén de datos esté disponible.
Red de la máquina virtual de agente personalizado faltante	Red de la máquina virtual de agente faltante	Se espera implementar una máquina virtual de agente en un host, pero no es posible hacerlo porque no se configuró la red de agente en el host.	Agregue el host a una de las redes especificadas en una red de máquina virtual de agente personalizada. El problema se resuelve automáticamente cuando haya una red de máquina virtual personalizada disponible.
Almacén de datos de la máquina virtual de agente personalizado faltante	Almacén de datos de la máquina virtual de agente faltante	Se espera implementar una máquina virtual de agente en un host, pero no es posible hacerlo porque no se configuró el almacén de datos del agente en el host.	Agregue el host a uno de los almacenes de datos especificados en un almacén de datos de máquina virtual de agente personalizado. El problema se resuelve automáticamente.
Agencia huérfana	Problema de agencia	La solución que creó la agencia ya no está registrada con vCenter Server.	Registre la solución con vCenter Server.

Tabla 10-10. Problemas de ESXi Agency Manager (continuación)

Conmutador DvFilter huérfano	Problema de host	Existe un conmutador dvFilter en un host, pero ningún agente del host depende de dvFilter. Esto sucede si se desconecta un host cuando se modifica la configuración de una agencia.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta conectar el host antes de que se actualice la configuración de la agencia.
Máquina virtual de agente desconocida	Problema de host	Se encontró una máquina virtual de agente en el inventario de vCenter Server que no corresponde a ninguna agencia en esta instancia del servidor vSphere ESX Agent Manager.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta colocar la máquina virtual en el inventario al que pertenece.
Propiedad de OVF no válida	Problema de máquina virtual	Una máquina virtual de agente debe estar encendida, pero una propiedad de OVF está ausente o tiene un valor no válido.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta volver a configurar la propiedad de OVF correcta.
Máquina virtual dañada	Problema de máquina virtual	Una máquina virtual de agente está dañada.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta reparar la máquina virtual.
Máquina virtual huérfana	Problema de máquina virtual	Existe una máquina virtual del agente en un host, pero el host ya no forma parte del ámbito de la agencia. Esto sucede si se desconecta un host cuando se modifica la configuración de la agencia.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta volver a conectar el host a la configuración de la agencia.
Máquina virtual implementada	Problema de máquina virtual	Se espera quitar una máquina virtual de agente de un host, pero esta no se eliminó. El motivo específico por el que vSphere ESX Agent Manager no pudo eliminar la máquina virtual de agente: por ejemplo, porque el host está en modo de mantenimiento, apagado o en modo de espera.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta eliminar la máquina virtual del agente del host.

Tabla 10-10. Problemas de ESXi Agency Manager (continuación)

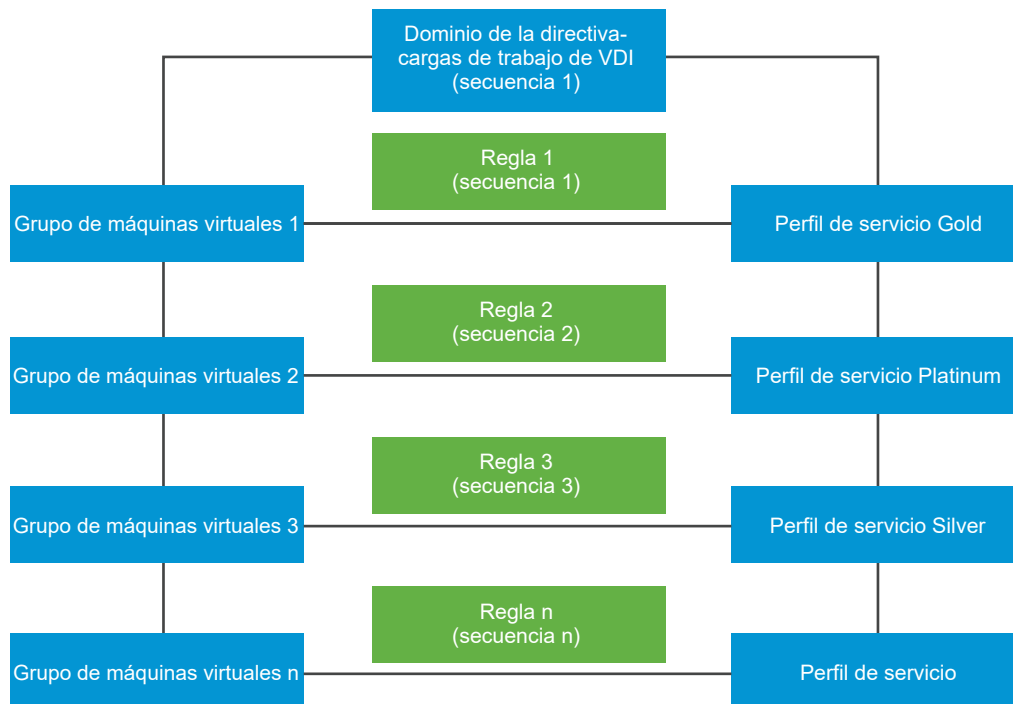
Máquina virtual apagada	Problema de máquina virtual	Se espera que una máquina virtual de agente esté encendida, pero está apagada.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta encender la máquina virtual.
Máquina virtual encendida	Problema de máquina virtual	Se espera que una máquina virtual de agente esté apagada, pero está encendida.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta apagar la máquina virtual.
Máquina virtual suspendida	Problema de máquina virtual	Se espera que una máquina virtual de agente esté encendida, pero está suspendida.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta encender la máquina virtual.
Carpeta incorrecta de máquina virtual	Problema de máquina virtual	Se espera que una máquina virtual de agente esté ubicada en una carpeta designada para ella, pero se encuentra en otra carpeta.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta colocar la máquina virtual del agente en la carpeta designada.
Grupo de recursos incorrecto de máquina virtual	Problema de máquina virtual	Se espera que una máquina virtual de agente esté ubicada en un grupo de recursos designado para ella, pero se encuentra en otro grupo de recursos.	Haga clic en Resolver . El servicio ESXi Agency Manager (EAM) intenta colocar la máquina virtual del agente en un grupo de recursos designado.
Máquina virtual no implementada	Problema de agente	Se espera que una máquina virtual de agente esté implementada en un host, pero no se implementó. El motivo específico por el que ESXi Agent Manager no pudo implementar el agente: por ejemplo, porque no se puede acceder al paquete OVF para el agente o porque falta una configuración del host. Este problema también ocurre si la máquina virtual de agente se elimina explícitamente del host.	Haga clic en Resolver para implementar la máquina agente virtual.

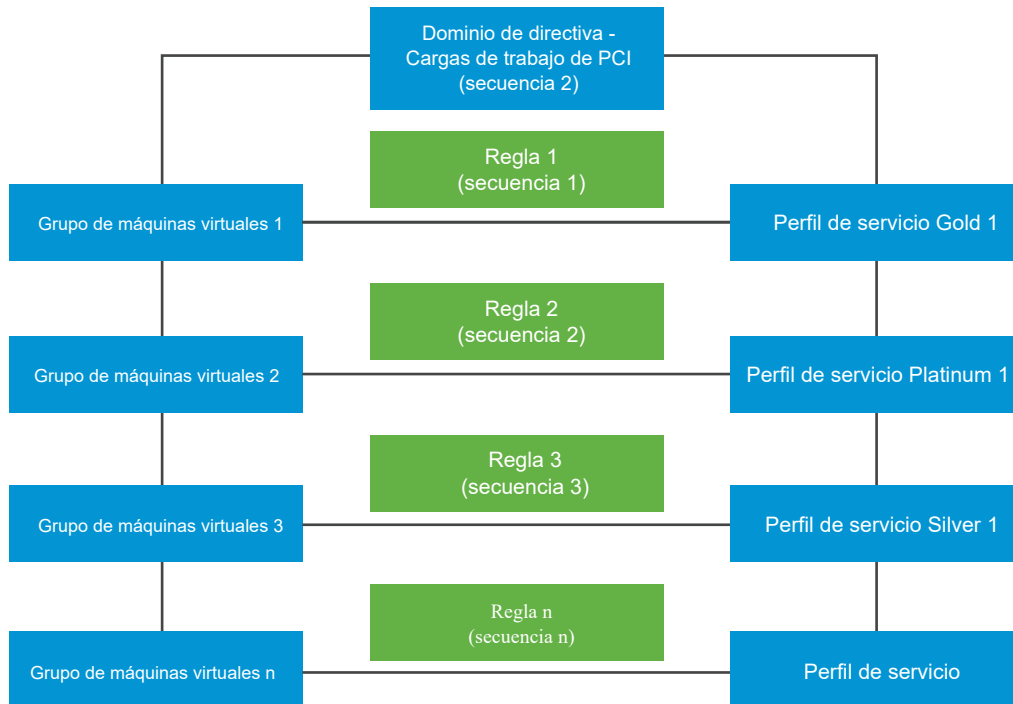
A continuación, configure la protección de endpoints para grupos de máquinas virtuales. Consulte [Protección de endpoints](#).

¿Cómo ejecuta Guest Introspection la directiva de protección de endpoints?

Las directivas de protección de endpoints se aplican en un orden específico. Al diseñar las directivas, tenga en cuenta el número de secuencia asociado a las reglas y los dominios que alojan a las reglas.

Escenario: De las muchas cargas de trabajo que se ejecutan en la organización, para fines ilustrativos tomaremos en cuenta las cargas de trabajo de máquinas virtuales que ejecutan la infraestructura de escritorio virtual (Virtual Desktop Infrastructure, VDI) y las cargas de trabajo de máquinas virtuales que ejecutan estándares de seguridad de datos para la industria de tarjetas de pago (Payments Cards Industry Data Security Standards, PCI-DSS). Parte de los empleados de la organización requiere acceso al escritorio remoto, el cual conforma la carga de trabajo de la infraestructura de escritorio virtual (Virtual Desktop Infrastructure, VDI). Estas cargas de trabajo de la VDI pueden requerir una directiva de protección de nivel Gold en función de las reglas de cumplimiento configuradas por la organización. Por su parte, una carga de trabajo de PCI-DSS necesita el nivel más alto de protección, el nivel Platinum.





Como hay dos tipos de cargas de trabajo, debe crear dos directivas: una de cada uno para las cargas de trabajo de VDI y para las cargas de trabajo del servidor. Dentro de cada directiva o sección, defina un dominio para que refleje el tipo de carga de trabajo; a su vez, dentro de esa sección, defina las reglas para esa carga de trabajo. Publique las reglas para iniciar los servicios de Guest Introspection en máquinas virtuales invitadas. Guest Introspection utiliza internamente los dos números de secuencia: el número de secuencia de la directiva y el número de secuencia de la regla para determinar la secuencia completa de reglas que se ejecutarán. Cada regla tiene dos propósitos: determina qué máquinas virtuales se van a proteger y qué directiva de protección debe aplicarse para proteger las máquinas virtuales.

Para cambiar el orden de la secuencia, arrastre una regla en la interfaz de usuario del administrador de directivas de NSX-T. Si lo prefiere, puede asignar explícitamente el número de secuencia para las reglas mediante la API.

Otra opción es hacer una llamada API a NSX-T Data Center para definir una regla manualmente mediante la asociación de un perfil de servicio con un grupo de máquinas virtuales y declarar el número de secuencia de las reglas. Los detalles de la API y de los parámetros se detallan en la *guía de API* de NSX-T Data Center. Realice llamadas API de configuración de servicios para aplicar perfiles a entidades, como grupos de máquinas virtuales, etc.

Tabla 10-11. API de NSX-T Data Center utilizadas para definir la regla que aplique el perfil de servicio a grupos de máquinas virtuales

API	Detalles
Obtenga todos los detalles de configuración de servicio.	<p>GET /api/v1/service-configs</p> <p>La API de configuración de servicio devuelve los detalles del perfil de servicio que se aplican a un grupo de máquinas virtuales, el grupo de máquinas virtuales protegidas y el número de secuencia o precedencia que decide la prioridad de la regla.</p>
Cree una configuración de servicio.	<p>POST /api/v1/service-configs</p> <p>La API de configuración de servicio toma parámetros de entrada de un perfil de servicio, el grupo de máquinas virtuales que deben protegerse y el número de secuencia o precedencia que debe aplicarse a la regla.</p>
Elimine una configuración de servicio.	<p>DELETE /api/v1/service-configs/<config-set-id></p> <p>La API de configuración de servicio elimina la configuración aplicada en el grupo de máquinas virtuales.</p>
Obtenga los detalles de una configuración específica.	<p>GET /api/v1/service-configs/<config-set-id></p> <p>Obtenga los detalles de una configuración específica.</p>
Actualice una configuración de servicio.	<p>PUT /api/v1/service-configs/<config-set-id></p> <p>Actualice una configuración de servicio.</p>
Obtenga perfiles efectivos.	<p>GET /api/v1/service-configs/effective-profiles?resource_id=<resource-id>&resource_type=<resource-type></p> <p>La API de configuración de servicio devuelve únicamente ese perfil que se aplica en un determinado grupo de máquinas virtuales.</p>

Administre las reglas de forma eficaz siguiendo estas recomendaciones:

- Establezca un número de secuencia superior en una directiva para las reglas que se deben ejecutar primero. Desde la interfaz de usuario, puede arrastrar las directivas para cambiar su prioridad.
- De forma similar, establezca un número de secuencia superior para las reglas dentro de cada directiva.
- Según cuántas reglas necesite, puede colocar las reglas separadas en múltiplos de 2, 3, 4 o incluso 10. Por lo tanto, dos reglas consecutivas que están separadas en 10 posiciones proporcionan más flexibilidad para volver a establecer la secuencia de las reglas sin tener

que cambiar el orden de la secuencia de todas las reglas. Por ejemplo, si no desea definir una gran cantidad de reglas, puede establecer 10 posiciones de separación entre cada regla. Por lo tanto, la regla 1 obtiene un número de secuencia 1, la regla 2 obtiene un número de secuencia 10, la regla 3 obtiene un número de secuencia 20 y así sucesivamente. Esta recomendación proporciona flexibilidad para administrar las reglas de forma eficaz de modo que no sea necesario volver a ordenar todas las reglas.

Internamente, la introspección de invitado establece la secuencia de estas reglas de directiva de la siguiente manera.

```
Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1↔ Service Profile ↔ Sequence Number 1 (1001)

- Rule 2 : Group 1↔ Service Profile ↔ Sequence Number 10 (1010)

- Rule 3 : Group 1↔ Service Profile ↔ Sequence Number 20 (1020)

- Rule 4 : Group 1↔ Service Profile ↔ Sequence Number 30 (1030)


Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1↔ Service Profile ↔ Sequence Number 1 (2001)

- Rule 2 : Group 1↔ Service Profile ↔ Sequence Number 10 (2010)

- Rule 3 : Group 1↔ Service Profile ↔ Sequence Number 20 (2020)

- Rule 4 : Group 1↔ Service Profile ↔ Sequence Number 30 (2030)
```

En función de los números de secuencia anteriores, Guest Introspection ejecuta las reglas de la directiva 1 antes de ejecutar las reglas de la directiva 2.

No obstante, hay situaciones donde no se aplican las reglas deseadas a un grupo de máquinas virtuales o a una máquina virtual. Estos conflictos deben solucionarse para aplicar los niveles de protección de directiva que desee.

Resolución de conflictos con la directiva de endpoints

Piense en un escenario con dos dominios de directiva, cada uno de los cuales consta de varias reglas. Como usuario admin, no siempre sabrá con seguridad cuáles son las máquinas virtuales que pueden acabar perteneciendo a un grupo, ya que las máquinas virtuales se asocian a un grupo en función de criterios de pertenencia dinámicos, como el nombre del sistema operativo, el nombre del equipo, el usuario o el etiquetado.

Los conflictos surgen en los siguientes escenarios:

- Una máquina virtual forma parte de dos grupos, y cada grupo está protegido por un perfil diferente.

- Una máquina virtual de servicio de partners está asociada con más de un perfil de servicio.
- Una regla inesperada se ejecutó en una máquina virtual invitada, o una regla no se ejecuta en un grupo de máquinas virtuales.
- El número de secuencia no se asigna a los dominios o las reglas de directivas.

Tabla 10-12. Resolver conflictos con la directiva

Escenario	Flujo de protección de endpoints esperado	Resolución
<p>Una máquina virtual consigue la pertenencia a varios grupos. Cada grupo está protegido por un tipo de perfil de servicio diferente.</p> <p>No se aplicó la protección esperada a la máquina virtual.</p>	<p>Un grupo de máquinas virtuales creado con un criterio de pertenencia implica que las máquinas virtuales se agregan al grupo de forma dinámica. En ese caso, la misma máquina virtual puede formar parte de varios grupos. No hay forma de determinar previamente el grupo del cual va a formar parte la máquina virtual porque los criterios de pertenencia cargan la máquina virtual en el grupo de manera dinámica.</p> <p>Supongamos que la máquina virtual 1 forma parte del grupo 1 y del grupo 2.</p> <ul style="list-style-type: none"> ■ Regla 1: al grupo 1 (según el nombre del sistema operativo) se le aplica el perfil Gold (perfil de servicio) con el número de secuencia 1 ■ Regla 2: al grupo 2 (según la etiqueta) se le aplica el perfil Platinum con el número de secuencia 10 <p>La directiva de protección de endpoints ejecuta el perfil de servicio Gold en la máquina virtual 1, pero no ejecuta el perfil de servicio Platinum en la máquina virtual 1.</p>	<p>Cambie el número de secuencia de la regla 2 de modo que se ejecute antes de la regla 1.</p> <ul style="list-style-type: none"> ■ En la interfaz de usuario del administrador de directivas de NSX-T, arrastre la regla 2 antes de la regla 1 en la lista de reglas. ■ Mediante la API de administrador de directivas de NSX-T, agregue manualmente un número de secuencia superior para la regla 2.
<p>Una regla asocia el mismo perfil de servicio para proteger los dos grupos de máquinas virtuales.</p> <p>La protección de endpoints no ejecuta la regla en el segundo grupo de máquinas virtuales.</p>	<p>Esta protección solo ejecuta el primer perfil de servicio en la máquina virtual debido a que el mismo perfil de servicio no se puede volver a aplicar a ninguna otra regla entre directivas o dominios.</p> <p>Supongamos que la máquina virtual 1 forma parte del grupo 1 y del grupo 2.</p> <p>Regla 1: al grupo 1 (según el nombre del sistema operativo) se le aplica el perfil Gold (perfil de servicio)</p> <p>Regla 2: al grupo 2 (según la etiqueta) se le aplica el perfil Gold (perfil de servicio)</p>	<ul style="list-style-type: none"> ■ Agregue el grupo 2 a la regla 1. (Regla 1: a los grupos 1 y 2 se les aplica el perfil 1)

Máquinas virtuales en cuarentena

Una vez que las reglas se aplican a los grupos de máquinas virtuales, en función del nivel de protección y la etiqueta que hayan establecido los partners, podría haber máquinas virtuales que se identifiquen como infectadas y que haya que poner en cuarentena.

Los partners utilizan la API con la etiqueta `virus_found=true` para etiquetar a las máquinas virtuales que están infectadas. Las máquinas virtuales afectadas se asocian con la etiqueta `virus_found=true`.

Como administrador, puede crear un grupo de cuarentena predefinido que se base en una etiqueta con el valor `virus_found=true`, de manera que el grupo se rellene con las máquinas virtuales infectadas conforme se vayan etiquetando. Como usuario admin, puede establecer reglas de firewall específicas para el grupo de cuarentena. Puede configurar las reglas de firewall para el grupo de cuarentena. Por ejemplo, puede decidir bloquear todo el tráfico entrante y saliente del grupo de cuarentena.

Comprobar el estado de mantenimiento de las instancias de servicio

El estado de mantenimiento de una instancia de servicio depende de muchos factores: el estado de la solución del partner, la conectividad entre Guest Introspection Agent (multiplexor de contexto) y el motor de contexto (Ops Agent), y la disponibilidad de la información de Guest Introspection Agent y la información del protocolo de la SVM con NSX Manager.

Procedimiento


- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Implementaciones de servicio > Instancias de servicio**.
- 3 En la columna Estado de mantenimiento, haga clic en  para conocer el estado de la instancia de servicio.

Tabla 10-13. Estado de mantenimiento de la instancia de servicio de terceros

Parámetro	Descripción
Estado de mantenimiento recibido a las	La última marca de tiempo en la que NSX Manager recibió los detalles del estado de mantenimiento de la instancia de servicio.
Estado de la solución	El estado de la solución del partner que se ejecuta en una SVM. El estado ACTIVO indica que la solución del partner se está ejecutando correctamente.
Conectividad entre Guest Introspection Agent de NSX-T Data Center y Ops Agent de NSX-T Data Center	El estado es ACTIVO cuando Guest Introspection Agent de NSX-T Data Center (multiplexor de contexto) está conectado con Ops Agent (incluye el motor de contexto). El multiplexor de contexto reenvía la información del estado de las SVM al motor de contexto. Adicionalmente, estas comparten la configuración SVM-VM entre sí para determinar qué máquinas virtuales invitadas están protegidas mediante la SVM.
Versión de protocolo de máquina virtual del servicio	La versión del protocolo de transporte que se utiliza internamente para resolver problemas.
Información de Guest Introspection Agent de NSX-T Data Center	Representa la compatibilidad de versiones del protocolo entre la SVM y Guest Introspection Agent de NSX-T Data Center.

- 4 Si el estado de mantenimiento es *Activo* (el estado que aparece en color verde) y la consola del partner muestra que todas las máquinas virtuales invitadas están protegidas, el estado de mantenimiento de la instancia de servicio es *Activo*.
- 5 Si el estado de mantenimiento es *Activo* (el estado que aparece en color verde), pero la consola del partner muestra que el estado de las máquinas virtuales invitadas es no protegido, realice el siguiente paso:
 - a Póngase en contacto con el soporte de VMware para solucionar el problema. El estado de mantenimiento de la instancia de servicio podría ser inactivo sin que esto lo refleje correctamente la interfaz de usuario de NSX Manager.
- 6 Si el estado de mantenimiento es *Inactivo* (el estado que aparece en color rojo), indica que uno o varios factores que determinan el estado de la instancia de servicio están inactivos.

Tabla 10-14. Solucionar problemas del estado de mantenimiento

Atributo del estado de mantenimiento	Resolución
El estado de la solución es <i>Inactivo</i> o No disponibles.	<ol style="list-style-type: none"> 1 Compruebe que el estado de implementación del servicio es <i>Activo</i> (verde). Si se produce algún error, consulte Solucionar problemas de servicios de partners. 2 Asegúrese de que al menos una máquina virtual invitada del host afectado esté protegida con una directiva de protección de endpoint. 3 Desde la consola del partner, compruebe si el servicio de la solución se está ejecutando en la SVM del host. Consulte la documentación del partner para conocer más detalles. 4 Si ninguno de los pasos anteriores resuelve el problema, póngase en contacto con el soporte de VMware.
El estado de la conectividad entre Guest Introspection Agent de NSX-T Data Center y Ops Agent de NSX-T Data Center es <i>Inactivo</i> .	<ol style="list-style-type: none"> 1 Compruebe que el estado de implementación del servicio es <i>Activo</i> (verde). Si se produce algún error, consulte Solucionar problemas de servicios de partners. 2 Asegúrese de que al menos una máquina virtual invitada del host afectado esté protegida con una directiva de protección de endpoint. 3 Desde la consola del partner, compruebe si el servicio de la solución se está ejecutando en la SVM del host. Consulte la documentación del partner para conocer más detalles. 4 Si ninguno de los pasos anteriores resuelve el problema, póngase en contacto con el soporte de VMware.

Tabla 10-14. Solucionar problemas del estado de mantenimiento (continuación)

Atributo del estado de mantenimiento	Resolución
La versión del protocolo de máquina virtual de servicio es No disponible.	<ol style="list-style-type: none"> 1 Compruebe que el estado de implementación del servicio es <code>Activo</code> (verde). Si se produce algún error, consulte Solucionar problemas de servicios de partners. 2 Asegúrese de que al menos una máquina virtual invitada del host afectado esté protegida con una directiva de protección de endpoint. 3 Desde la consola del partner, compruebe si el servicio de la solución se está ejecutando en la SVM del host. Consulte la documentación del partner para conocer más detalles. 4 Si ninguno de los pasos anteriores resuelve el problema, póngase en contacto con el soporte de VMware.
El estado de la información de Guest Introspection Agent de NSX-T Data Center es No disponible.	Póngase en contacto con el soporte de VMware.

Eliminar servicios de partners

Para eliminar los servicios de partners, realice una llamada API. Antes de hacer la llamada API para eliminar los servicios de partners o las SVM implementadas en un host, debe realizar las siguientes acciones desde la interfaz de usuario de NSX Manager.

Para eliminar los servicios de partners:

Procedimiento

- 1 Quite las reglas de EPP aplicadas a grupos de máquinas virtuales que se ejecutan en el host.
- 2 Quite la protección del perfil de servicio que se aplica a grupos de máquinas virtuales.
- 3 Para quitar las SVM de enlace con la solución mediante Service Manager de partners, realice la siguiente llamada API.

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/{{service_id}}/
solution-configs/<solution-config-id>
```

- 4 Para eliminar la implementación del servicio, realice la siguiente llamada API.

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/<service-id>/service-
deployments/<service-deployment-id>
```

Consulte la *Guía de API de NSX-T Data Center* para obtener más información acerca de los parámetros de la API.

Perfiles de seguridad

Esta sección contiene perfiles que ajustan las operaciones de firewall: temporizadores de sesión, protección contra inundación y seguridad de DNS

Crear un temporizador de sesión

Los temporizadores de sesión definen el tiempo que se mantendrá una sesión en el firewall cuando esté inactiva.

Cuando se agota el tiempo de espera de sesión del protocolo, se cierra la sesión. En el firewall, se pueden especificar varios tiempos de espera para sesiones TCP, UDP e ICMP con el objetivo de aplicarlos a un grupo definido por el usuario o una puerta de enlace de nivel 0 o 1. Los valores de sesión predeterminados se pueden modificar dependiendo de las necesidades de su red. Tenga en cuenta que establecer un valor muy bajo podría dar lugar a que se produzca frecuentemente el agotamiento de los tiempos de espera. Del mismo modo, establecer un valor muy alto podría demorar la detección de fallos.

Procedimiento

- 1 Desplácese a **Seguridad > Configuración > Perfiles de seguridad > Temporizador de sesión**.
- 2 Haga clic en **Agregar perfil**.
Aparecerá la pantalla **Perfil**, que se rellena con los valores predeterminados.
- 3 Escriba un **nombre** y una **descripción** (opcional) para el perfil de temporizador.
- 4 Haga clic en **Establecer** para seleccionar el grupo o la puerta de enlace de nivel 0 o de nivel 1 para aplicar el perfil de temporizador.
- 5 Seleccione el protocolo. Acepte los valores predeterminados o introduzca sus propios valores.

Variables TCP	Descripción
First Packet	El valor de tiempo de espera para la conexión después de que se haya enviado el primer paquete. El valor predeterminado es de 120 segundos.
Abriendo	El valor de tiempo de espera para la conexión después de que se transfiriera un segundo paquete. El valor predeterminado es de 30 segundos.
Establecido	El valor de tiempo de espera para la conexión una vez que esta se estableciera completamente.
CLOSING	El valor de tiempo de espera para la conexión después de que se enviara el primer FIN. El valor predeterminado es de 120 segundos.
FIN WAIT	El valor de tiempo de espera para la conexión después de que se intercambiaran ambas FIN y se haya cerrado la conexión. El valor predeterminado es de 45 segundos.
CLOSED	El valor de tiempo de espera para la conexión después de que un endpoint envíe un RST. El valor predeterminado es de 20 segundos.

Variables UDP	Descripción
First Packet	El valor de tiempo de espera para la conexión después de que se envíe el primer paquete. Este será el tiempo de espera inicial para el nuevo flujo UDP. El valor predeterminado es de 60 segundos.
SINGLE	El valor de tiempo de espera para la conexión si el host de origen envía más de un paquete y el host de destino no ha enviado uno de vuelta. El valor predeterminado es de 30 segundos.
MULTIPLE	El valor de tiempo de espera para la conexión si ambos hosts han enviado paquetes. El valor predeterminado es de 60 segundos.

Variables ICMP	Descripción
First Packet	El valor de tiempo de espera para la conexión después de que se envíe el primer paquete. Este será el tiempo de espera inicial para el nuevo flujo ICMP. El valor predeterminado es de 20 segundos.
Respuesta de error (Error reply)	El valor de tiempo de espera para la conexión después de que se devuelva un error ICMP en respuesta a un paquete ICMP. El valor predeterminado es de 10 segundos.

6 Haga clic en **Guardar**.

Pasos siguientes

Después de guardar, haga clic en [Administrar prioridad grupo-perfil](#) para administrar la prioridad a grupo-perfil.

Valores de temporizador de sesión predeterminados

El perfil de temporizador de sesión aplica los valores de tiempo de espera a los grupos o a las interfaces del enrutador de nivel 0 o 1 que contienen segmentos. Los valores de tiempo de espera determinan el tiempo que una sesión de protocolo permanece activa después de que se cierra la sesión.

Valores de temporizador de sesión

- El perfil de temporizador predeterminado que se muestra con la API y la interfaz de usuario se aplica solo al firewall distribuido (DFW).
- Los temporizadores de sesión predeterminados de firewall de puerta de enlace (GFW) son diferentes al temporizador de perfil predeterminado que se ve al utilizar la API y la interfaz de usuario. Los temporizadores de sesión predeterminados de GFW están optimizados para el tráfico de norte a sur y tienen un valor más bajo de forma predeterminada.
- Los temporizadores de sesión de FW se pueden cambiar tanto para DFW como para GFW mediante la API y la interfaz de usuario.
- Si es necesario, se puede aplicar el mismo perfil de temporizador no predeterminado a DFW y GFW.

Si no se personalizan los valores del temporizador, la puerta de enlace tomará los valores predeterminados. Valores de temporizador predeterminados de firewall de puerta de enlace:

Propiedad del temporizador	Valor predeterminado de Edge (seg)	Mínimo (segundos)	Máximo (segundos)
Respuesta de error de ICMP	6	10	4320000
Primer paquete ICMP	6	10	4320000
TCP cerrado	2	10	4320000
Cierre de TCP	900	10	4320000
TCP establecido	7200	120	4320000
TCP FIN-WAIT	4	10	4320000
Primer paquete TCP	120	10	4320000
Apertura de TCP	30	10	4320000
Primer paquete UDP	30	10	4320000
UDP múltiple	30	10	4320000
UDP único	30	10	4320000

Valores de temporizador de sesión predeterminados de firewall distribuido:

Propiedad del temporizador	Predeterminado de DFW (segundos)	Mínimo (segundos)	Máximo (segundos)
Respuesta de error de ICMP	10	10	4320000
Primer paquete ICMP	20	10	4320000
TCP cerrado	20	10	4320000
Cierre de TCP	120	10	4320000
TCP establecido	43200	120	4320000
TCP FIN-WAIT	45	10	4320000
Primer paquete TCP	120	10	4320000
Apertura de TCP	30	10	4320000
Primer paquete UDP	60	10	4320000
UDP múltiple	60	10	4320000
UDP único	30	10	4320000

Protección contra inundación

La protección contra inundaciones ayuda a proteger contra ataques de denegación de servicio (DDoS).

Los ataques DDoS tienen como objetivo hacer que un servidor no esté disponible para el tráfico legítimo mediante el consumo de todos los recursos de servidor disponibles, ya que el servidor estará inundado con solicitudes. La creación de un perfil de protección contra inundación impone límites de sesión activa para los flujos ICMP, UDP y TCP medio abiertos. El firewall distribuido puede almacenar en caché las entradas de flujo que se encuentran en los estados SYN_SENT y SYN_RECEIVED, y hacer que cada entrada pase a un estado de TCP después de recibir una confirmación del iniciador, completando el protocolo de enlace de tres vías.

Procedimiento

- 1 Vaya a **Seguridad > Perfiles de seguridad > Protección contra inundación**.
- 2 Haga clic en **Agregar perfil** y seleccione **Agregar perfil de puerta de enlace Edge** o **Agregar perfil de firewall**.
- 3 Rellene los parámetros del perfil de protección contra inundación:

Tabla 10-15. Parámetros de los perfiles de puerta de enlace Edge y firewall

Parámetro	Valores mínimo y máximo	Predeterminado	
Límite de conexiones medio abiertas de TCP: los ataques de inundación SYN de TCP se evitan al limitar el número de flujos TCP activos no establecidos completamente que permite el firewall.	1-1000000	Firewall: Ninguno Puerta de enlace Edge: 1.000.000	Rellene este cuadro de texto para limitar el número de conexiones medio abiertas de TCP. Si este cuadro de texto está vacío, este límite se deshabilitará en los nodos de ESX y se establecerá el valor predeterminado de las puertas de enlace Edge.
Límite de flujos activos de UDP: los ataques de inundación de UDP se evitan al limitar el número de flujos de UDP activos que permite el firewall. Una vez que se alcanza el límite de flujo UDP establecido, se anularán los paquetes UDP posteriores que pueden establecer un flujo nuevo.	1-1000000	Firewall: Ninguno Puerta de enlace Edge: 1.000.000	Rellene este cuadro de texto para limitar el número de conexiones activas de UDP. Si este cuadro de texto está vacío, este límite se deshabilitará en los nodos de ESX y se establecerá el valor predeterminado de las puertas de enlace Edge.

Tabla 10-15. Parámetros de los perfiles de puerta de enlace Edge y firewall (continuación)

Parámetro	Valores mínimo y máximo	Predeterminado	
Límite de flujos activos de ICMP: los ataques de inundación de ICMP se evitan al limitar el número de flujos de ICMP activos que permite el firewall. Una vez que se alcanza el límite de flujo establecido, se anularán los paquetes ICMP posteriores que pueden establecer un flujo nuevo.	1-10000000	Firewall: Ninguno Puerta de enlace Edge: 10000	Rellene este cuadro de texto para limitar el número de conexiones abiertas de ICPM. Si este cuadro de texto está vacío, este límite se deshabilitará en los nodos de ESX y se establecerá el valor predeterminado de las puertas de enlace Edge.
Límite de otras conexiones activas	1-10000000	Firewall: Ninguno Puerta de enlace Edge: 10000	Rellene este cuadro de texto para limitar el número de conexiones activas que no sean conexiones medio abiertas de UDP, TCP e ICMP. Si este cuadro de texto está vacío, este límite se deshabilitará en los nodos de ESX y se establecerá el valor predeterminado de las puertas de enlace Edge.

Tabla 10-15. Parámetros de los perfiles de puerta de enlace Edge y firewall (continuación)

Parámetro	Valores mínimo y máximo	Predeterminado	
Caché SYN: la caché SYN se utiliza cuando también se ha configurado un límite de conexiones medio abiertas de TCP. El número de conexiones medio abiertas activas se aplica manteniendo una entrada syncache de las sesiones TCP no establecidas por completo. Esta caché mantiene las entradas de flujo que se encuentran en los estados SYN_SENT y SYN_RECEIVED. Cada entrada syncache se cambiará a una entrada de estado TCP completo una vez que se reciba una ACK del iniciador, lo que completará el protocolo de enlace de tres vías.		Solo disponible para perfiles de firewall.	Activar y desactivar. Habilitar la caché SYN solo es efectivo cuando se ha configurado un límite de conexiones medio abiertas de TCP.
Suplantación RST: genera RST suplantado al servidor al purgar estados medio abiertos de la memoria caché SYN. Permite al servidor limpiar los estados asociados con el desbordamiento SYN (medio abierto).		Solo disponible para perfiles de firewall.	Activar y desactivar. La opción Caché SYN debe estar seleccionada para que esta opción esté disponible

4 Para aplicar el perfil a las puertas de enlace de Edge y los grupos de firewall, haga clic en **Establecer**.

5 Haga clic en **Guardar**.

Pasos siguientes

Después de guardar, haga clic en [Administrar prioridad grupo-perfil](#) para administrar la prioridad a grupo-perfil.

Configurar la seguridad de DNS

Crear un perfil de seguridad de DNS ayuda a protegerle frente a ataques relacionados con DNS.

Después de configurar el perfil de seguridad de DNS, puede hacer lo siguiente:

- Busque respuestas de DNS de una máquina virtual o un grupo de máquinas virtuales en el nodo de transporte para asociar FQDN con direcciones IP.

- Agregue la información del servidor DNS global y predeterminado y aplíquela a todas las máquinas virtuales que utilicen reglas de DFW.
- Especifique la información del servidor DNS seleccionado para las máquinas virtuales que elija.
- Aplique los perfiles de DNS a los grupos.

Nota En la versión actual, solo se admite ESXi.

Procedimiento

- 1 Desplácese a **Seguridad > Configuración > Perfiles de seguridad > Seguridad de DNS**.
- 2 Haga clic en **Agregar perfil**.
- 3 Introduzca los siguientes valores:

Opción	Descripción
Nombre del perfil	Proporcione un nombre del perfil.
TTL	<p>Este campo captura el tiempo de vida de la entrada de la memoria caché de DNS en segundos. Tiene las siguientes opciones:</p> <p>TTL 0: la entrada de la memoria caché no caduca nunca.</p> <p>TTL entre 1 y 3599: no es una opción válida.</p> <p>TTL entre 3.600 a 864.000: opción válida.</p> <p>TTL vacía o TTL automático: se establece a partir del paquete de respuesta de DNS.</p> <p>Nota El perfil de seguridad de DNS tiene un tiempo de espera predeterminado para la memoria caché de DNS de 24 horas.</p>
Se aplica a	<p>Puede seleccionar un grupo según los criterios que se apliquen al perfil de seguridad de DNS.</p> <p>Nota Solo se aplica un perfil de servidor DNS a una máquina virtual.</p>
Etiquetas	Opcional. Asigne una etiqueta y un ámbito al perfil de DNS para facilitar la búsqueda. Consulte Agregar etiquetas a un objeto para obtener más información.

- 4 Haga clic en **Guardar**.

Pasos siguientes

Después de guardar, haga clic en [Administrar prioridad grupo-perfil](#) para administrar la prioridad a grupo-perfil.

Administrar prioridad grupo-perfil

Puede enlazar varios grupos a un perfil de seguridad. NSX-T Data Center aplica el perfil de seguridad al grupo con el nivel de prioridad más alto.

Si enlaza un perfil de seguridad a varios grupos, NSX-T Data Center asignará la prioridad más alta al grupo más reciente de esa lista. Sin embargo, puede cambiar el nivel de prioridad de los grupos.

Para asignar prioridad a los grupos:

Requisitos previos

- Los grupos de temporizadores de sesión solo deben contener como miembros segmentos, puertos de segmentos y máquinas virtuales. No se admiten otros tipos de categorías.
- Los grupos de seguridad de DNS solo deben contener como miembros máquinas virtuales. No se admiten otros tipos de categorías.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Vaya a **Seguridad > Perfiles de seguridad**.
- 3 Haga clic en **Administrar prioridad grupo-perfil**.
- 4 Para asignar un nivel más alto de prioridad a un grupo, muévelo a la parte superior de la lista.
- 5 Haga clic en **Cerrar**.

Resultados

El perfil de seguridad se aplicará al grupo con el nivel de prioridad más alto.

Puede configurar servicios, grupos, perfiles de contexto y máquinas virtuales para el inventario de NSX-T Data Center.

Al hacer clic en la pestaña **Inventario**, se muestra una vista general de los objetos del inventario, donde se especifica el número de grupos, servicios, máquinas virtuales y perfiles de contexto que se encuentran en el inventario. Además, se muestra la siguiente información sobre grupos:

- el número de grupos utilizados en las directivas
- el número de grupos que no se utilizan en las directivas
- el número de grupos con miembros
- el número de grupos sin miembros
- el número de grupos de identidades
- el número de grupos de identidades utilizados en las directivas
- el número de grupos de identidades no utilizados en las directivas

Este capítulo incluye los siguientes temas:

- [Agregar un servicio](#)
- [Agregar un grupo](#)
- [Agregar un perfil de contexto](#)

Agregar un servicio

Puede configurar un servicio y especificar parámetros para el tráfico de red coincidente, como un emparejamiento de protocolos y puertos.

También puede utilizar un servicio para permitir o bloquear determinados tipos de tráfico en las reglas de firewall. No puede cambiar el tipo después de crear un servicio. Algunos servicios están predefinidos y no se pueden modificar ni eliminar.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

- 2 Seleccione **Inventario > Servicios**.
- 3 Haga clic en **Agregar nuevo servicio**.
- 4 Introduzca un nombre.
- 5 Haga clic en **Establecer entradas de servicio**. Haga clic en **Agregar nueva entrada de servicio**.
- 6 Para un nuevo servicio, seleccione un tipo de servicio y especifique propiedades adicionales. Los tipos disponibles son **IP**, **IGMP**, **ICMPv4**, **ICMPv6**, **ALG**, **TCP**, **UDP** y **Ether**.
- 7 Haga clic en **Guardar**.
- 8 (opcional) Agregue una o varias etiquetas.
- 9 (opcional) Escriba una descripción.
- 10 Haga clic en **Guardar**.

Agregar un grupo

Los grupos incluyen distintos objetos que se agregan tanto de forma estática como dinámica y pueden utilizarse como origen y destino de una regla de firewall.

Los grupos se pueden configurar para que contengan una combinación de máquinas virtuales, conjuntos de direcciones IP, conjuntos de direcciones MAC, puertos de segmentos, segmentos, grupos de usuarios de AD y otros grupos. La inclusión dinámica de grupos puede basarse en la etiqueta, el nombre del equipo, el nombre del sistema operativo o el nombre del equipo. Los grupos basados en objetos dinámicos o lógicos no pueden utilizarse en el campo Se aplica a de las reglas de firewall distribuido.

Las etiquetas en NSX distinguen entre mayúsculas y minúsculas, pero los grupos basados en etiquetas no. Por ejemplo, si el criterio de pertenencia a grupos dinámicos es `VM Tag Equals 'quarantine'`, el grupo incluirá todas las máquinas virtuales que contengan las etiquetas "Cuarentena" o "CUARENTENA".

Los grupos también se pueden excluir de las reglas de firewall, pudiendo incluir en la lista un máximo de 100 grupos. Los conjuntos de direcciones IP, los conjuntos de direcciones MAC y los grupos de AD no se pueden incluir como miembros de un grupo que se utiliza en una lista de exclusión de firewall. Consulte [Administrar una lista de exclusión de firewall](#) para obtener más información.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte [Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública](#) para obtener información sobre cómo usar las etiquetas de nube pública para agrupar las máquinas virtuales de carga de trabajo en NSX Manager.

Un único grupo basado en identidad se puede utilizar como origen solo dentro de una regla de firewall distribuido. Si necesita utilizar grupos basados en identificadores y direcciones IP en el origen, cree dos reglas de firewall independientes.

Los grupos que constan únicamente de direcciones IP, direcciones MAC o grupos de Active Directory no se pueden utilizar en el cuadro de texto **Se aplica a**.

Nota Cuando se agrega un host a vCenter Server o se elimina de este sistema, el identificador externo de las máquinas virtuales del host cambia. Si una máquina virtual es un miembro estático de un grupo y su identificador externo cambia, esta máquina virtual dejará de aparecer como miembro del grupo en la interfaz de usuario de NSX Manager. Sin embargo, el grupo en el que se incluye la máquina virtual seguirá apareciendo con su identificador externo original en la API que contiene los grupos. Si agrega una máquina virtual como un miembro estático de un grupo y cambia el identificador externo de la máquina virtual, deberá volver a agregar la máquina virtual con el nuevo identificador externo. También puede utilizar los criterios dinámicos de pertenencia al grupo para evitar este problema.

Procedimiento

- 1 Seleccione **Inventario > Grupos** en el panel de navegación.
- 2 Haga clic en **Agregar grupo**.
- 3 Introduzca un nombre de grupo.
- 4 (opcional) Haga clic en **Establecer miembros**.

Para cada criterio de pertenencia, puede especificar hasta cinco reglas, que se combinan con el operador lógico AND. El criterio de miembro disponible puede aplicarse a lo siguiente:

- **Puerto de segmento:** puede especificar una etiqueta y un ámbito opcional.
- **Segmento:** puede especificar una etiqueta y un ámbito opcional.
- **Máquina virtual:** puede especificar un nombre, una etiqueta, un nombre de sistema operativo de equipo o un nombre de equipo que coincida con una cadena específica, que no coincida con ella, que la contenga, o que comience o termine con ella.
- **Conjunto de direcciones IP:** puede especificar una etiqueta y, opcionalmente, un ámbito.

- 5 (opcional) Haga clic en **Miembros** para seleccionar miembros.

Los tipos de miembro disponibles son:

- **Grupo**
- **Segmento**
- **Puerto de segmento**
- **Interfaz de red virtual**
- **Máquina virtual**

- 6 (opcional) Haga clic en **Direcciones IP/MAC** para agregar direcciones IP y MAC como miembros del grupo.

Se admiten direcciones IPv4, IPv6 y de multidifusión.

- 7 (opcional) Haga clic en **Grupos de AD** para agregar grupos de Active Directory. Los grupos con miembros de Active Directory se pueden utilizar en el campo de origen de una regla de firewall distribuido para el firewall de identidad. Los grupos pueden contener tanto miembros de equipos como de AD.
- 8 (opcional) Introduzca una descripción y una etiqueta.
- 9 Haga clic en **Aplicar**.
Se muestra una lista de grupos, con una opción para ver los miembros y donde se utiliza el grupo.

Agregar un perfil de contexto

Los perfil de contexto permiten crear pares de valores y claves para atributos, como el identificador de aplicación de Capa 7 y los nombres de dominio. Después de definir un perfil de contexto, puede usarlo en una regla de firewall distribuido y una regla de firewall de puerta de enlace o en varias.

Hay dos atributos que se pueden utilizar en los perfiles de contexto: identificador de aplicación y nombre de dominio (FQDN). Determinados identificadores de aplicaciones pueden tener uno o más subatributos, como TLS_Version y CIPHER_SUITE. Tanto el nombre de dominio como el identificador de aplicación pueden utilizarse en un solo perfil de contexto. Es posible utilizar varios identificadores de aplicación en el mismo perfil. Se puede utilizar un identificador de aplicación con subatributos; los subatributos se borran cuando se utilizan varios atributos de identificador de aplicación en un único perfil.

Actualmente se admite una lista predefinida de dominios. Puede ver la lista de FQDN cuando agrega un nuevo perfil de contexto del tipo de atributo *Nombre de dominio (FQDN)*. También puede ver una lista de FQDN ejecutando la llamada API `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`.

Nota

- No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace en perfiles de contexto.
 - Los perfiles de contexto no se admiten en la directiva de firewall de puerta de enlace de nivel 0. No se pueden utilizar atributos FQDN u otros subatributos con las reglas de firewall de puerta de enlace.
-

Procedimiento

- 1 Seleccione **Inventario > Perfiles de contexto**.
- 2 Haga clic en **Agregar nuevo perfil de contexto**.
- 3 Introduzca un valor en **Nombre de perfil**.
- 4 En la columna Atributos, haga clic en **Establecer**.

- 5 Seleccione un atributo o haga clic en **Agregar atributo** y, a continuación, seleccione **Identificador de aplicación** o **Nombre de dominio (FQDN)**.
- 6 Seleccione uno o varios atributos.
- 7 (opcional) Si seleccionó un atributo con subatributos, como SSL o CIFS, haga clic en **Establecer** en la columna Subatributos/Valores.
 - a Haga clic en **Agregar subatributo** y seleccione una categoría de subatributo en el menú desplegable.
 - b Seleccione uno o varios subatributos.
 - c Haga clic en **Agregar**. Si desea agregar otro subatributo, haga clic en **Agregar subatributo**.
 - d Haga clic en **Aplicar**.
- 8 Haga clic en **Agregar**.
- 9 (opcional) Para agregar otro tipo de atributo, haga clic en **Agregar atributo** nuevamente.
- 10 Haga clic en **Aplicar**.
- 11 (opcional) Escriba una descripción.
- 12 (opcional) Introduzca una etiqueta.
- 13 Haga clic en **Guardar**.

Pasos siguientes

Aplique este perfil de contexto a una regla de firewall distribuido de Capa 7 (para Capa 7 o el nombre de dominio) o a una regla de firewall de puerta de enlace (para Capa 7).

Existen varias formas de supervisar el entorno de NSX-T, así como el tráfico de red.

Este capítulo incluye los siguientes temas:

- Agregar un perfil de IPFIX para firewall
- Agregar un perfil de IPFIX para conmutador
- Agregar un recopilador IPFIX
- Agregar un perfil de creación de reflejo del puerto
- Protocolo de administración de red simple (SNMP)
- Utilizar vRealize Log Insight para supervisar el sistema
- Utilizar vRealize Operations Manager para supervisar el sistema
- Utilizar vRealize Network Insight Cloud para la supervisión del sistema
- Herramientas de supervisión avanzadas

Agregar un perfil de IPFIX para firewall

Puede configurar perfiles de IPFIX para los firewalls.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Planificar y solucionar problemas > IPFIX**.
- 3 Haga clic en la pestaña **Perfiles de IPFIX para los firewalls**.
- 4 Haga clic en **Agregar perfil de IPFIX de firewall**.

5 Proporcione los siguientes detalles.

Opción	Descripción
Nombre y descripción	<p>Introduzca un nombre y, si lo desea, una descripción.</p> <p>Nota Si desea crear un perfil global, asigne al perfil el nombre Global. No se puede editar ni eliminar un perfil global de la interfaz de usuario, pero puede hacerlo con las API de NSX-T Data Center.</p>
Tiempo de espera de exportación de flujo activo (minutos)	El tiempo tras el que se agotará el tiempo de espera de un flujo aunque se reciban más paquetes asociados al flujo. El valor predeterminado es 1.
Identificador de dominio de observación	Este parámetro identifica desde qué dominio de observación se originan los flujos de red. El valor predeterminado es 0, que indica que no hay ningún dominio de observación específico.
Configuración del recopilador	Seleccione un recopilador en el menú desplegable.
Se aplica a	Haga clic en Establecer y seleccione un grupo al que quiera aplicar el filtro, o bien cree uno.
Prioridad	Este parámetro resuelve los conflictos cuando se aplican varios perfiles. El exportador IPFIX solo usará el perfil con la prioridad más alta. Un valor inferior significa una prioridad más elevada.

6 Haga clic en **Guardar** y, a continuación, en **Sí** para seguir configurando el perfil.

7 Haga clic en **Guardar**.

Agregar un perfil de IPFIX para conmutador

Puede configurar perfiles de IPFIX para conmutadores, también conocidos como segmentos.

La supervisión de una red basada en flujos permite a los administradores de red obtener información sobre el tráfico que pasa por una red.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Planificar y solucionar problemas > IPFIX**.
- 3 Haga clic en la pestaña **Perfiles de IPFIX para el conmutador**.
- 4 Haga clic en **Agregar perfil de IPFIX de conmutador**.

5 Introduzca la siguiente información:

Opción	Descripción
Nombre y descripción	<p>Introduzca un nombre y, si lo desea, una descripción.</p> <p>Nota Si desea crear un perfil global, asigne al perfil el nombre Global. No se puede editar ni eliminar un perfil global de la interfaz de usuario, pero puede hacerlo con las API de NSX-T Data Center.</p>
Tiempo de espera activo (segundos)	El tiempo tras el que se agota el tiempo de espera de un flujo aunque se reciban más paquetes asociados al mismo. El valor predeterminado es 300.
Tiempo de espera inactivo (segundos)	El tiempo tras el que se agota el tiempo de espera de un flujo si no se reciben más paquetes asociados al mismo (solo en ESXi, KVM agota el tiempo de espera de todos los flujos basándose en el tiempo de espera activo). El valor predeterminado es 300.
Probabilidad de muestreo de paquetes (%)	El porcentaje de paquetes que se van a muestrear (aproximadamente). Si se aumenta este valor, puede verse afectado negativamente el rendimiento de hipervisores y recopiladores. Si todos los hipervisores envían más paquetes IPFIX al recopilador, este podría no ser capaz de recopilálos todos. Si se establece la probabilidad en el valor predeterminado (0,1 %), se mantendrá bajo el impacto sobre el rendimiento.
Configuración del recopilador	Seleccione un recopilador del menú desplegable.
Se aplica a	Seleccione una categoría: Segmento, Puerto de segmento o Grupos. El perfil de IPFIX se aplica al objeto seleccionado.
Prioridad	Este parámetro resuelve los conflictos cuando se aplican varios perfiles. El exportador IPFIX usa el perfil solo con la prioridad más alta. Un valor inferior significa una prioridad más elevada.
Flujos máximos	Los flujos máximos que se almacenan en caché en un puente (solo en KVM, no se puede configurar en ESXi). El valor predeterminado es 16384.
Identificador de dominio de observación	El identificador del dominio de observación identifica desde qué dominio de observación se originan los flujos de red. Escriba 0 para indicar que no hay un dominio de observación específico.
Exportar flujo superpuesto	Este parámetro define si se deben muestrear y exportar los flujos de superposición en los puertos de vínculo superior y de túnel. Tanto el flujo de vNIC como el flujo de superposición se incluirán en la muestra. El valor predeterminado es Habilitado . Cuando se deshabilita, solo se muestran y se exportan los flujos de vNIC.
Etiquetas	Introduzca una etiqueta para facilitar la búsqueda.

6 Haga clic en **Guardar** y, a continuación, en **Sí** para seguir configurando el perfil.

7 Haga clic en **Se aplica a** para aplicar el perfil en los objetos.

Seleccione uno o varios de los objetos.

8 Haga clic en **Guardar**.

Agregar un recopilador IPFIX

Puede configurar recopiladores IPFIX para firewalls y conmutadores.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Planificar y solucionar problemas > IPFIX**.
- 3 Haga clic en la pestaña **Recopiladores**.
- 4 Seleccione **Agregar nuevo recopilador > Conmutador de IPFIX** o **Agregar nuevo recopilador > Firewall de IPFIX**.
- 5 Introduzca un nombre.
- 6 Introduzca la dirección IP y el puerto de hasta cuatro recopiladores. Se admiten las direcciones IPv4 e IPv6.
- 7 Haga clic en **Guardar**.

Agregar un perfil de creación de reflejo del puerto

Puede configurar perfiles de creación de reflejo del puerto para las sesiones de reflejo del puerto.

Tenga en cuenta que la extensión lógica solo es compatible con segmentos de superposición y no con segmentos de VLAN.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Planificar y solucionar problemas > Reflejo del puerto**.
- 3 Seleccione **Agregar perfil > SPAN de Capa 3 remoto** o **Agregar perfil > SPAN lógico**.
- 4 Introduzca un nombre y, si lo desea, una descripción.
- 5 Complete los siguientes detalles del perfil.

Tipo de sesión	Parámetros
SPAN de Capa 3 remoto	<ul style="list-style-type: none"> ■ Dirección: seleccione Bidireccional, Entrada o Salida. ■ Ajustar longitud: especifique el número de bytes para capturar desde un paquete. ■ Tipo de encapsulación: seleccione GRE, ERSPAN TWO o ERSPAN THREE. ■ Clave de GRE: especifique una clave de GRE si el tipo de encapsulación es GRE. ■ Identificador de ERSPAN: especifique un identificador de ERSPAN si el tipo de encapsulación es ERSPAN TWO o ERSPAN THREE.
SPAN lógico	<ul style="list-style-type: none"> ■ Dirección: seleccione Bidireccional, Entrada o Salida. ■ Ajustar longitud: especifique el número de bytes para capturar desde un paquete.

- 6 Haga clic en **Establecer** en la columna **Origen** para establecer un destino.

Para SPAN lógico, los orígenes disponibles son **Puerto de segmento** , **Grupo de máquinas virtuales** y **Grupo de interfaces de red virtual**.

Para SPAN de Capa 3 remoto, los orígenes disponibles son **Segmento**, **Puerto de segmento**, **Grupo de máquinas virtuales** y **Grupo de interfaces de red virtual**.

- 7 Haga clic en **Establecer** en la columna **Destino** para establecer un destino.
- 8 Haga clic en **Guardar**.

Protocolo de administración de red simple (SNMP)

Puede usar el protocolo de administración de red simple (SNMP) para supervisar los componentes de NSX-T Data Center. El servicio SNMP no se inicia de forma predeterminada tras la instalación.

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager o de NSX Edge.
- 2 Ejecute los siguientes comandos

- Para SNMPv1 o SNMPv2:

```
set snmp community <community-string>
start service snmp
```

El límite de caracteres máximo establecido para **community-string** es 64.

- Para SNMPv3

```
set snmp v3-users <user_name> auth-password <auth_password> priv-password
<priv_password>

start service snmp
```

El límite de caracteres máximo establecido para **user_name** es 32. Asegúrese de que las contraseñas cumplan con las restricciones de PAM. Si desea cambiar el identificador del motor predeterminado, utilice el siguiente comando:

```
set snmp v3-engine-id <v3-engine-id>

start service snmp
```

v3-engine-id es una cadena hexadecimal con un máximo de entre 10 y 64 caracteres.

NSX-T Data Center es compatible con SHA1 y AES128 como protocolos de autenticación y privacidad. También puede usar llamadas API para configurar SNMPv3. Para obtener más información, consulte la *Guía de la API de NSX-T Data Center*.

Ejemplo:

Utilizar vRealize Log Insight para supervisar el sistema

Puede supervisar el entorno de NSX-T Data Center mediante el paquete de contenido de Log Insight NSX-T.

Este paquete de contenido incluye las siguientes alertas:

Nombre de la alerta	Descripción
SysCpuUsage	El uso de la CPU es superior al 95 % durante más de 10 minutos.
SysMemUsage	El uso de la memoria es superior al 95 % durante más de 10 minutos.
SysDiskUsage	El uso del disco en una o más particiones es superior al 89 % durante más de 10 minutos.
PasswordExpiry	La contraseña de la cuenta de usuario del dispositivo está a punto de caducar o ya caducó.
CertificateExpiry	Uno o varios certificados firmados por la CA caducaron.
ClusterNodeStatus	El nodo de clúster de Edge local está inactivo.
BackupFailure	Error en la operación de copia de seguridad programada de NSX.
VipLeadership	La VIP del clúster de administración de NSX está inactiva.
ApiRateLimit	La API del cliente alcanzó el umbral configurado.
CorfuQuorumLost	Dos nodos estaban inactivos en el clúster y perdieron el quórum de Corfu.
DfwHeapMem	La memoria de pila de DFW superó el umbral configurado.
ProcessStatus	Cambió el estado de proceso crítico.
ClusterFailoverStatus	Cambió el estado de alta disponibilidad de SR o se produjo una conmutación por error de los servicios activos/en espera.
DhcpPoolUsageOverloadedEvent	El grupo de DHCP alcanzó el umbral de uso configurado.
FabricCryptoStatus	El controlador MUX criptográfico de Edge está inactivo por no pasar las pruebas Known_Answer_Tests (KAT).
VpnTunnelState	El túnel de VPN está inactivo.
BfdTunnelStatus	Cambió el estado del túnel de BFD.
RoutingBgpNeighborStatus	El estado del vecino BGP es inactivo.
VpnL2SessionStatus	La sesión de VPN de capa 2 está inactiva.
VpnIkeSessionStatus	La sesión de IKE está inactiva.
RoutingStatus	El enrutamiento (BGP/BFD) está inactivo.
DnsForwarderStatus	El estado de ejecución del reenviador de DNS es inactivo.
TnConnDown_15min	La conexión entre el nodo de transporte y un controlador/administrador está inactiva durante al menos 15 minutos.
TnConnDown_5min	La conexión entre el nodo de transporte y el controlador/administrador está inactiva durante al menos 5 minutos.
ServiceDown	Uno o varios servicios están inactivos.
IpNotAvailableInPool	No hay direcciones IP disponibles en el grupo o se alcanza el umbral configurado.

Nombre de la alerta	Descripción
LoadBalancerError	El estado del servicio del equilibrador de carga de NSX es ERROR.
LoadBalancerDown	El estado del servicio del equilibrador de carga de NSX es INACTIVO.
LoadBalancerVsDown	Estado de VS: todos los miembros del grupo están inactivos.
LoadBalancerPoolDown	Estado del grupo: todos los miembros del grupo están inactivos.
ProcessCrash	El proceso o el daemon se bloquean en la ruta de datos u otro proceso de LB, como el distribuidor.

Utilizar vRealize Operations Manager para supervisar el sistema

Puede supervisar el entorno de NSX-T Data Center mediante vRealize Operations Manager.

Tabla 12-1. Alertas del paquete de gestión de NSX-T

Alerta	Descripción	Recomendación
Error en el servicio de administración de NSX-T	Se activa cuando el servicio de administración del host de NSX-T Data Center no se está ejecutando.	Inicie sesión en el NSX-T Manager y reinicie el servicio de administración con errores.
El estado de administración del conmutador lógico no está activo	Se activa cuando el estado de administración está deshabilitado en el conmutador lógico.	Inicie sesión en NSX-T y habilite el estado de administración si es necesario.
La conectividad del controlador/administrador del nodo de Edge no está activa	Se activa cuando el estado de conectividad del nodo de Edge es inactivo en NSX-T Data Center.	Compruebe el estado de conexión del nodo de Edge con el clúster de controladores y el clúster de administrador y solucione el problema de conexión.
El nodo del host de Edge se encuentra en estado de error	Se activa cuando el nodo del host en NSX-T Data Center está en estado de error debido a uno de los siguientes motivos: <ul style="list-style-type: none"> ■ Error de configuración de Edge ■ Error de instalación ■ Error de desinstalación ■ Error de actualización ■ Error de implementación de la máquina virtual ■ Error de desconexión de la máquina virtual ■ Error de encendido de la máquina virtual ■ Error de anulación de implementación de la máquina virtual 	El nodo del host de Edge se encuentra en estado de error. Compruebe el estado del nodo del host y solucione el problema.

Tabla 12-1. Alertas del paquete de gestión de NSX-T (continuación)

Alerta	Descripción	Recomendación
El servicio de BFD está deshabilitado	Se activa cuando el servicio de BFD no está habilitado en el enrutador lógico.	El servicio de BFD de un enrutador de nivel 0 no está habilitado aunque los vecinos estén configurados. Habilite el servicio de BFD si es necesario.
Regla NAT no configurada	Se activa cuando la regla NAT del enrutador lógico no está configurada.	Inicie sesión en la instancia de NSX-T Manager y agregue las reglas NAT para el enrutador lógico.
Ruta estática no configurada	Se activa cuando la ruta estática del enrutador lógico no está configurada.	Inicie sesión en la instancia de NSX-T Manager y agregue las rutas estáticas para el enrutador lógico si es necesario.
El servicio de anuncio de rutas está deshabilitado	Se activa cuando el servicio de anuncio de rutas no está habilitado en el enrutador lógico.	El servicio de anuncio de rutas de un enrutador de nivel 1 no está habilitado, aunque los anuncios de rutas están configurados. Inicie sesión en NSX-T Manager y habilite el servicio.
El servicio de redistribución de rutas está deshabilitado	Se activa cuando el servicio de redistribución de rutas no está habilitado en el enrutador lógico.	El servicio de redistribución de rutas de un enrutador de nivel 0 no está habilitado, aunque las reglas de redistribución de rutas están configuradas. Inicie sesión en NSX-T Manager y habilite el servicio.
El servicio ECMP está deshabilitado en el enrutador lógico	Se activa cuando el servicio ECMP no está habilitado en el enrutador lógico.	El servicio ECMP de BGP de un enrutador de nivel 0 no está habilitado, aunque los vecinos están configurados. Inicie sesión en NSX-T Manager y habilite el servicio.
La conectividad del nodo del controlador se interrumpió	Se activa cuando el estado de conexión del nodo del controlador es inactivo en NSX-T Data Center.	Inicie sesión en NSX-T Manager, compruebe la conectividad del nodo del controlador con el nodo de administración y el clúster de controladores, y resuelva el estado de desconexión.
Se implementaron menos de 3 nodos de controlador	Se activa cuando el servidor de NSX-T Data Center tiene menos de tres nodos de controlador.	Implemente al menos 3 nodos de controlador en el clúster.

Tabla 12-1. Alertas del paquete de gestión de NSX-T (continuación)

Alerta	Descripción	Recomendación
El estado del clúster de controladores no es estable	Se activa cuando todos los nodos de controlador están inactivos en NSX-T Data Center.	Compruebe el estado del clúster de controladores.
El estado de administración no es estable	Se activa cuando el estado de cualquier nodo del clúster de administración es inactivo.	Compruebe el estado del clúster de administración.
El uso del sistema de archivos es superior al 85 %	Se activa cuando el uso del sistema de archivos invitado de la máquina virtual del controlador es superior al 85 %.	El uso del sistema de archivos es superior a 85 %. Compruebe y limpie el sistema de archivos para liberar espacio.
El uso del sistema de archivos es superior al 75 %	Se activa cuando el uso del sistema de archivos invitado de la máquina virtual del controlador es superior al 75 %.	El uso del sistema de archivos es superior a 75 %. Compruebe y limpie el sistema de archivos para liberar espacio.
El uso del sistema de archivos es superior al 70 %	Se activa cuando el uso del sistema de archivos invitado de la máquina virtual del controlador es superior al 70 %.	El uso del sistema de archivos es superior a 70 %. Compruebe y limpie el sistema de archivos para liberar espacio.
El estado del clúster de Edge es inactivo	Se activa cuando el estado del clúster de Edge es inactivo.	Compruebe el estado del clúster de Edge y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
El conmutador lógico tiene un estado de error	Se activa cuando se produce un error en el conmutador lógico.	Compruebe el estado del conmutador lógico y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
Estado operativo del servicio del equilibrador de carga inactivo	Se activa cuando el estado operativo del servicio del equilibrador de carga es inactivo.	Compruebe el estado operativo del servicio del equilibrador de carga y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.

Tabla 12-1. Alertas del paquete de gestión de NSX-T (continuación)

Alerta	Descripción	Recomendación
El estado operativo del servicio del equilibrador de carga es de error	Se activa cuando el estado operativo del servicio del equilibrador de carga contiene un error.	Compruebe el estado operativo del servicio del equilibrador de carga y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
Estado operativo del servidor virtual del equilibrador de carga inactivo	Se activa cuando el estado operativo del servidor virtual del equilibrador de carga es inactivo.	Compruebe el estado operativo del servidor virtual del equilibrador de carga y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
Estado operativo del servidor virtual del equilibrador de carga desconectado	Se activa cuando el estado operativo del servidor virtual del equilibrador de carga es desconectado.	Compruebe el estado operativo del servidor virtual del equilibrador de carga y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
El estado de la configuración del nodo de Edge es de error	Se activa cuando el estado de la configuración del nodo de Edge es de error.	Compruebe el estado de configuración del nodo de Edge y, si es necesario, siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
El estado del tiempo de ejecución del monitor del servicio de administración es de error	Se activa cuando el tiempo de ejecución del monitor del servicio de administración deja de ejecutarse.	Inicie sesión en NSX-T Manager VA y reinicie el servicio de administración con errores.
El estado de administración de un clúster de administración no es estable.	Se activa cuando el estado de administración de un clúster de administración no es estable.	Compruebe el estado del clúster de administración.
Se implementaron menos de 3 nodos de Manager	Se activa cuando el servidor de NSX-T tiene menos de tres nodos de administrador implementados.	Implemente al menos 3 nodos de Manager en el clúster.

Tabla 12-1. Alertas del paquete de gestión de NSX-T (continuación)

Alerta	Descripción	Recomendación
La conectividad del nodo de Manager se ha interrumpido	Se activa cuando el estado de conexión del administrador del nodo de Manager está inactivo.	Inicie sesión en NSX-T Manager y compruebe la conectividad del nodo de Manager y siga los pasos para solucionar problemas estándar recomendados en la documentación de NSX-T y VMware.
El uso del sistema de archivos del nodo de Manager es superior al 85 %	Se activa cuando el uso del sistema de archivos invitado del nodo de Manager es superior al 85 %.	El uso del sistema de archivos es superior a 85 %. Compruebe y limpie el sistema de archivos para liberar espacio.
El uso del sistema de archivos del nodo de Manager es superior al 75 %	Se activa cuando el uso del sistema de archivos invitado del nodo de Manager es superior al 75 %.	El uso del sistema de archivos es superior a 75 %. Compruebe y limpie el sistema de archivos para liberar espacio.
El uso del sistema de archivos del nodo de Manager es superior al 70 %	Se activa cuando el uso del sistema de archivos invitado del nodo de Manager es superior al 70 %.	El uso del sistema de archivos es superior a 70 %. Compruebe y limpie el sistema de archivos para liberar espacio.

Utilizar vRealize Network Insight Cloud para la supervisión del sistema

Puede supervisar el entorno de NSX-T Data Center mediante vRealize Network Insight Cloud.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	Advertencia	Evento de desconexión de enrutador lógico de nivel 1 de NSX-T	El enrutador lógico de nivel 1 de NSX-T está desconectado del enrutador de nivel 0. No se puede acceder a las redes de este enrutador desde fuera y viceversa.
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	Advertencia	Anuncio de enrutamiento deshabilitado	El anuncio de enrutamiento está deshabilitado para el enrutador lógico de nivel 1 de NSX-T. No se puede acceder a las redes de este enrutador desde fuera.
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	Crítico	El nodo de Edge de NSX-T no tiene conectividad con el administrador	El nodo de Edge de NSX-T perdió la conectividad con el administrador.
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	Advertencia	Conectividad de controlador degradada para el nodo de Edge de NSX-T	El nodo de Edge de NSX-T no puede comunicarse con uno o varios controladores.
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	Crítico	El nodo de Edge de NSX-T no tiene conectividad con los controladores	El nodo de Edge de NSX-T no puede comunicarse con ninguno de los controladores.
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMTuMismatchEvent	Advertencia	Error de coincidencia de MTU entre el nivel 0 de NSX-T y el conmutador/enrutador de vínculo superior	La MTU configurada en las interfaces del enrutador lógico de nivel 0 no coincide con las interfaces del conmutador/enrutador de vínculo superior de la misma red de capa 2. Esto puede afectar al rendimiento de la red.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	Información	Una o varias máquinas virtuales excluidas del firewall DFW de NSX-T.	Una o varias máquinas virtuales no están protegidas por el firewall DFW de NSX-T. vRealize Network Insight no recibirá flujos de IPFIX para estas máquinas virtuales.
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	Advertencia	Configuración errónea de VLAN de vínculo superior	Se interrumpe la comunicación debido a que la VLAN en el puerto de vínculo superior del enrutador de nivel 0 es diferente de la VLAN en la puerta de enlace externa.
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	Advertencia	No hay ninguna zona de transporte asociada al nodo de transporte.	No hay zonas de transporte asociadas al nodo de transporte. Es posible que las máquinas virtuales pierdan conectividad debido a esto.
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	Advertencia	No hay ningún VTEP disponible en el nodo de transporte.	Todos los VTEP se eliminaron del nodo de transporte. Es posible que las máquinas virtuales pierdan conectividad debido a esto.
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	Crítico	El nodo del controlador de NSX-T no tiene conectividad con el clúster de control	El nodo del controlador de NSX-T perdió la conectividad con el clúster de control.
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	Crítico	El nodo del controlador de NSX-T no tiene conectividad con el plano de administración	El nodo del controlador de NSX-T perdió la conectividad con el plano de administración.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	Crítico	El nodo de administración de NSX-T no tiene conectividad con el clúster de administración	El nodo de administración de NSX-T perdió la conectividad con el clúster de administración.
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	Advertencia	El nodo de host de NSX-T no tiene conectividad con el administrador	Desincronización entre el estado de la conectividad de NSX Manager y los nodos de transporte de host
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	Crítico	No se conoce la conectividad del controlador para el nodo de Edge de NSX-T.	La conectividad del controlador del nodo de Edge de NSX-T es desconocida.
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	Advertencia	El nodo de host de NSX-T no tiene conectividad con el controlador	El nodo de host de NSX-T no puede comunicarse con ninguno de los controladores.
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	Advertencia	Conectividad de controlador degradada para el nodo de host de NSX-T	El nodo de host de NSX-T no puede comunicarse con uno o varios controladores.
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	Advertencia	No se conoce la conectividad del controlador para el nodo de host de NSX-T.	La conectividad del controlador del nodo de host de NSX-T es desconocida.
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	Advertencia	El estado de la PNIC del nodo de transporte de host de NSX-T es 'Inactivo'.	El estado de la PNIC del nodo de transporte de host de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	Advertencia	El estado de la PNIC del nodo de transporte de host de NSX-T es 'Degradado'	El estado de la PNIC del nodo de transporte de host de NSX-T es 'Degradado'.
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	Advertencia	El estado de la PNIC del nodo de transporte de host de NSX-T es 'Desconocido'.	El estado de la PNIC del nodo de transporte de host de NSX-T es 'Desconocido'.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnic StatusDownEvent	Crítico	El estado de la PNIC del nodo de transporte de Edge de NSX-T es 'Inactivo'.	El estado de la PNIC del nodo de transporte de Edge de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnic StatusDegradedEvent	Crítico	El estado de la PNIC del nodo de transporte de Edge de NSX-T es 'Degradado'.	El estado de la PNIC del nodo de transporte de Edge de NSX-T es 'Degradado'.
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnic StatusUnknownEvent	Crítico	El estado de la PNIC del nodo de transporte de Edge de NSX-T es 'Desconocido'.	El estado de la PNIC del nodo de transporte de Edge de NSX-T es 'Desconocido'.
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnel StatusDownEvent	Advertencia	El estado del túnel del nodo de transporte de host de NSX-T es 'Inactivo'.	El estado del túnel del nodo de transporte de host de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnel StatusDegradedEvent	Advertencia	El estado del túnel del nodo de transporte de host de NSX-T es 'Degradado'.	El estado del túnel del nodo de transporte de host de NSX-T es 'Degradado'.
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnel StatusUnknownEvent	Advertencia	El estado del túnel del nodo de transporte de host de NSX-T es 'Desconocido'.	El estado del túnel del nodo de transporte de host de NSX-T es 'Desconocido'.
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnel StatusDownEvent	Crítico	El estado del túnel del nodo de transporte de Edge de NSX-T es 'Inactivo'.	El estado del túnel del nodo de transporte de Edge de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnel StatusDegradedEvent	Crítico	El estado del túnel del nodo de transporte de Edge de NSX-T es 'Degradado'.	El estado del túnel del nodo de transporte de Edge de NSX-T es 'Degradado'.
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnel StatusUnknownEvent	Crítico	El estado del túnel del nodo de transporte de Edge de NSX-T es 'Desconocido'.	El estado del túnel del nodo de transporte de Edge de NSX-T es 'Desconocido'.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	Advertencia	El estado del nodo de transporte de host de NSX-T es 'Inactivo'.	El estado del nodo de transporte de host de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	Advertencia	El estado del nodo de transporte de host de NSX-T es 'Degradado'.	El estado del nodo de transporte de host de NSX-T es 'Degradado'.
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	Advertencia	El estado del nodo de transporte de host de NSX-T es 'Desconocido'.	El estado del nodo de transporte de host de NSX-T es 'Desconocido'.
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	Crítico	El estado del nodo de transporte de Edge de NSX-T es 'Inactivo'.	El estado del nodo de transporte de Edge de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	Crítico	El estado del nodo de transporte de Edge de NSX-T es 'Degradado'.	El estado del nodo de transporte de Edge de NSX-T es 'Degradado'.
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	Crítico	El estado del nodo de transporte de Edge de NSX-T es 'Desconocido'.	El estado del nodo de transporte de Edge de NSX-T es 'Desconocido'.
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	Advertencia	El estado de administración del conmutador lógico de NSX-T es 'Inactivo'.	El estado de administración del conmutador lógico de NSX-T es 'Inactivo'.
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	Crítico	El estado operativo del puerto lógico de NSX-T es 'Inactivo'.	El estado operativo del puerto lógico de NSX-T es 'Inactivo'. Esto podría provocar un error de comunicación entre dos interfaces virtuales (VIF) conectadas al mismo conmutador lógico (por ejemplo, no se puede hacer ping en una máquina virtual desde otra).

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	Advertencia	El estado operativo del puerto lógico de NSX-T es 'Desconocido'	El estado operativo del puerto lógico de NSX-T es 'Desconocido'. Esto podría provocar un error de comunicación entre dos interfaces virtuales (VIF) conectadas al mismo conmutador lógico (por ejemplo, no se puede hacer ping en una máquina virtual desde otra).
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	Advertencia	El estado de conexión del administrador de equipos de NSX-T no es activo	El estado de conexión del administrador de equipos de NSX-T no es activo
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	Advertencia	No se programó la copia de seguridad de NSX-T Manager.	No se programó la copia de seguridad de NSX-T Manager
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	Crítico	El firewall DFW de NSX-T está deshabilitado.	El firewall distribuido está deshabilitado en NSX-T Manager
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	Advertencia	Se están descartando los paquetes recibidos en el puerto lógico de NSX-T.	Los paquetes recibidos se están descartando en el puerto lógico de NSX-T y las entidades asociadas podrían verse afectadas
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	Advertencia	Se están descartando los paquetes transmitidos en el puerto lógico de NSX-T.	Los paquetes transmitidos se están descartando en el puerto lógico de NSX-T y las entidades asociadas podrían verse afectadas
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	Advertencia	Se están descartando los paquetes recibidos en el conmutador lógico de NSX-T.	Los paquetes recibidos se están descartando en el conmutador lógico de NSX-T y las entidades asociadas podrían verse afectadas

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	Advertencia	Se están descartando los paquetes transmitidos en el conmutador lógico de NSX-T.	Los paquetes transmitidos se están descartando en el conmutador lógico de NSX-T y las entidades asociadas podrían verse afectadas
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	Advertencia	Se están descartando los paquetes recibidos en la interfaz de red del nodo de administración de NSX-T	Los paquetes recibidos se están descartando en la interfaz de red del nodo de administración de NSX-T. Esto puede afectar al tráfico de red relacionado con el clúster de administración de NSX-T.
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	Crítico	Se están descartando los paquetes recibidos en la interfaz de red del nodo de Edge de NSX-T	Los paquetes recibidos se están descartando en la interfaz de red del nodo de Edge de NSX-T. Esto puede afectar al tráfico de red del clúster de Edge.
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	Advertencia	Se están descartando los paquetes recibidos en la interfaz de red del nodo de host de NSX-T	Los paquetes recibidos se están descartando en la interfaz de red del nodo de host de NSX-T. Esto puede afectar al tráfico de red en el host ESXi.
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	Advertencia	Se están descartando los paquetes transmitidos en la interfaz de red del nodo de administración de NSX-T	Los paquetes recibidos se están transmitidos en la interfaz de red del nodo de administración de NSX-T. Esto puede afectar al tráfico de red relacionado con el clúster de administración de NSX-T.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	Crítico	Se están descartando los paquetes transmitidos en la interfaz de red del nodo de Edge de NSX-T	Los paquetes recibidos se están transmitidos en la interfaz de red del nodo de Edge de NSX-T. Esto puede afectar al tráfico de red del clúster de Edge.
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	Advertencia	Se están descartando los paquetes transmitidos en la interfaz de red del nodo de host de NSX-T	Los paquetes recibidos se están transmitidos en la interfaz de red del nodo de host de NSX-T. Esto puede afectar al tráfico de red en el host ESXi.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	Advertencia	El estado de inventario de CM dejó de ejecutarse	El estado del servicio de inventario de CM se detuvo.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	Advertencia	El servicio del controlador dejó de ejecutarse.	El estado del servicio del controlador se detuvo.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	Advertencia	El servicio de almacén de datos dejó de ejecutarse.	El estado del servicio de almacén de datos se detuvo.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	Advertencia	El servicio HTTP dejó de ejecutarse.	El estado del servicio HTTP se detuvo.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	Advertencia	El servicio de actualización de instalación dejó de ejecutarse.	El estado del servicio de actualización de instalación se detuvo.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Advertencia	El servicio Liagent dejó de ejecutarse.	El estado del servicio Liagent se detuvo.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Advertencia	El servicio de administrador dejó de ejecutarse.	El estado del servicio de administrador se detuvo.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Advertencia	El servicio del plano de administración dejó de ejecutarse.	El estado del servicio de administración se detuvo.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Advertencia	El servicio del coordinador de migración dejó de ejecutarse.	El estado del servicio del coordinador de migración se detuvo.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEvent	Advertencia	El servicio de administración de nodos dejó de ejecutarse.	El estado del servicio de administración de nodos se detuvo.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	Advertencia	El servicio de estadísticas de nodos dejó de ejecutarse.	El estado del servicio de estadísticas de nodos se detuvo.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	Advertencia	El servicio de bus de mensajes dejó de ejecutarse.	El estado del servicio de cliente de bus de mensajería se detuvo.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	Advertencia	El servicio de cliente de plataforma dejó de ejecutarse.	El estado del servicio de cliente de plataforma se detuvo.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	Advertencia	El servicio del agente de actualización dejó de ejecutarse.	El estado del servicio de actualización se detuvo.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	Advertencia	El servicio NTP dejó de ejecutarse.	El estado del servicio NTP se detuvo.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	Advertencia	El servicio de directivas dejó de ejecutarse.	El estado del servicio de directivas se detuvo.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	Advertencia	El servicio de búsqueda dejó de ejecutarse.	El estado del servicio de búsqueda se detuvo.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	Advertencia	El servicio SNMP dejó de ejecutarse.	El estado del servicio SNMP se detuvo.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	Advertencia	El servicio SSH dejó de ejecutarse.	El estado del servicio SSH se detuvo.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	Advertencia	El servicio syslog dejó de ejecutarse.	El estado del servicio syslog se detuvo.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	Advertencia	El servicio de telemetría dejó de ejecutarse.	El estado del servicio de telemetría se detuvo.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	Advertencia	El servicio de interfaz de usuario dejó de ejecutarse.	El estado del servicio de interfaz de usuario se detuvo.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	Crítico	El servicio de inventario de CM se detuvo.	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de inventario de CM, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	Crítico	El servicio del controlador se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio del controlador, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	Crítico	El servicio de almacén de datos se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio del almacén de datos, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	Crítico	El servicio HTTP se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio HTTP, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	Advertencia	El servicio de actualización de instalación se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de actualización de instalación, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	Advertencia	El servicio Liagent se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio Liagent, dejó de ejecutarse.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	Crítico	El servicio de administrador de detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de administrador, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	Advertencia	El servicio del plano de administración se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de bus del plano de administración, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	Advertencia	El servicio del coordinador de migración se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio del coordinador de migración, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEvent	Crítico	El servicio de administración de nodos se detuvo.	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de administración de nodos, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	Crítico	El servicio de estadísticas de nodos se detuvo.	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de estadísticas de nodos, dejó de ejecutarse.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	Advertencia	El servicio de bus de mensajes se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de bus de mensajes, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	Crítico	El servicio de cliente de plataforma se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de cliente de plataforma, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	Advertencia	El servicio del agente de actualización se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio del agente de actualización, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	Crítico	El servicio NTP se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio NTP, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	Crítico	El servicio de directivas se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de directivas, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	Crítico	El servicio de búsqueda se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de búsqueda, dejó de ejecutarse.

Tabla 12-2. Eventos de NSX-T computados de vRealize Network Insight (continuación)

OID	Nombre del evento	Gravedad predeterminada	Nombre de la interfaz de usuario	Descripción
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	Advertencia	El servicio SNMP se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio SNMP, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	Crítico	El servicio SSH se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio SSH, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	Crítico	El servicio syslog se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio syslog, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	Advertencia	El servicio de telemetría se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de telemetría, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	Crítico	El servicio de interfaz de usuario se detuvo	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de interfaz de usuario, dejó de ejecutarse.
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	Crítico	El servicio de administrador de clústeres se detuvo.	Uno de los servicios del nodo de administración de NSX-T, concretamente el servicio de administrador de clústeres, dejó de ejecutarse.

Eventos del sistema de NSX-T

A continuación se muestra la lista de eventos de NSX-T 2.2 a 2.5 compatibles con vRealize Network Insight. El identificador de objeto (OID) de todos estos eventos del sistema de NSX-T es 1.3.6.1.4.1.6876.100.1.0.80203.

Tabla 12-3. Eventos del sistema de NSX-T

Nombre del evento	Descripción
vmwNSXPlatformSysCpuUsage	Uso de la CPU en los dispositivos de Manager y Edge (NSX-T 2.2).
vmwNSXPlatformSysDiskUsage	Uso del espacio en disco en los dispositivos de Manager y Edge para la partición /var/log (NSX-T 2.2).
vmwNSXPlatformSysMemUsage	Uso de la memoria en los dispositivos de Manager y Edge (NSX-T 2.2).
vmwNSXPlatformSysConfigDiskUsage	Uso del disco en los dispositivos de Manager y Edge para la partición /config (NSX-T 2.4).
vmwNSXPlatformSysVarDumpDiskUsage	Uso del disco en los dispositivos de Manager y Edge para la partición /var/dump (NSX-T 2.5).
vmwNSXPlatformSysRepositoryDiskUsage	Uso del disco en los dispositivos de Manager y Edge para la partición /repository (NSX-T 2.5).
vmwNSXPlatformSysRootDiskUsage	Uso del disco en los dispositivos de Manager y Edge para la partición root (NSX-T 2.5).
vmwNSXPlatformSysTmpDiskUsage	Uso del disco en los dispositivos de Manager y Edge para la partición tmp (NSX-T 2.5).
vmwNSXPlatformSysImageDiskUsage	Uso del disco en los dispositivos de Manager y Edge para la partición /image (NSX-T 2.5).
vmwNSXDhcpPoolUsageOverloadedEvent	Grupo de DHCP sobrecargado/normal (NSX-T 2.5).
vmwNSXDhcpPoolLeaseAllocationFailedEvent	La asignación de concesión de grupo de DHCP se realizó/no se realizó correctamente (NSX-T 2.5).
vmwNSXPlatformPasswordExpiryStatus	Caducidad de la contraseña de Manager (NSX-T 2.4).
vmwNSXPlatformCertificateExpiryStatus	Caducidad del certificado de Manager (NSX-T 2.4).
vmwNSXRoutingBgpNeighborStatus	Estado de vecino BGP (NSX-T 2.2).
vmwNSXVpnTunnelState	Túnel de VPN activo/inactivo (NSX-T 2.2).
vmwNSXVpnL2TunnelStatus	Sesión de VPN de capa 2 activa/inactiva (NSX-T 2.2).
vmwNSXVpnIkeSessionStatus	Sesión de IKE activa/inactiva (NSX-T 2.2).
vmwNSXDnsForwarderStatus	Estado del reenviador de DNS (NSX-T 2.4).
vmwNSXClusterNodeStatus	Estado del nodo de clúster (NSX-T 2.4).
vmwNSXFabricCryptoStatus	El controlador MUX criptográfico de Edge pasó/no pasó las pruebas Known_Answer_Tests (KAT) (NSX-T 2.4).

Tabla 12-3. Eventos del sistema de NSX-T (continuación)

Nombre del evento	Descripción
El uso del disco de Manager no es correcto	
Vecino BGP inactivo	Necesita una alerta cuando el vecino BGP está inactivo.
Vecino BGP activo	La alarma se borra cuando un vecino se active.
Uso de almacenamiento superior a X	Se genera una alarma para el evento Uso de almacenamiento superior a X en todos los nodos de transporte (Edge, host) o las máquinas virtuales (MP, CCP) del dispositivo.
Uso de memoria superior a X	Se genera una alarma para el evento Uso de memoria superior a X en todos los nodos de transporte (Edge, host) o las máquinas virtuales (MP, CCP) del dispositivo.
Uso de CPU superior a X	Se genera una alarma para el evento Uso de CPU superior a X en todos los nodos de transporte (Edge, host) o las máquinas virtuales (MP, CCP) del dispositivo.

Herramientas de supervisión avanzadas

NSX-T admite métodos de supervisión avanzados, como la visualización de conexiones de puerto, Traceflow, creación de reflejo de puertos, supervisión de actividades, etc.

Consultar información sobre la conexión de puertos

Puede utilizar la herramienta de conexión de puertos para ver rápidamente la conexión entre dos máquinas virtuales, así como para solucionar los problemas relacionados con dicha conexión.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > Conexión de puertos** en el panel de navegación.
- 3 Seleccione una máquina virtual en el menú desplegable **Máquina virtual de origen**.
- 4 Seleccione una máquina virtual en el menú desplegable **Máquina virtual de destino**.
- 5 Haga clic en **Ir**.

Se mostrará un mapa visual de la topología de la conexión de puertos. Puede hacer clic en cualquiera de los componentes de este mapa para obtener más información sobre ese componente.

Traceflow

Traceflow le permite introducir un paquete en la red y supervisar su flujo. Este flujo le permite supervisar su red e identificar problemas, como cuellos de botella o interrupciones.

De esta forma, puede identificar qué ruta (o rutas) toma un paquete para llegar a su destino o, a la inversa, en qué parte del trayecto se descarta un paquete. Cada entidad informa sobre la entrega del paquete en la entrada y la salida, por lo que es posible determinar si se producen problemas al recibir un paquete o al reenviarlo.

Traceflow no es lo mismo que la respuesta o la solicitud de ping que va de una pila a otra de la máquina virtual invitada. Traceflow observa el recorrido de un paquete marcado por la red de superposición. Cada paquete se supervisa a medida que cruza la red de superposición hasta que llega a la máquina virtual invitada de destino o a un vínculo superior de Edge. Tenga en cuenta que el paquete marcado inyectado nunca se entrega realmente a la máquina virtual invitada de destino.

Traceflow se puede utilizar en nodos de transporte y es compatible con los protocolos IPv4 e IPv6, incluidos: ICMP, TCP, UDP, DHCP, DNS y ARP/NDP.

Puede construir paquetes con campos de encabezado y tamaños de paquete personalizados. En Traceflow, se puede utilizar como origen o destino un puerto de conmutador lógico, un puerto de vínculo superior del enrutador lógico, un puerto de CPS o un puerto de DHCP. El extremo de destino puede ser cualquier dispositivo de la red superpuesta o subordinada de NSX. Sin embargo, no puede seleccionar un destino que esté por encima de un nodo de NSX Edge. El destino debe estar en la misma subred o debe ser accesible mediante enrutadores lógicos distribuidos de NSX.

Si se configura el puente de NSX, los paquetes con direcciones MAC de destino desconocido siempre se envían al puente. Normalmente, el puente reenvía estos paquetes a una VLAN e informa de que el paquete de Traceflow se ha entregado. El hecho de que un paquete se marque como entregado no implica necesariamente que el paquete de seguimiento se haya entregado al destino especificado.

Las observaciones de Traceflow pueden incluir las observaciones de los paquetes difundidos de Traceflow. El host ESXi difunde un paquete de Traceflow si no conoce las direcciones MAC del host de destino. Para el tráfico de difusión, el origen es una vNIC de máquina virtual. La dirección MAC de destino de Capa 2 para el tráfico de difusión es FF:FF:FF:FF:FF:FF. Si desea crear un paquete válido para la inspección de firewall, la operación de Traceflow de difusión requiere una longitud de prefijo de subred. La máscara de subred permite que NSX calcule una dirección de red IP para el paquete.

Rastrear la ruta de un paquete con Traceflow

Utilice Traceflow para inspeccionar la ruta de acceso de un paquete. Traceflow rastrea la ruta de nivel de nodo de transporte de un paquete. El paquete de rastreo atraviesa la superposición del conmutador lógico, pero no es visible para las interfaces asociadas al conmutador lógico. En otras palabras, no se envía ningún paquete a los destinatarios objetivo del paquete de prueba.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

2 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > Traceflow**.

3 Seleccione el tipo de dirección IPv4 o IPv6.

4 Seleccione un tipo de tráfico.

Para las direcciones IPv4, los tipos de tráfico disponibles son Unidifusión, Multidifusión y Difusión. Para las direcciones IPv6, las opciones de tipo de tráfico disponibles son Unidifusión o Multidifusión.

Nota: No se admiten la difusión ni la multidifusión en entornos de VMware Cloud (VMC).

5 Especifique la información de origen y de destino según el tipo de tráfico.

Tipo de tráfico	Origen	Destino
Unidifusión	<p>Seleccione una máquina virtual o un puerto lógico. Para una máquina virtual:</p> <ul style="list-style-type: none"> ■ Seleccione una máquina virtual de la lista desplegable. ■ Seleccione una interfaz virtual. ■ La dirección MAC y la dirección IP se muestran si VMtools está instalado en la máquina virtual o si esta se implementa con el complemento de OpenStack (se utilizarán enlaces de direcciones en este caso). Si la máquina virtual tiene varias direcciones IP, seleccione una de la lista desplegable. ■ Si la dirección IP y la dirección MAC no se muestran, introdúzcalas en los cuadros de texto. <p>Para un puerto lógico:</p> <ul style="list-style-type: none"> ■ Seleccione un tipo de archivo adjunto: VIF, DHCP, Vínculo superior de Edge o Servicio centralizado de Edge. ■ Seleccione un puerto. 	<p>Seleccione una máquina virtual, un puerto lógico o una IP de MAC. Para una máquina virtual:</p> <ul style="list-style-type: none"> ■ Seleccione una máquina virtual de la lista desplegable. ■ Seleccione una interfaz virtual. ■ La dirección MAC y la dirección IP se muestran si VMtools está instalado en la máquina virtual o si esta se implementa con el complemento de OpenStack (se utilizarán enlaces de direcciones en este caso). Si la máquina virtual tiene varias direcciones IP, seleccione una de la lista desplegable. ■ Si la dirección IP y la dirección MAC no se muestran, introdúzcalas en los cuadros de texto. <p>Para un puerto lógico:</p> <ul style="list-style-type: none"> ■ Seleccione un tipo de archivo adjunto: VIF, DHCP, Vínculo superior de Edge o Servicio centralizado de Edge. ■ Seleccione un puerto. <p>Para una IP de MAC:</p> <ul style="list-style-type: none"> ■ Seleccione el tipo de rastreo (Capa 2 o 3). Para Capa 2, introduzca una dirección IP y una dirección MAC. Para Capa 3, introduzca una dirección IP.
Multidifusión	Se aplican las instrucciones anteriores.	Introduzca una dirección IP. Debe ser una dirección de multidifusión desde 224.0.0.0 hasta 239.255.255.255.
Difusión	Se aplican las instrucciones anteriores.	Introduzca una longitud de prefijo de subred.

6 (opcional) Haga clic en **Avanzado** para ver las opciones avanzadas.

- 7 (opcional) En la columna de la izquierda, escriba los valores que desee o introduzca datos en los siguientes campos:

Opción	Descripción
Tamaño de trama	El valor predeterminado es 128.
TTL	El valor predeterminado es 64.
Tiempo de espera (ms)	El valor predeterminado es 10000.
EtherType	El valor predeterminado es 2048.
Tipo de carga útil	Seleccione Base64 , Hexadecimal , Texto sin formato , Binario o Decimal .
Datos de carga útil	La carga útil con formato según el tipo seleccionado.

- 8 (opcional) Seleccione un protocolo y proporcione la información relacionada.

Protocolo	Parámetros
TCP	Especifique un puerto de origen, un puerto de destino y las marcas TCP.
UDP	Especifique un puerto de origen y un puerto de destino.
ICMPv6	Especifique un identificador de ICMP y una secuencia.
ICMP	Especifique un identificador de ICMP y una secuencia.
DHCPv6	Seleccione un tipo de mensaje DHCP: Petición , Anuncio , Solicitud o Respuesta .
DHCP	Seleccione un código de operación de DHCP: Solicitud de arranque o Respuesta de arranque .
DNS	Especifique una dirección y seleccione un tipo de mensaje: Consulta o Respuesta .

- 9 Haga clic en **Rastrear**.

Se mostrará información sobre las conexiones, los componentes y las capas. El resultado incluye una tabla con el Tipo de observación, ya sea Entregado, Descartado, Recibido o Reenviado, el Nodo de transporte y el Componente, así como un mapa gráfico de la topología si la difusión y el conmutador lógico como destino están seleccionados. Puede aplicar un filtro, ya sea **Todo**, **Enviado** o **Descartado**, en las observaciones que se muestran. Si hay observaciones descartadas, el filtro **Descartado** se aplica de forma predeterminada. De lo contrario, se aplica el filtro **Todo**. El mapa gráfico muestra los vínculos del backplane y el enrutador. Tenga en cuenta que no se muestra la información de puentes.

Supervisar las sesiones de creación de reflejo del puerto

Puede supervisar las sesiones de creación de reflejo del puerto para solucionar problemas y para otros fines.

Tenga en cuenta que la extensión lógica solo es compatible con conmutadores lógicos de superposición y no con conmutadores lógicos de VLAN.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

Esta función tiene las siguientes restricciones:

- Un puerto de reflejo de origen no puede encontrarse en más de una sesión de reflejo.
- Con KVM, se pueden asociar varias NIC al mismo puerto OVS. La creación del reflejo se produce en el puerto de vínculo superior OVS, lo que significa que el tráfico de todas las pNIC asociadas al puerto OVS se refleja.
- Para una sesión de SPAN, los puertos de origen y destino de la sesión de reflejo deben estar en el mismo vSwitch del host. Por lo tanto, si ejecuta vMotion en la máquina virtual que tiene el puerto de origen o de destino en otro host, el tráfico de ese puerto no podrá reflejarse.
- En ESXi, cuando la creación de reflejo está habilitada en el vínculo superior, VDL2 encapsula en paquetes UDP los paquetes TCP de producción sin procesar usando el protocolo Geneve. Una NIC física que admite TSO (descarga de segmentación TCP) puede cambiar los paquetes y asignarles la marca MUST_TSO. En una máquina virtual de supervisión con vNIC VMXNET3 o E1000, el controlador trata el paquete como los paquetes UDP normales, no puede permitir la marca MUST_TSO y descartará los paquetes.

Si una gran cantidad de tráfico se refleja en una máquina virtual de supervisión, existe la posibilidad de que el anillo del búfer de la unidad se llene y los paquetes se descarten. Para mitigar el problema, puede llevar a cabo una o varias de las siguientes acciones:

- Aumentar el tamaño del anillo del búfer rx.
- Asignar más recursos de CPU a la máquina virtual.

- Utilizar el kit de desarrollo de plano de datos (DPDK) para mejorar el rendimiento del procesamiento de paquetes.

Nota Compruebe que la configuración de MTU de la máquina virtual de supervisión (en el caso de KVM, también la configuración de MTU del dispositivo de la NIC virtual del hipervisor) sea lo suficientemente grande para gestionar los paquetes. Esto es especialmente importante para los paquetes encapsulados, ya que la encapsulación aumenta el tamaño de los paquetes. De lo contrario, es posible que los paquetes se descarten. Esto no supone un problema con las máquinas virtuales ESXi con las NIC VMXNET3, pero sí puede serlo con otros tipos de NIC tanto en máquinas virtuales ESXi como en KVM.

Nota En una sesión de creación de reflejo del puerto L3 que incluye las máquinas virtuales que se encuentran en los hosts KVM, debe configurar el tamaño de MTU para que sea lo suficientemente grande para admitir los bits adicionales que requiere la encapsulación. El tráfico de creación de reflejo se dirige a través de una interfaz OVS y un vínculo superior OVS. Debe establecer la MTU de la interfaz de OVS para que sea, al menos, 100 bits superior al tamaño del paquete original (antes de la encapsulación y de la creación de reflejo). Si observa que se descarten paquetes, aumente la opción de la MTU para la interfaz OVS y la NIC virtual del host. Use el siguiente comando para establecer la MTU de una interfaz OVS:

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

Nota Cuando supervisa el puerto lógico de una máquina virtual y el puerto del vínculo superior de un host donde se encuentra la máquina virtual, observará diferentes comportamientos dependiendo de si el host es ESXi o KVM. Para ESXi, los paquetes de creación de reflejo del puerto lógico y los paquetes de creación de reflejo del vínculo superior se etiquetan con el mismo ID de VLAN y aparecen igual en la máquina virtual de supervisión. Para KVM, los paquetes de creación de reflejo del puerto lógico no se etiquetan con una ID de VLAN, pero los paquetes de creación de reflejo del vínculo superior se etiquetan y aparecen de forma diferente en la máquina virtual de supervisión.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 3 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > Sesión de creación de reflejo de puerto**.
- 4 Haga clic en **Agregar** y seleccione un tipo de sesión.
Los tipos disponibles son **SPAN local**, **SPAN remoto**, **SPAN de Capa 3 remoto** y **SPAN lógico**.
- 5 Introduzca un nombre de sesión y, si lo desea, una descripción.

6 Proporcione parámetros adicionales.

Tipo de sesión	Parámetros
SPAN local	<ul style="list-style-type: none"> ■ Nodo de transporte: seleccione un nodo de transporte. ■ Dirección: seleccione Bidireccional, Entrada o Salida. ■ Truncamiento de paquetes: seleccione un valor de truncamiento de paquetes.
SPAN remoto	<ul style="list-style-type: none"> ■ Tipo de sesión: seleccione Sesión de origen de RSPAN o Sesión de destino de RSPAN. ■ Nodo de transporte: seleccione un nodo de transporte. ■ Dirección: seleccione Bidireccional, Entrada o Salida. ■ Truncamiento de paquetes: seleccione un valor de truncamiento de paquetes. ■ Identificador de VLAN encapsulado: especifique un identificador de VLAN encapsulado. ■ Conservar VLAN original (Preserve Original VLAN): seleccione si desea conservar el identificador de VLAN original.
SPAN de Capa 3 remoto	<ul style="list-style-type: none"> ■ Encapsulación: seleccione GRE, ERSPAN TWO o ERSPAN THREE. ■ Clave de GRE: especifique una clave de GRE si la encapsulación es GRE. Identificador de ERSPAN: especifique un identificador de ERSPAN si la encapsulación es ERSPAN TWO o ERSPAN THREE. ■ Dirección: seleccione Bidireccional, Entrada o Salida. ■ Truncamiento de paquetes: seleccione un valor de truncamiento de paquetes.
SPAN lógico	<ul style="list-style-type: none"> ■ Conmutador lógico: seleccione un conmutador lógico. ■ Dirección: seleccione Bidireccional, Entrada o Salida. ■ Truncamiento de paquetes: seleccione un valor de truncamiento de paquetes.

7 Haga clic en **Siguiente**.

8 Proporcione la información de origen.

Tipo de sesión	Parámetros
SPAN local	<ul style="list-style-type: none"> ■ Seleccione un N-VDS. ■ Seleccione las interfaces físicas. ■ Habilite o deshabilite el paquete encapsulado. ■ Seleccione las máquinas virtuales. ■ Seleccione las interfaces virtuales.
SPAN remoto	<ul style="list-style-type: none"> ■ Seleccione las máquinas virtuales. ■ Seleccione las interfaces virtuales.
SPAN de Capa 3 remoto	<ul style="list-style-type: none"> ■ Seleccione las máquinas virtuales. ■ Seleccione las interfaces virtuales. ■ Seleccione un conmutador lógico.
SPAN lógico	<ul style="list-style-type: none"> ■ Seleccione los puertos lógicos.

9 Haga clic en **Siguiente**.

10 Proporcione la información de destino.

Tipo de sesión	Parámetros
SPAN local	<ul style="list-style-type: none"> ■ Seleccione las máquinas virtuales. ■ Seleccione las interfaces virtuales.
SPAN remoto	<ul style="list-style-type: none"> ■ Seleccione un N-VDS. ■ Seleccione las interfaces físicas.
SPAN de Capa 3 remoto	<ul style="list-style-type: none"> ■ Especifique una dirección IPv4.
SPAN lógico	<ul style="list-style-type: none"> ■ Seleccione los puertos lógicos.

11 Haga clic en **Guardar**.

No puede cambiar el origen ni el destino después de guardar la sesión de creación de reflejo del puerto.

Configurar filtros para un sesión de creación de reflejo del puerto

Es posible configurar filtros para las sesiones de creación de reflejo del puerto que ayuden a limitar la cantidad de datos que se reflejan.

Esta función presenta las siguientes capacidades y restricciones:

- Solo se admiten nodos de transporte de host de ESXi y KVM.
- Se admite la dirección IP, el prefijo IP y los rangos de IP de origen y destino.
- No se admite IPSet para el origen o el destino.
- No se admiten las estadísticas de reflejo en ESXi ni KVM.

Debe configurar los filtros mediante la API. No se permite usar la interfaz de usuario de NSX Manager. Si necesita más información sobre la API de creación de reflejo del puerto y el esquema de `PortMirroringFilter`, consulte la *Referencia de API de NSX-T Data Center*.

Procedimiento

- 1 Configure una sesión de creación de reflejo del puerto con la API o la interfaz de usuario de NSX Manager.
- 2 Llame a la API de GET `/api/v1/mirror-sessions` para obtener información sobre la sesión de creación de reflejo del puerto.
- 3 Llame a la API de GET `/api/v1/mirror-sessions/<mirror-session-id>` para agregar uno o varios filtros. Por ejemplo,

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
  "display_name": "port-mirror-session-1",
  "description": "Pnic port mirror session 1",
```

```

"mirror_sources": [
  {
    "resource_type": "LogicalPortMirrorSource",
    "port_ids": [
      "6a361832-43e4-430d-a48a-b84a6cba73c3"
    ]
  }
],
"mirror_destination": {
  "resource_type": "LogicalPortMirrorDestination",
  "port_ids": [
    "3e42e8b2d-3047-4550-b230-dd1ee0e10b34"
  ]
},
"port_mirroring_filters": [
  {
    "filter_action": "MIRROR",
    "src_ips": {
      "ip-addresses": [
        "192.168.175.250",
        "2001:bd6::c:2957:160:126"
      ]
    },
    "dst_ips": {
      "ip-addresses": [
        "192.168.160.126",
        "2001:bd6::c:2957:175:250"
      ]
    }
  }
]
"session_type": "LogicalPortMirrorSession",
"preserve_original_vlan": false,
"direction": "BIDIRECTIONAL",
"_revision": 0
}

```

- 4 (opcional) Puede llamar al comando CLI de `get mirroring-session <session-number>` para mostrar las propiedades de la sesión de creación de reflejo del puerto, incluidos los filtros.

Configurar IPFIX

IPFIX (Exportación de información de flujo de protocolo de Internet) es un estándar para el formato y la exportación de información de flujo de red. Puede configurar IPFIX para conmutadores y firewalls. En el caso de los conmutadores, se exporta el flujo de la red en las VIF (interfaces virtuales) y las pNIC (NIC físicas). En el caso de los firewalls, se exporta el flujo que administra el componente del firewall distribuido.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

Esta función cumple con los criterios especificados en RFC 7011 y RFC 7012.

Al habilitar IPFIX, todos los nodos de transporte host enviarán mensajes IPFIX a los recopiladores IPFIX mediante el puerto 4739. En el caso de ESXi, NSX-T Data Center abre el puerto 4739 de forma automática. En el caso de KVM, si no está habilitado el firewall, se abre el puerto 4739, pero, si está habilitado, debe asegurarse de que el puerto esté abierto, porque NSX-T Data Center no lo abre de forma automática.

IPFIX en ESXi y KVM realiza el muestreo de paquetes de túnel siguiendo diferentes procedimientos. En ESXi, se realiza el muestreo del paquete de túnel como dos registros:

- Registro de paquetes externo con alguna información del paquete interno
 - SrcAddr, DstAddr, SrcPort, DstPort y Protocol se refieren al paquete externo.
 - Contiene entradas empresariales para describir el paquete interno.
- Registro de paquete interno
 - SrcAddr, DstAddr, SrcPort, DstPort y Protocol se refieren al paquete interno.

En KVM, se realiza el muestreo del paquete de túnel según un registro:

- Registro del paquete interno con alguna información del túnel externo
 - SrcAddr, DstAddr, SrcPort, DstPort y Protocol se refieren al paquete interno.
 - Contiene algunas entradas empresariales para describir el paquete externo.

Configurar recopiladores IPFIX para conmutadores

Puede configurar recopiladores IPFIX para conmutadores.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > IPFIX**.
- 3 Haga clic en la pestaña **Recopiladores IPFIX para el conmutador**.
- 4 Haga clic en **Agregar** para agregar un recopilador.
- 5 Introduzca un nombre y, si lo desea, una descripción.
- 6 Haga clic en **Agregar** y escriba la dirección IP y el puerto de un recopilador.
Puede agregar hasta 4 recopiladores.
- 7 Haga clic en **Agregar**.

Configurar perfiles IPFIX para los conmutadores

Puede configurar perfiles IPFIX para los conmutadores.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > IPFIX**.
- 3 Haga clic en la pestaña **Perfiles de IPFIX para el conmutador**.
- 4 Haga clic en **Agregar** para agregar un perfil.

Opción	Descripción
Nombre y descripción	<p>Introduzca un nombre y, si lo desea, una descripción.</p> <p>Nota Si desea crear un perfil global, asigne al perfil el nombre Global. No se puede editar ni eliminar un perfil global de la interfaz de usuario, pero puede hacerlo con las API de NSX-T Data Center.</p>
Tiempo de espera activo (segundos)	El tiempo tras el que se agotará el tiempo de espera de un flujo aunque se reciban más paquetes asociados al flujo. El valor predeterminado es 300.
Tiempo de espera inactivo (segundos)	El tiempo tras el que se agotará el tiempo de espera de un flujo si no se reciben más paquetes asociados al flujo (solo en ESXi, KVM agota el tiempo de todos los flujos basándose en el tiempo de espera activo). El valor predeterminado es 300.
Flujos máximos	Los flujos máximos que se almacenan en caché en un puente (solo en KVM, no se puede configurar en ESXi). El valor predeterminado es 16384.
Exportar flujo superpuesto	Ajuste que controla si el resultado de muestra incluye información sobre el flujo superpuesto.
Probabilidad de muestreo (%)	El porcentaje de paquetes que se van a muestrear (aproximadamente). Aumentar este valor podría afectar negativamente al rendimiento de hipervisores y recopiladores. Si todos los hipervisores envían más paquetes IPFIX al recopilador, este podría no ser capaz de recopilálos todos. Establecer la probabilidad en el valor predeterminado, que es del 0,1%, mantiene bajo el impacto que se tiene sobre el rendimiento.
Identificador de dominio de observación	El identificador del dominio de observación identifica desde qué dominio de observación se originan los flujos de red. Escriba 0 para indicar que no hay un dominio de observación específico.
Perfil del recopilador	Seleccione un recopilador IPFIX para el conmutador que haya configurado en el paso anterior.
Prioridad	Este parámetro resuelve los conflictos cuando se aplican varios perfiles. El exportador IPFIX solo usará el perfil con la prioridad más alta. Un valor inferior significa una prioridad más elevada.

- 5 Haga clic en **Agregar**.

Configurar recopiladores IPFIX para los firewalls

Puede configurar recopiladores IPFIX para los firewalls.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > IPFIX**.
- 3 Haga clic en la pestaña **Recopiladores IPFIX para los firewalls**.
- 4 Haga clic en **Agregar** para agregar un recopilador.
- 5 Introduzca un nombre y, si lo desea, una descripción.
- 6 Haga clic en **Agregar** y escriba la dirección IP y el puerto de un recopilador.
Puede agregar hasta 4 recopiladores.
- 7 Haga clic en **Agregar**.

Configurar perfiles de IPFIX para los firewalls

Puede configurar perfiles de IPFIX para los firewalls.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Herramientas > IPFIX**.
- 3 Haga clic en la pestaña **Perfiles de IPFIX para los firewalls**.
- 4 Haga clic en **Agregar** para agregar un perfil.

Opción	Descripción
Nombre y descripción	<p>Introduzca un nombre y, si lo desea, una descripción.</p> <p>Nota Si desea crear un perfil global, asigne al perfil el nombre Global. No se puede editar ni eliminar un perfil global de la interfaz de usuario, pero puede hacerlo con las API de NSX-T Data Center.</p>
Configuración del recopilador	Seleccione un recopilador de la lista desplegable.
Tiempo de espera de exportación de flujo activo (minutos)	El tiempo tras el que se agotará el tiempo de espera de un flujo aunque se reciban más paquetes asociados al flujo. El valor predeterminado es 1.
Prioridad	Este parámetro resuelve los conflictos cuando se aplican varios perfiles. El exportador IPFIX solo usará el perfil con la prioridad más alta. Un valor inferior significa una prioridad más elevada.
Identificador de dominio de observación	Este parámetro identifica desde qué dominio de observación se originan los flujos de red. El valor predeterminado es 0, que indica que no hay ningún dominio de observación específico.

- 5 Haga clic en **Agregar**.

Plantillas IPFIX de ESXi

Un nodo de transporte de host ESXi admite ocho plantillas de flujos de IPFIX de conmutadores lógicos y dos plantillas de flujos de IPFIX de firewall distribuido.

En la siguiente tabla se indican los elementos específicos de VMware en los paquetes de IPFIX de conmutadores lógicos.

ID de elemento	Nombre del parámetro	Tipo de datos	Unidad
880	tenantProtocol	unsigned8	1 byte
881	tenantSourceIPv4	ipv4Address	4 bytes
882	tenantDestIPv4	ipv4Address	4 bytes
883	tenantSourceIPv6	ipv6Address	16 bytes
884	tenantDestIPv6	ipv6Address	16 bytes
886	tenantSourcePort	unsigned16	2 bytes
887	tenantDestPort	unsigned16	2 bytes
888	egressInterfaceAttr	unsigned16	2 bytes
889	vxlانExportRole	unsigned8	1 byte
890	ingressInterfaceAttr	unsigned16	2 bytes
898	virtualObsID	string	longitud variable

En la siguiente tabla se indican los elementos específicos de VMware en los paquetes de IPFIX de firewall distribuido.

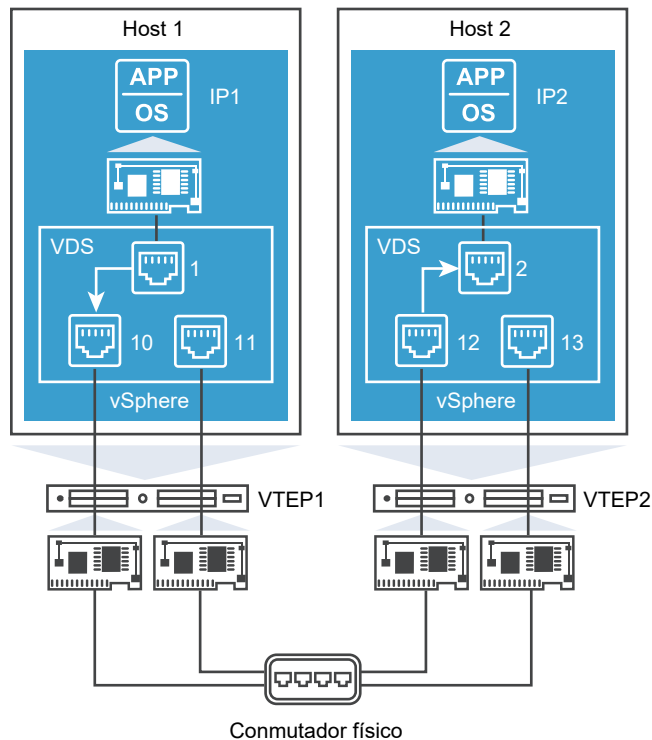
ID de elemento	Nombre del parámetro	Tipo de datos	Unidad
950	ruleId	unsigned32	4 bytes
951	vmUuid	string	16 bytes
952	vnidIndex	unsigned32	4 bytes
953	sessionFlags	unsigned8	1 byte
954	flowDirection	unsigned8	1 byte
955	algControlFlowId	unsigned64	8 bytes
956	algType	unsigned8	1 byte
957	algFlowType	unsigned8	1 byte
958	averageLatency	unsigned32	4 bytes
959	retransmissionCount	unsigned32	4 bytes

ID de elemento	Nombre del parámetro	Tipo de datos	Unidad
960	vifUuid	octetArray	16 bytes
961	vifId	string	longitud variable

Plantillas IPFIX de conmutadores lógicos ESXi

Un nodo de transporte de host ESXi es compatible con ocho plantillas de flujo IPFIX de conmutadores lógicos.

El siguiente diagrama muestra el flujo de tráfico entre las máquinas virtuales conectadas a los hosts ESXi supervisados por la función IPFIX:



La plantilla encapsulada de IPv4 incluye los siguientes elementos:

- elementos estándar
- SrcAddr: VTEP1
- DstAddr: VTEP2
- tenantSourceIPv4: IP1
- tenantDestIPv4: IP2
- tenantSourcePort: 10000
- tenantDestPort: 80
- tenantProtocol: TCP

- ingressInterfaceAttr: 0x03 (puerto de túnel)
- egressInterfaceAttr: 0x01
- encapExportRole: 01
- virtualObsID: 89fd5032-2dc9-4fc3-993a-9bb4b616de54 (identificador de puerto lógico)

Plantilla IPv4

ID de plantilla: 256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

Plantilla encapsulada de IPv4

ID de plantilla: 257

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
```

```

IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

Plantilla IPv4 ICMP

ID de plantilla: 258

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

Plantilla encapsulada de IPv4 ICMP

ID de plantilla: 259

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)

```

```

IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

Plantilla IPv6

ID de plantilla: 260

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS,1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

Plantilla encapsulada de IPv6

ID de plantilla: 261

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()
```

Plantilla IPv6 ICMP

ID de plantilla: 262

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
```

```
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()
```

Plantilla encapsulada de IPv6 ICMP

ID de plantilla: 263

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

Plantillas IPFIX de firewall distribuido de ESXi

Los nodos de transporte de host ESXi admiten dos plantillas de flujo IPFIX de firewall distribuido.

Plantilla IPv4

ID de plantilla: 288

```
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD icmpTypeIPv4, 1)
IPFIX_TEMPLATE_FIELD icmpCodeIPv4, 1)
```

```

IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

Plantilla IPv6

ID de plantilla: 289

```

IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

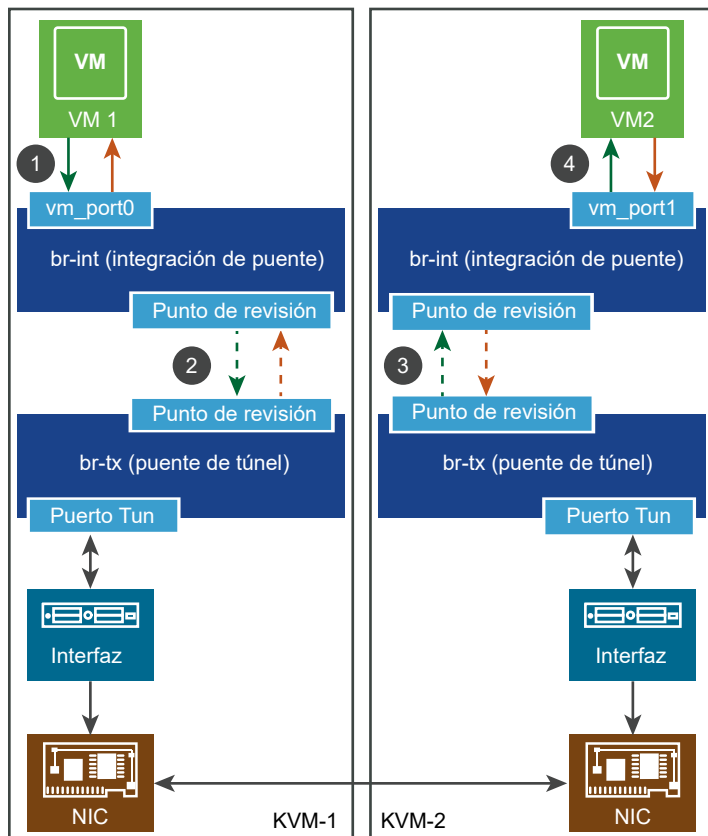
Plantillas IPFIX de KVM

Un nodo de transporte de host KVM admite 88 plantillas de flujo IPFIX y 1 plantilla de opciones.

En la siguiente tabla, se enumeran los elementos específicos de VMware en los paquetes IPFIX de KVM.

ID de elemento	Nombre del parámetro	Tipo de datos	Unidad
891	tunnelType	unsigned8	1 byte
892	tunnelKey	bytes	longitud variable
893	tunnelSourceIPv4Address	unsigned32	4 bytes
894	tunnelDestinationIPv4Address	unsigned32	4 bytes
895	tunnelProtocolIdentifier	unsigned8	1 byte
896	tunnelSourceTransportPort	unsigned16	2 bytes
897	tunnelDestinationTransportPort	unsigned16	2 bytes
898	virtualObsID	string	longitud variable

El siguiente diagrama muestra el flujo de tráfico entre las máquinas virtuales conectadas a los hosts de KVM supervisados por la función IPFIX:



La plantilla de entrada de IPFIX de KVM IPv4 tendrá los siguientes elementos:

- elementos estándar
- `virtualObsID`: 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34 (identificador de puerto lógico)

Plantillas IPFIX de KVM Ethernet

Existen cuatro plantillas IPFIX de KVM Ethernet: entrada, salida, entrada con túnel y salida con túnel.

Entrada de Ethernet

ID de plantilla: 256. Recuento de campo: 27.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)

- flowEndReason (longitud: 1)

Salida de Ethernet

ID de plantilla: 257. Recuento de campo: 31.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 8)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)

- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Entrada de Ethernet con túnel

ID de plantilla: 258. Recuento de campo: 34.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)

- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Salida de Ethernet con túnel

ID de plantilla: 259. Recuento de campo: 38.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 8)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])

- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Plantillas IPFIX de KVM IPv4

Existen cuatro plantillas IPFIX de KVM IPv4: entrada, salida, entrada con túnel y salida con túnel.

Entrada de IPv4

ID de plantilla: 276. Recuento de campo: 45.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)

- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)

- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de IPv4

ID de plantilla: 277. Recuento de campo: 49.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)

- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Entrada de IPv4 con túnel

ID de plantilla: 278. Recuento de campo: 52.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)

- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)

- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de IPv4 con túnel

ID de plantilla: 279. Recuento de campo: 56.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)

- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)

- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM TCP por IPv4

Existen cuatro plantillas IPFIX de KVM TCP por IPv4: entrada, salida, entrada con túnel y salida con túnel.

Entrada de TCP por IPv4

ID de plantilla: 280. Recuento de campo: 53.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)

- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)

- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv4

ID de plantilla: 281. Recuento de campo: 57.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])

- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Entrada de TCP por IPv4 con túnel

ID de plantilla: 282. Recuento de campo: 60.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)

- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv4 con túnel

ID de plantilla: 283. Recuento de campo: 64.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])

- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)

- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Plantillas IPFIX de KVM UDP por IPv4

Existen cuatro plantillas IPFIX de KVM UDP por IPv4: entrada, salida, entrada con túnel y salida con túnel.

Entrada de UDP por IPv4

ID de plantilla: 284. Recuento de campo: 47.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)

- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de UDP por IPv4

ID de plantilla: 285. Recuento de campo: 51.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)

- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)

- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de UDP por IPv4 con túnel

ID de plantilla: 286. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)

- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)

- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de UDP por IPv4 con túnel

ID de plantilla: 287. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)

- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)

- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM SCTP por IPv4

Existen cuatro plantillas IPFIX de KVM SCTP por IPv4: entrada, salida, entrada con túnel y salida con túnel.

Entrada de SCTP por IPv4

ID de plantilla: 288. Recuento de campo: 47.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)

- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv4

ID de plantilla: 289. Recuento de campo: 51.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)

- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)

- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Entrada de SCTP por IPv4 con túnel

ID de plantilla: 290. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)

- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)

- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv4 con túnel

ID de plantilla: 291. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)

- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)

- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM ICMPv4

Existen cuatro plantillas IPFIX de KVM ICMPv4: entrada, salida, entrada con túnel y salida con túnel.

Entrada de ICMPv4

ID de plantilla: 292. Recuento de campo: 47.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])

- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de ICMPv4

ID de plantilla: 293. Recuento de campo: 51.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)

- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)

- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de ICMPv4 con túnel

ID de plantilla: 294. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)

- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)

- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de ICMPv4 con túnel

ID de plantilla: 295. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)

- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)

- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM IPv6

Existen cuatro plantillas IPFIX de KVM IPv6: entrada, salida, entrada con túnel y salida con túnel.

Entrada de IPv6

ID de plantilla: 296. Recuento de campo: 46.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)

- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de IPv6

ID de plantilla: 297. Recuento de campo: 50.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)

- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)

- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de IPv6 con túnel

ID de plantilla: 298. Recuento de campo: 53.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)

- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)

- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de IPv6 con túnel

ID de plantilla: 299. Recuento de campo: 57.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)

- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)

- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM TCP por IPv6

Existen cuatro plantillas IPFIX de KVM TCP por IPv6: entrada, salida, entrada con túnel y salida con túnel.

Entrada de TCP por IPv6

ID de plantilla: 300. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)

- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv6

ID de plantilla: 301. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)

- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Entrada de TCP por IPv6 con túnel

ID de plantilla: 302. Recuento de campo: 61.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)

- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)

- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv6 con túnel

ID de plantilla: 303. Recuento de campo: 65.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)

- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)

- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Plantillas IPFIX de KVM UDP por IPv6

Existen cuatro plantillas IPFIX de KVM UDP por IPv6: entrada, salida, entrada con túnel y salida con túnel.

Entrada de UDP por IPv6

ID de plantilla: 304. Recuento de campo: 48.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)

- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de UDP por IPv6

ID de plantilla: 305. Recuento de campo: 52.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)

- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)

- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de UDP por IPv6 con túnel

ID de plantilla: 306. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)

- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)

- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de UDP por IPv6 con túnel

ID de plantilla: 307. Recuento de campo: 59.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)

- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)

- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM SCTP por IPv6

Existen cuatro plantillas IPFIX de KVM SCTP por IPv6: entrada, salida, entrada con túnel y salida con túnel.

Entrada de SCTP por IPv6

ID de plantilla: 308. Recuento de campo: 48.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)

- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv6

ID de plantilla: 309. Recuento de campo: 52.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)

- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)

- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de SCTP por IPv6 con túnel

ID de plantilla: 310. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)

- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)

- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv6 con túnel

ID de plantilla: 311. Recuento de campo: 59.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)

- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM ICMPv6

Existen cuatro plantillas IPFIX de KVM ICMPv6: entrada, salida, entrada con túnel y salida con túnel.

Entrada de ICMPv6

ID de plantilla: 312. Recuento de campo: 48.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)

- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de ICMPv6

ID de plantilla: 313. Recuento de campo: 52.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)

- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Entrada de ICMPv6 con túnel

ID de plantilla: 314. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)

- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)

- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de ICMPv6 con túnel

ID de plantilla: 315. Recuento de campo: 59.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)

- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)

- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM Ethernet VLAN

Existen cuatro plantillas IPFIX de KVM Ethernet VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de Ethernet VLAN

ID de plantilla: 316. Recuento de campo: 30.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)

- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Salida de Ethernet VLAN

ID de plantilla: 317. Recuento de campo: 34.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)

- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 8)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Entrada de Ethernet VLAN con túnel

ID de plantilla: 318. Recuento de campo: 37.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)

- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Salida de Ethernet VLAN con túnel

ID de plantilla: 319. Recuento de campo: 41.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 8)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)

- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

Plantillas IPFIX de KVM IPv4 VLAN

Existen cuatro plantillas IPFIX de KVM IPv4 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de IPv4 VLAN

ID de plantilla: 336. Recuento de campo: 48.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)

- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)

- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de IPv4 VLAN

ID de plantilla: 337. Recuento de campo: 52.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)

- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de IPv4 VLAN con túnel

ID de plantilla: 338. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)

- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)

- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de IPv4 VLAN con túnel

ID de plantilla: 339. Recuento de campo: 59.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)

- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)

- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM TCP por IPv4 VLAN

Existen cuatro plantillas IPFIX de KVM TCP por IPv4 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de TCP por IPv4 VLAN

ID de plantilla: 340. Recuento de campo: 56.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)

- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)

- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv4 VLAN

ID de plantilla: 341. Recuento de campo: 60.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)

- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)

- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Entrada de TCP por IPv4 VLAN con túnel

ID de plantilla: 342. Recuento de campo: 63.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)

- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv4 VLAN con túnel

ID de plantilla: 343. Recuento de campo: 67.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)

- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)

- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Plantillas IPFIX de KVM UDP por IPv4 VLAN

Existen cuatro plantillas IPFIX de KVM UDP por IPv4 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de UDP por IPv4 VLAN

ID de plantilla: 344. Recuento de campo: 50.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)

- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)

- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de UDP por IPv4 VLAN

ID de plantilla: 345. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)

- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)

- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Entrada de UDP por IPv4 VLAN con túnel

ID de plantilla: 346. Recuento de campo: 57.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)

- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)

- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de UDP por IPv4 VLAN con túnel

ID de plantilla: 347. Recuento de campo: 61.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)

- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)

- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM SCTP por IPv4 VLAN

Existen cuatro plantillas IPFIX de KVM SCTP por IPv4 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de SCTP por IPv4 VLAN

ID de plantilla: 348. Recuento de campo: 50.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)

- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv4 VLAN

ID de plantilla: 349. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)

- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)

- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de SCTP por IPv4 VLAN con túnel

ID de plantilla: 350. Recuento de campo: 57.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)

- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)

- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv4 VLAN con túnel

ID de plantilla: 351. Recuento de campo: 61.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)

- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)

- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM ICMPv4 VLAN

Existen cuatro plantillas IPFIX de KVM ICMPv4 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de ICMPv4 VLAN

ID de plantilla: 352. Recuento de campo: 50.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)

- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)

- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de ICMPv4 VLAN

ID de plantilla: 353. Recuento de campo: 54.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)

- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)

- postMCastOctetTotalCount (longitud: 8)

Entrada de ICMPv4 VLAN con túnel

ID de plantilla: 354. Recuento de campo: 57.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])

- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de ICMPv4 VLAN con túnel

ID de plantilla: 355. Recuento de campo: 61.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IP_SRC_ADDR (longitud: 4)
- IP_DST_ADDR (longitud: 4)
- ICMP_IPv4_TYPE (longitud: 1)
- ICMP_IPv4_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])

- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM IPv6 VLAN

Existen cuatro plantillas IPFIX de KVM IPv6 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de IPv6 VLAN

ID de plantilla: 356. Recuento de campo: 49.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)

- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de IPv6 VLAN

ID de plantilla: 357. Recuento de campo: 53.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)

- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)

- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Entrada de IPv6 VLAN con túnel

ID de plantilla: 358. Recuento de campo: 56.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)

- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)

- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de IPv6 VLAN con túnel

ID de plantilla: 359. Recuento de campo: 60.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)

- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)

- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM TCP por IPv6 VLAN

Existen cuatro plantillas IPFIX de KVM TCP por IPv6 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de TCP por IPv6 VLAN

ID de plantilla: 360. Recuento de campo: 57.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)

- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)

- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv6 VLAN

ID de plantilla: 361. Recuento de campo: 61.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)

- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)

- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Entrada de TCP por IPv6 VLAN con túnel

ID de plantilla: 362. Recuento de campo: 64.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)

- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)

- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Salida de TCP por IPv6 VLAN con túnel

ID de plantilla: 363. Recuento de campo: 68.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)

- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)

- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)
- tcpAckTotalCount (longitud: 8)
- tcpFinTotalCount (longitud: 8)
- tcpPshTotalCount (longitud: 8)
- tcpRstTotalCount (longitud: 8)
- tcpSynTotalCount (longitud: 8)
- tcpUrgTotalCount (longitud: 8)

Plantillas IPFIX de KVM UDP por IPv6 VLAN

Existen cuatro plantillas IPFIX de KVM UDP por IPv6 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de UDP por IPv6 VLAN

ID de plantilla: 364. Recuento de campo: 51.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)

- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)

- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de UDP por IPv6 VLAN

ID de plantilla: 365. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)

- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)

- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de UDP por IPv6 VLAN con túnel

ID de plantilla: 366. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)

- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)

- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de UDP por IPv6 VLAN con túnel

ID de plantilla: 367. Recuento de campo: 62.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)

- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)

- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM SCTP por IPv6 VLAN

Existen cuatro plantillas IPFIX de KVM SCTP por IPv6 VLAN: entrada, salida, entrada con túnel y salida con túnel.

Entrada de SCTP por IPv6 VLAN

ID de plantilla: 368. Recuento de campo: 51.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)

- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv6 VLAN

ID de plantilla: 369. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)

- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)

- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de SCTP por IPv6 VLAN con túnel

ID de plantilla: 370. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)

- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)

- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de SCTP por IPv6 VLAN con túnel

ID de plantilla: 371. Recuento de campo: 62.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)

- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- L4_SRC_PORT (longitud: 2)
- L4_DST_PORT (longitud: 2)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)

- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Plantillas IPFIX de KVM ICMPv6 VLAN

Existen cuatro plantillas IPFIX de KVM ICMPv6: entrada, salida, entrada con túnel y salida con túnel.

Entrada de ICMPv6

ID de plantilla: 372. Recuento de campo: 51.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)

- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)

- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Salida de ICMPv6

ID de plantilla: 373. Recuento de campo: 55.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)

- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)

- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Entrada de ICMPv6 con túnel

ID de plantilla: 374. Recuento de campo: 58.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)
- FLOW_LABEL (longitud: 4)

- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMcastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)
- BYTES_SQUARED_PERMANENT (longitud: 8)

- IP_LENGTH_MINIMUM (longitud: 8)
- IP_LENGTH_MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMcastOctetTotalCount (longitud: 8)

Salida de ICMPv6 con túnel

ID de plantilla: 375. Recuento de campo: 62.

Los campos son:

- observationPointId (longitud: 4)
- DIRECTION (longitud: 1)
- SRC_MAC (longitud: 6)
- DESTINATION_MAC (longitud: 6)
- ethernetType (longitud: 2)
- ethernetHeaderLength (longitud: 1)
- INPUT_SNMP (longitud: 4)
- Unknown(368) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- OUTPUT_SNMP (longitud: 4)
- Unknown(369) (longitud: 4)
- IF_NAME (longitud: variable)
- IF_DESC (longitud: variable)
- SRC_VLAN (longitud: 2)
- dot1qVlanId (longitud: 2)
- dot1qPriority (longitud: 1)
- IP_PROTOCOL_VERSION (longitud: 1)
- IP_TTL (longitud: 1)
- PROTOCOLO (longitud: 1)
- IP_DSCP (longitud: 1)
- IP_PRECEDENCE (longitud: 1)
- IP_TOS (longitud: 1)
- IPV6_SRC_ADDR (longitud: 4)
- IPV6_DST_ADDR (longitud: 4)

- FLOW_LABEL (longitud: 4)
- ICMP_IPv6_TYPE (longitud: 1)
- ICMP_IPv6_CODE (longitud: 1)
- 893 (longitud: 4, PEN: VMware Inc. [6876])
- 894 (longitud: 4, PEN: VMware Inc. [6876])
- 895 (longitud: 1, PEN: VMware Inc. [6876])
- 896 (longitud: 2, PEN: VMware Inc. [6876])
- 897 (longitud: 2, PEN: VMware Inc. [6876])
- 891 (longitud: 1, PEN: VMware Inc. [6876])
- 892 (longitud: variable, PEN: VMware Inc. [6876])
- 898 (longitud: variable, PEN: VMware Inc. [6876])
- flowStartDeltaMicroseconds (longitud: 4)
- flowEndDeltaMicroseconds (longitud: 4)
- DROPPED_PACKETS (longitud: 8)
- DROPPED_PACKETS_TOTAL (longitud: 8)
- PKTS (longitud: 8)
- PACKETS_TOTAL (longitud: 8)
- Unknown(354) (longitud: 8)
- Unknown(355) (longitud: 8)
- Unknown(356) (longitud: 8)
- Unknown(357) (longitud: 8)
- Unknown(358) (longitud: 8)
- MUL_DPKTS (longitud: 8)
- postMCastPacketTotalCount (longitud: 8)
- Unknown(352) (longitud: 8)
- Unknown(353) (longitud: 8)
- flowEndReason (longitud: 1)
- DROPPED_BYTES (longitud: 8)
- DROPPED_BYTES_TOTAL (longitud: 8)
- BYTES (longitud: 8)
- BYTES_TOTAL (longitud: 8)
- BYTES_SQUARED (longitud: 8)

- BYTES_SQUARED_PERMANENT (longitud: 8)
- IP LENGTH MINIMUM (longitud: 8)
- IP LENGTH MAXIMUM (longitud: 8)
- MUL_DOCTETS (longitud: 8)
- postMCastOctetTotalCount (longitud: 8)

Plantillas IPFIX de opciones de KVM

Existe una plantilla de opciones de KVM, según IETF RFC 7011, sección 3.4.2.

Plantilla de opciones

ID de plantilla: 462. Recuento de ámbito: 1. Recuento de datos: 1.

Supervisar la actividad de un puerto del conmutador lógico

Puede supervisar la actividad del puerto lógico para, por ejemplo, solucionar los problemas relacionados con la congestión de la red y los paquetes que se descartan.

Requisitos previos

Compruebe que haya un puerto de conmutador lógico configurado. Consulte [Conectar una VM a un conmutador lógico](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccionar **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos**
- 3 Haga clic en el nombre de un puerto.
- 4 Haga clic en la pestaña **Supervisar**.
Se muestran las estadísticas y el estado del puerto.
- 5 Para descargar un archivo CSV de las direcciones MAC que el host ha aprendido, haga clic en **Descargar tabla de MAC**.
- 6 Para supervisar la actividad en el puerto, haga clic en **Iniciar seguimiento**.
Se abrirá una página de seguimiento de puertos. Puede consultar el tráfico bidireccional del puerto e identificar los paquetes descartados. La página de seguimiento de los puertos también incluye los perfiles de conmutación asociados al puerto de conmutador lógico.


Resultados

Si observa paquetes descartados debido a la congestión de la red, puede configurar un perfil de conmutación de calidad de servicio para el puerto de conmutador lógico con el fin de evitar que se pierdan datos en los paquetes preferidos. Consulte [Información sobre el perfil de conmutación de QoS](#).

Conmutadores lógicos

13

Puede configurar los conmutadores lógicos y los objetos relacionados desde la pestaña **Opciones avanzadas de redes y seguridad**. Un conmutador lógico reproduce la funcionalidad de conmutación y el tráfico de multidifusión (BUM), unidifusión desconocida y difusión en un entorno virtual independiente del hardware subyacente.

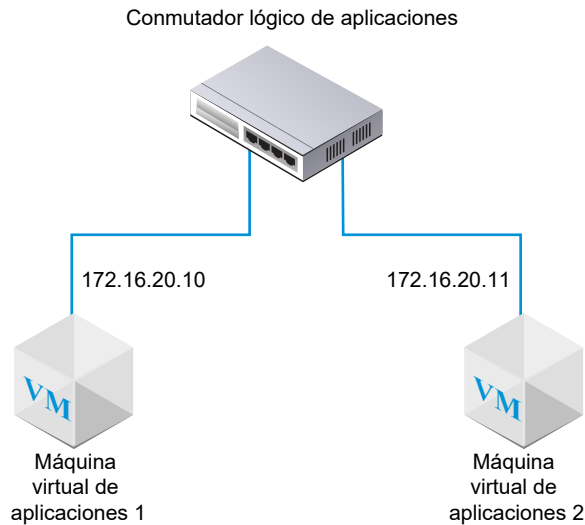
Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Los conmutadores lógicos son similares a las VLAN en cuanto a que proporcionan conexiones de red a las que se pueden conectar máquinas virtuales. De este modo, las máquinas virtuales pueden comunicarse entre ellas mediante túneles entre hipervisores si están conectadas al mismo conmutador lógico. Cada conmutador lógico tiene un identificador de red virtual (VNI), como un ID de VLAN. A diferencia de VLAN, los VNI se escalan bien más allá de los límites de los ID de VLAN.

Para ver y editar el grupo de VNI de valores, inicie sesión en NSX Manager, desplácese hasta **Tejido > Perfiles** y haga clic en la pestaña **Configuración**. Si el grupo es demasiado pequeño, tenga en cuenta que se producirá un error al crear un conmutador lógico cuando todos los valores VNI estén en uso. Si elimina un conmutador lógico, el valor VNI se volverá a utilizar, pero solo después de 6 horas.

Al agregar conmutadores lógicos, es importante que planifique la topología que crea.

Figura 13-1. Topología del conmutador lógico



Por ejemplo, la topología anterior muestra un único conmutador lógico conectado a dos máquinas virtuales. Las dos máquinas virtuales pueden estar en hosts diferentes o en el mismo host, en clústeres de hosts diferentes o en el mismo clúster de hosts. Como las máquinas virtuales del ejemplo están en la misma red virtual, las direcciones IP subyacentes configuradas en las máquinas virtuales deben estar en la misma subred.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

Este capítulo incluye los siguientes temas:

- [Información sobre los modos de replicación del marco BUM](#)
- [Crear un conmutador lógico](#)
- [Conectar una VM a un conmutador lógico](#)
- [Crear un puerto de conmutador lógico](#)
- [Probar la conectividad de Capa 2](#)
- [Crear un conmutador lógico VLAN para el vínculo superior de NSX Edge](#)
- [Perfiles de conmutación para conmutadores lógicos y puertos lógicos](#)
- [Pila de red mejorada](#)
- [Puente de Capa 2](#)

Información sobre los modos de replicación del marco BUM

Cada nodo de transporte del host es un endpoint de túnel. Cada endpoint de túnel tiene una dirección IP. Estas direcciones IP pueden encontrarse en la misma subred o en diferentes

subredes en función de la configuración de los grupos de direcciones IP o de DHCP para los nodos de transporte.

Cuando dos máquinas virtuales de hosts diferentes se comunican directamente, el tráfico encapsulado de unidifusión se intercambia entre las dos direcciones IP del endpoint de túnel asociadas a los dos hipervisores sin utilizar la inundación.

Sin embargo, al igual que con cualquier red de Capa 2, a veces el tráfico que origina una máquina virtual necesita inundarse, lo que significa que necesita enviarse al resto de las máquinas virtuales que pertenecen al mismo conmutador lógico. Esto sucede con el tráfico de multidifusión, de unidifusión desconocida y de difusión de Capa 2 (tráfico BUM). Recuerde que un único conmutador lógico de NSX-T Data Center puede abarcar varios hipervisores. El tráfico BUM que origina una máquina virtual de un determinado hipervisor necesita replicarse en los hipervisores remotos que alojan otras máquinas virtuales que están conectadas al mismo conmutador lógico. Para habilitar esta inundación, NSX-T Data Center admite dos modos de replicación diferentes:

- Segundo nivel jerárquico (en ocasiones denominado MTEP)
- Encabezado (en ocasiones denominado origen)

El modo de replicación del segundo nivel jerárquico queda ilustrado en el siguiente ejemplo. Imaginemos que tiene un host A, que cuenta con dos máquinas virtuales conectadas a los identificadores de red virtual (virtual network identifier, VNI) 5.000, 5.001 y 5.002. Imagine que los VNI son similares a las VLAN, pero cada conmutador lógico tiene un único VNI asociado a él. Por esta razón, los términos VNI y el conmutador lógico se suelen utilizar indistintamente. Cuando decimos que un host se encuentra en un VNI, queremos decir que tiene máquinas virtuales que están conectadas a un conmutador lógico con ese VNI.

Una tabla de endpoints de túnel muestra las conexiones entre el VNI y el host. El host A examina la tabla de endpoints de túnel del VNI 5.000 y determina las direcciones IP de endpoints de túneles de los otros hosts del VNI 5.000.

Algunas de estas conexiones de VNI se encontrarán en la misma subred IP, también denominado segmento de IP, como el endpoint de túnel del host A. Para cada una de ellas, el host A creará una copia independiente de cada marco BUM y enviará la copia directamente a cada host.

Otros endpoints de túneles de los hosts se encuentran en diferentes subredes o segmentos de IP. Para cada segmento en el que haya varios endpoints de túneles, el host A propone uno de estos endpoints para que sea el replicador.

El replicador recibe del host A una copia de cada marco BUM del VNI 5.000. Esta copia se marca como Replicar localmente en el encabezado de encapsulación. El host A no envía copias a otros hosts del mismo segmento de IP como el replicador. El replicador deberá crear una copia del marco BUM para cada host que sabe que está en el VNI 5.000 y en el mismo segmento de IP como ese host del replicador.

El proceso se replica para el VNI 5.001 y 5.002. Es posible que la lista de endpoints de túneles y los replicadores resultantes sean distintos para otros VNI.

Con la replicación de encabezado (también conocida como replicación de cabecera), no hay ningún replicador. El host A simplemente crea una copia de cada marco BUM para cada endpoint de túnel que sabe que está en el VNI 5.000 y lo envía.

Si todos los endpoints de túneles del host están en la misma subred, la opción del modo de replicación no será distinta porque el comportamiento no será diferente. Si los endpoints de túneles del host están en diferentes subredes, la replicación del segundo nivel jerárquico ayudará a distribuir la carga entre varios hosts. El segundo nivel jerárquico es el modo predeterminado.

Crear un conmutador lógico

Los conmutadores lógicos se asocian a una o varias máquinas virtuales en la red. Las máquinas virtuales conectadas a un conmutador lógico pueden comunicarse entre sí con los túneles entre los hipervisores.

Requisitos previos

- Compruebe que esté configurada una zona de transporte. Consulte la *Guía de instalación de NSX-T Data Center*.
- Compruebe que los nodos de tejido estén conectados correctamente al agente de plano de gestión (MPA) de NSX-T Data Center y al plano de control local (LCP) de NSX-T Data Center.

En la llamada de API `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`, el valor de `state` debe ser `success`. Consulte la *Guía de instalación de NSX-T Data Center*.

- Compruebe que los nodos de transporte se agregaron a la zona de transporte. Consulte la *Guía de instalación de NSX-T Data Center*.
- Compruebe que los hipervisores se agregaron al tejido de NSX-T Data Center y que las máquinas virtuales estén alojadas en dichos hipervisores.
- Familiarícese con los conceptos de replicación del marco BUM y la topología del conmutador lógico. Consulte [Capítulo 13 Conmutadores lógicos](#) y [Información sobre los modos de replicación del marco BUM](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Conmutadores > Agregar**.
- 3 Escriba un nombre para el conmutador lógico y, opcionalmente, una descripción.
- 4 Seleccione una zona de transporte para el conmutador lógico.

Las máquinas virtuales asociadas a los conmutadores lógicos que se encuentren en la misma zona de transporte pueden comunicarse entre sí.

- 5 Escriba el nombre de una directiva de formación de equipos de vínculo superior.
- 6 Establezca la opción **Estado de administración** como **Activo** o **Inactivo**.
- 7 Seleccione un modo de replicación para el conmutador lógico.

El modo de replicación (de encabezado o segundo nivel jerárquico) es necesario para los conmutadores lógicos de superposición, pero no para los conmutadores lógicos basados en VLAN.

Modo de replicación	Descripción
Segundo nivel jerárquico	El replicador es un host que realiza una replicación del tráfico BUM a otros hosts con el mismo VNI. Cada host propone un endpoint de túnel de host en cada VNI para que sea el replicador. Este proceso se realiza para cada VNI.
HEAD	Los hosts crean una copia de cada marco BUM y la envían a cada endpoint de túnel que conoce de cada VNI.

- 8 (opcional) Especifique un identificador de VLAN o rangos de identificadores de VLAN para el etiquetado de VLAN.

Para admitir el etiquetado de VLAN invitado en las máquinas virtuales conectadas a este conmutador, debe especificar los rangos de identificadores de VLAN, también denominados rangos de identificadores de VLAN de tronco. El puerto lógico filtrará los paquetes según los rangos de identificadores de VLAN de tronco, y una máquina virtual invitada podrá etiquetar sus paquetes con su propio identificador de VLAN en función de los rangos de identificadores de VLAN de tronco.

- 9 (opcional) Haga clic en la pestaña **Perfiles de conmutación** y seleccione perfiles de conmutación.

- 10 Haga clic en **Guardar**.

En la interfaz de usuario de NSX Manager, el conmutador lógico nuevo es un vínculo en el que se puede hacer clic.

Pasos siguientes

Asocie máquinas virtuales al conmutador lógico. Consulte [Conectar una VM a un conmutador lógico](#).

Conectar una VM a un conmutador lógico

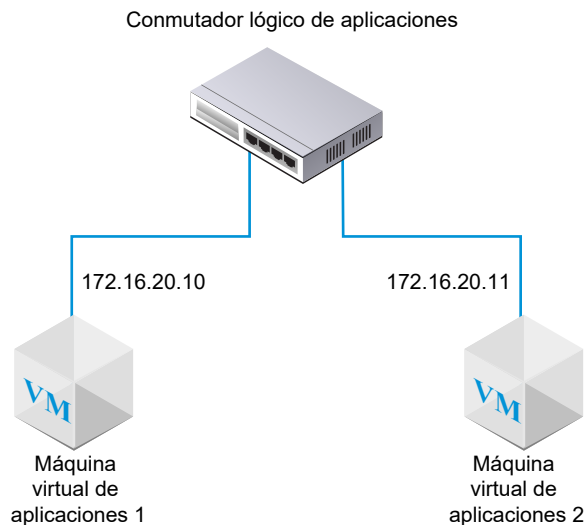
Dependiendo de su host, la configuración para conectar una VM a un conmutador lógico puede variar.

Los hosts compatibles que se pueden conectar a un conmutador lógico son: un host ESXi que se administra en vCenter Server, un host ESXi independiente y un host de KVM.

Adjuntar una máquina virtual alojada en vCenter Server a un conmutador lógico NSX-T Data Center

Si posee un host ESXi administrado en vCenter Server, puede acceder al host de las máquinas virtuales mediante el servicio vSphere Web Client basado en web. En este caso, puede utilizar este procedimiento para adjuntar VM a conmutadores lógicos de NSX-T Data Center.

El ejemplo mostrado en este procedimiento indica cómo adjuntar una VM denominada app-vm a un conmutador lógico denominado app-switch.



La aplicación vSphere Client basada en la instalación no es compatible con la conexión de una máquina virtual a un conmutador lógico NSX-T Data Center. Si no posee vSphere Web Client (basado en web), consulte [Adjuntar una VM alojada en ESXi independiente a un conmutador lógico de NSX-T Data Center](#).

Requisitos previos

- Las máquinas virtuales deben alojarse en hipervisores añadidos al tejido NSX-T Data Center.
- Los nodos del tejido deben tener conectividad del plano de administración (MPA) de NSX-T Data Center y del plano de control (LCP) de NSX-T Data Center.
- Los nodos de tejido deben agregarse a una zona de transporte.
- Se debe crear un conmutador lógico.

Procedimiento

- 1 En vSphere Web Client, edite la configuración de la máquina virtual y adjúntela al conmutador lógico NSX-T Data Center.

Por ejemplo:

1-vm_ubuntu_1404_srv_64-local-645-bfd95df0-ea28-4408-ae9a-2561750b0674: editar config...

Hardware virtual | Opciones de máquina virtual | Reglas de SDRS | Opciones de vApp

CPU	1	
Memoria	1024	MB
Disco duro 1	16	GB
Controladora SCSI 0	LSI Logic Parallel	
*Adaptador de red 1	LS. ONE (nsx.LogicalSwitch)	<input checked="" type="checkbox"/> Conectado
Adaptador de red 2	lswitch301 (nsx.LogicalSwitch)	<input checked="" type="checkbox"/> Conectado
Tarjeta de vídeo	Especificar configuración personalizada	
Dispositivo VMCI		

2 Haga clic en **Aceptar**.

Resultados

Tras adjuntar la máquina virtual al conmutador lógico, los puertos de conmutador lógicos se agregan al conmutador lógico. Puede ver los puertos de conmutador lógico y el identificador de la asociación VIF de NSX Manager en **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos**.

Utilice la llamada de API GET <https://<mgr-ip>/api/v1/logical-ports/> para ver los detalles del puerto y el estado del administrador del identificador de asociación VIF correspondiente. Para ver el estado operativo, utilice la llamada de API <https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status> con el identificador de puerto lógico adecuado.

Si hay dos VM conectadas al mismo conmutador lógico y tienen direcciones IP configuradas en la misma subred, deberían ser capaces de hacerse ping entre sí.

Pasos siguientes

Agregue un enrutador lógico.

Puede supervisar la actividad en el puerto del conmutador lógico para solucionar problemas. Consulte "Supervisar la actividad de un puerto del conmutador lógico" en *Guía de administración de NSX-T Data Center*.

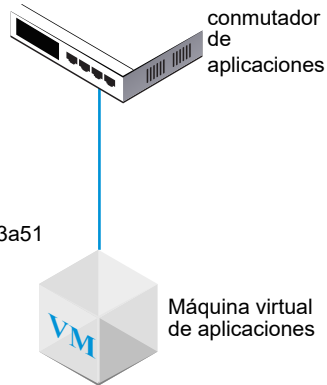
Adjuntar una VM alojada en ESXi independiente a un conmutador lógico de NSX-T Data Center

Si tiene un host ESXi independiente, no puede acceder a las VM del host mediante el vSphere Web Client basado en la web. En este caso, puede utilizar este procedimiento para adjuntar VM a conmutadores lógicos de NSX-T Data Center.

El ejemplo mostrado en este procedimiento indica cómo adjuntar una VM denominada app-vm a un conmutador lógico denominado app-switch.

ID de la red opaca del conmutador:
22b22448-38bc-419b-bea8-b51126bec7ad

ID externo de la máquina virtual:
50066bae-0f8a-386b-e62e-b0b9c6013a51



Requisitos previos

- La VM debe alojarse en hipervisores que se agregaran al tejido de NSX-T Data Center.
- Los nodos del tejido deben tener conectividad del plano de administración (MPA) de NSX-T Data Center y del plano de control (LCP) de NSX-T Data Center.
- Los nodos de tejido deben agregarse a una zona de transporte.
- Se debe crear un conmutador lógico.
- Debe tener acceso a la API de NSX Manager.
- Debe tener acceso de escritura al archivo VMX de la VM.

Procedimiento

- 1 Mediante el uso de la aplicación (basada en instalación) vSphere Client o alguna otra herramienta de administración de VM, edite la VM y agregue un adaptador Ethernet VMXNET 3.

Seleccione cualquier red con nombre. En un paso posterior cambiará la conexión de red.

Personalizar hardware

Permite configurar el hardware de la máquina virtual.

The screenshot shows the 'Personalizar hardware' window in vSphere Client. The 'Hardware virtual' tab is active. The configuration list includes:

- CPU:** 1
- Memoria:** 2048 MB
- Nuevo disco duro:** 16 GB
- Nueva controladora SCSI:** VMware Paravirtual
- *Nueva red:** VM Network (selected), VMXNET 3 (adapter type), ☒ Conectar al encender, Automático (MAC address).
- Nueva unidad de CD/DVD:** Dispositivo cliente, ☐ Conectar...
- Nueva unidad de disquete:** Dispositivo cliente, ☐ Conectar...

At the bottom, the 'Nuevo dispositivo:' section shows a dropdown menu with 'Red' selected and an 'Agregar' button.

- 2 Utilice la API NSX-T Data Center para emitir la llamada API GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>`.

En los resultados, localice el `externalId` de la VM.

Por ejemplo:

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735

{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    {
      "instanceUuid": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
      "moIdOnHost": 5,
      "externalId": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
      "hostLocalId": 5,
      "locationId": "564dc020-1565-e3f4-f591-ee3953eef3ff",
      "biosUuid": "4206f47d-fef7-08c5-5bf7-ea26a4c6b18d"
    }
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
}
```



```
"type": "REGULAR",
"host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
"local_id_on_host": "5"
}
```

3 Apague y elimine del registro la VM del host.

Puede utilizar su herramienta de administración de VM o la CLI de ESXi, tal como se muestra aquí.

```
[user@host:~] vim-cmd /vmtoolsd/getallvms
Vmid    Name      File           Guest OS      Version  Annotation
5       app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest  vmx-08
8       web-vm    [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08

[user@host:~] vim-cmd /vmtoolsd/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmtoolsd/unregister 5
```

4 Desde la IU de NSX Manager, obtenga el ID del conmutador lógico.

Por ejemplo:

app-switch

Información General
Supervisar
Administrar
Relacionado

Resumen
EDITAR

Nombre	app-switch
Identificador	b68e7ac3-877a-420e-af47-53e974c17915
Ubicación	
Descripción	lswitch202 (created through automation)
Estado de administración	● Activo
Modo de replicación	Replicación de encabezado
VLAN	N/C
VNI	71681
Puertos lógicos	1
Tipo de tráfico	Superpuesta
Zona de transporte	transportzone1
Nombre de directiva de forma...	[Use Default]
Modo de N-VDS	STANDARD
Fecha de creación	9/10/2018, 12:20:46 PM por admin
Ultima actualización	9/26/2018, 2:01:14 PM por admin

5 Modifique el archivo VMX de la VM.

Elimine el campo **ethernet1.networkName = "<name>"** y agregue los siguientes campos:

- ethernet1.opaqueNetwork.id = "<logical switch's ID>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<VM's externalId>"
- ethernet1.connected = "TRUE"
- ethernet1.startConnected = "TRUE"

Por ejemplo:

ANTIGUO

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
```

```
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
```

NUEVO

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"
```

- 6 En la IU de NSX Manager, agregue un puerto de conmutador lógico y utilice el externalId de la VM para la conexión de VIF.
- 7 Vuelva a registrar la VM y encienda el sistema.

Puede utilizar su herramienta de administración de VM o la CLI de ESXi, tal como se muestra aquí.

```
[user@host:~] vim-cmd /solo/register /path/to/file.vmx

For example:
[user@host:~] vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx
9

[user@host:~] vim-cmd /vmsvc/power.on 9
Powering on VM:
```

Resultados

En la interfaz de usuario de NSX Manager, en **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos**, busque el identificador de conexión de VIF que coincide con el externalId de la máquina virtual y asegúrese de que el estado de administrador y operativo aparezca como activo/activo.

Si hay dos VM conectadas al mismo conmutador lógico y tienen direcciones IP configuradas en la misma subred, deberían ser capaces de hacerse ping entre sí.

Pasos siguientes

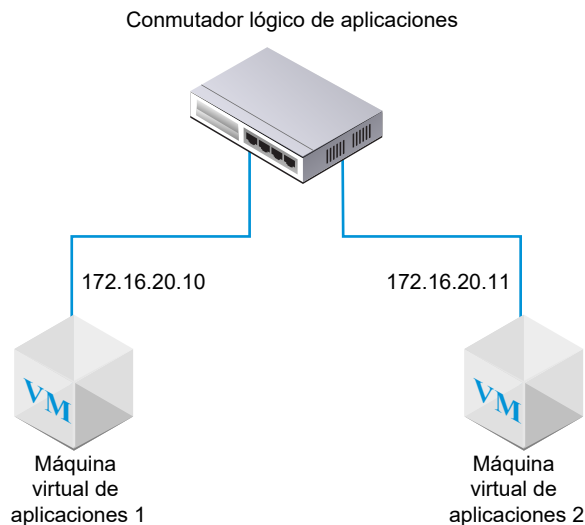
Agregue un enrutador lógico.

Puede supervisar la actividad en el puerto del conmutador lógico para solucionar problemas. Consulte "Supervisar la actividad de un puerto del conmutador lógico" en *Guía de administración de NSX-T Data Center*.

Adjuntar una máquina virtual alojada en KVM a un conmutador lógico NSX-T Data Center

Si posee un host KVM, puede utilizar este procedimiento para adjuntar máquinas virtuales a conmutadores lógicos NSX-T Data Center.

El ejemplo mostrado en este procedimiento indica cómo adjuntar una VM denominada app-vm a un conmutador lógico denominado app-switch.



Requisitos previos

- La VM debe alojarse en hipervisores que se agregaran al tejido de NSX-T Data Center.
- Los nodos del tejido deben tener conectividad del plano de administración (MPA) de NSX-T Data Center y del plano de control (LCP) de NSX-T Data Center.
- Los nodos de tejido deben agregarse a una zona de transporte.
- Se debe crear un conmutador lógico.

Procedimiento

- 1 Del CLI KVM, ejecute el comando `virsh dumpxml <your vm> | grep interfaceid`.
- 2 En la interfaz de usuario de NSX Manager, agregue un puerto de conmutador lógico y utilice el ID de interfaz de las máquinas virtuales para el VIF adjunto.

Resultados

En la interfaz de usuario de NSX Manager, en **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos**, busque el identificador de la asociación VIF y asegúrese de que el estado de administración y el estado operativo aparezcan como activo/activo.

Si hay dos VM conectadas al mismo conmutador lógico y tienen direcciones IP configuradas en la misma subred, deberían ser capaces de hacerse ping entre sí.

Pasos siguientes

Agregue un enrutador lógico.

Puede supervisar la actividad en el puerto del conmutador lógico para solucionar problemas. Consulte "Supervisar la actividad de un puerto del conmutador lógico" en *Guía de administración de NSX-T Data Center*.

Crear un puerto de conmutador lógico

Un conmutador lógico tiene varios puertos de conmutador. Un puerto de conmutador lógico conecta otro componente de red, una máquina virtual o un contenedor a un conmutador lógico.

Si conecta una máquina virtual a un conmutador lógico en un host de ESXi administrado por vCenter Server, se creará automáticamente un puerto de conmutador lógico. Para obtener más información sobre cómo conectar una máquina virtual a un conmutador lógico, consulte [Conectar una VM a un conmutador lógico](#).

Para obtener más información sobre cómo conectar un contenedor a un conmutador lógico, consulte la *Guía de instalación y administración de NSX-T Container Plug-in para Kubernetes*.

Nota NSX Manager asigna la dirección IP y la dirección MAC enlazadas a un puerto de conmutador lógico para un contenedor. No cambie el enlace de direcciones de forma manual.

Para supervisar la actividad de un puerto de conmutador lógico, consulte [Supervisar la actividad de un puerto del conmutador lógico](#).

Requisitos previos

Compruebe que se creó un conmutador lógico. Consulte [Capítulo 13 Conmutadores lógicos](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos > Agregar**.
- 3 En la pestaña **General**, complete los detalles del puerto.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y, si lo desea, una descripción.
Conmutador lógico	Seleccione un conmutador lógico del menú desplegable.
Estado de administración	Seleccione Activo o Inactivo .

Opción	Descripción
Tipo de archivo adjunto	Seleccione Ninguno o VIF .
ID del archivo adjunto	Si el tipo de archivo adjunto es VIF, introduzca el ID de este archivo.

Con la API, puede establecer el tipo de archivo adjunto en valores adicionales (LOGICALROUTER, BRIDGEENDPOINT, DHCP_SERVICE, METADATA_PROXY, L2VPN_SESSION). Si el tipo de archivo adjunto es servicio DHCP, proxy de metadatos o sesión VPN de capa 2, los perfiles de conmutación del puerto deberán ser los predeterminados. No puede usar ningún perfil definido por el usuario.

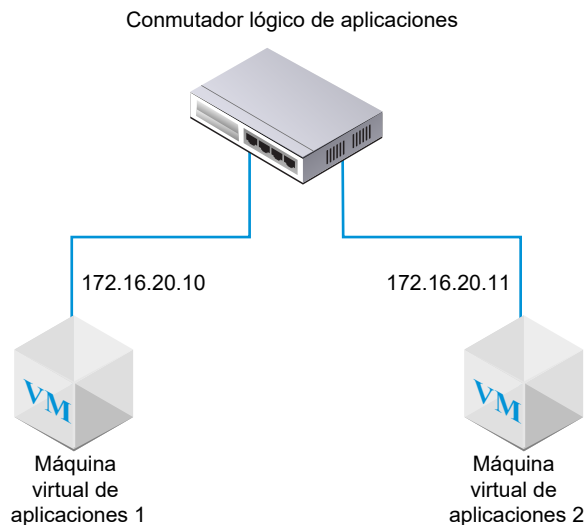
- 4 (opcional) En la pestaña **Perfiles de conmutación**, seleccione perfiles de conmutación.
- 5 Haga clic en **Guardar**.

Probar la conectividad de Capa 2

Después de configurar correctamente el conmutador lógico y asociar las máquinas virtuales a dicho conmutador, puede probar la conectividad de red de las máquinas virtuales asociadas.

Si el entorno de red está configurado correctamente, la máquina virtual de aplicaciones 2 puede hacer ping a la máquina virtual de aplicaciones 1 según la topología.

Figura 13-2. Topología del conmutador lógico



Procedimiento

- 1 Inicie sesión en una de las máquinas virtuales asociadas al conmutador lógico con la consola de la máquina virtual o SSH.

Por ejemplo, la máquina virtual de aplicaciones 2 172.16.20.11.

- 2 Haga ping a la segunda máquina virtual asociada al conmutador lógico para probar la conectividad.

```
$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
```

- 3 (opcional) Identifique el problema que provoca que se produzcan errores al hacer ping.
 - a Compruebe que la configuración de red de la máquina virtual sea correcta.
 - b Compruebe que el adaptador de red de la máquina virtual esté conectado al conmutador lógico correcto.
 - c Compruebe que el estado Administración del conmutador lógico sea ACTIVO.
 - d En NSX Manager, seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Conmutadores**.

- e Haga clic en el conmutador lógico y anote la información de VNI y UUID.
- f Ejecute los siguientes comandos para solucionar el problema.

Comando	Descripción
<code>get logical-switch <vni-or-uuid> arp-table</code>	<p>Muestra la tabla ARP del conmutador lógico especificado.</p> <p>Resultados de muestra</p> <pre>nsx-manager1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
<code>get logical-switch <vni-or-uuid> connection-table</code>	<p>Muestra las conexiones del conmutador lógico especificado.</p> <p>Resultados de muestra</p> <pre>nsx-manager1> get logical-switch 41866 connection-table Host-IP Port ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre>
<code>get logical-switch <vni-or-uuid> mac-table</code>	<p>Muestra la tabla de direcciones MAC del conmutador lógico especificado.</p> <p>Resultados de muestra</p> <pre>nsx-manager1> get logical-switch 41866 mac-table VNI MAC VTEP-IP Connection-ID 41866 00:50:56:86:f2:b2 192.168.250.102 295421 41866 00:50:56:b1:70:5e 192.168.250.101 295422</pre>
<code>get logical-switch <vni-or-uuid> stats</code>	<p>Muestra la información estadística del conmutador lógico especificado.</p> <p>Resultados de muestra</p> <pre>nsx-manager1> get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre>
<code>get logical-switch <vni-or-uuid> stats-sample</code>	<p>Muestra un resumen de todas las estadísticas del conmutador lógico a lo largo del tiempo.</p> <p>Resultados de muestra</p> <pre>nsx-manager1> get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre>

Comando	Descripción
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
get logical-switch <vni-or-uuid> vtep	<p>Muestra todos los endpoints de túneles virtuales relacionados con el conmutador lógico especificado.</p> <p>Resultados de muestra</p> <pre>nsx-manager1> get logical-switch 41866 vtep VNI IP LABEL Segment MAC Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c:28 295422</pre>

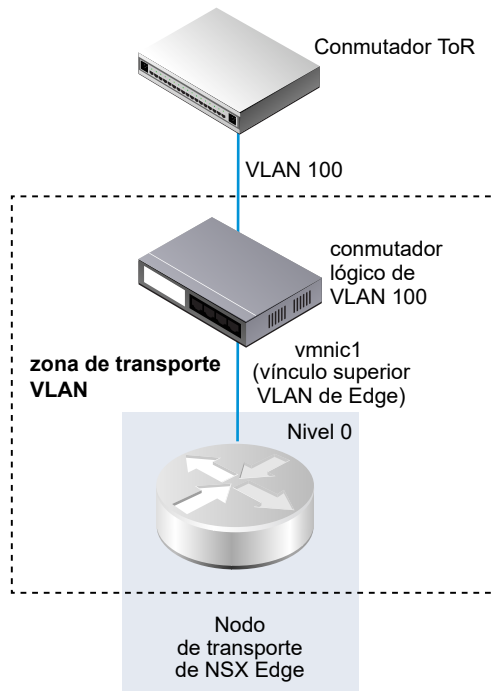
Resultados

La primera máquina virtual asociada al conmutador lógico puede enviar paquetes a la segunda máquina virtual.

Crear un conmutador lógico VLAN para el vínculo superior de NSX Edge

Los vínculos de carga de Edge pasan por los conmutadores lógicos VLAN.

Al crear un conmutador lógico VLAN, es importante elegir una topología en particular para el diseño. Por ejemplo, la siguiente topología sencilla muestra un único conmutador lógico VLAN dentro de una zona de transporte VLAN. El conmutador lógico VLAN tiene el ID de VLAN 100. Esto coincide con el ID de VLAN del puerto TOR conectado al puerto de host de hipervisor que se utiliza para el vínculo superior VLAN de Edge.



Requisitos previos

- Para crear un conmutador lógico VLAN, primero debe crear una zona de transporte VLAN.
- Se debe agregar un vSwitch de NSX-T Data Center a NSX Edge. Para confirmar un Edge, ejecute el comando `get host-switches`. Por ejemplo:

```
nsx-edge1> get host-switches

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name     : hs1
Transport Zone   : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone   : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port    : fp-eth0
Uplink Name     : uplink-1
Transport VLAN   : 4096
Default Gateway  : 192.168.150.1
Subnet Mask      : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP    : 192.168.150.102
```

- Compruebe que los nodos de tejido estén conectados correctamente al agente de plano de gestión (MPA) de NSX-T Data Center y al plano de control local (LCP) de NSX-T Data Center.

En la llamada de API `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`, el valor de `state` debe ser `success`. Consulte la *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 Desde un explorador, inicie sesión en un NSX Manager en `https://<nsx-mgr>`.

- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Conmutadores > Agregar**.
- 3 Escriba un nombre para el conmutador lógico.
- 4 Seleccione una zona de transporte para el conmutador lógico.
- 5 Seleccione una directiva de formación de equipos de vínculo superior.
- 6 Para el estado de administración, seleccione **Activo** o **Inactivo**.
- 7 Escriba un ID de VLAN.

Introduzca el valor 0 en el campo de VLAN si no hay ningún ID de VLAN para el vínculo superior al TOR físico.
- 8 (opcional) Haga clic en la pestaña **Perfiles de conmutación** y seleccione perfiles de conmutación.

Resultados

Nota Si cuenta con dos conmutadores lógicos VLAN que tienen el mismo identificador de VLAN, estos no se podrán conectar al mismo N-VDS de Edge (anteriormente conocido como conmutador de host). Si cuenta con un conmutador lógico VLAN y un conmutador lógico de superposición, y el identificador de VLAN del conmutador lógico VLAN es igual al identificador de VLAN de transporte del conmutador lógico de superposición, tampoco se podrán conectar al mismo N-VDS de Edge.

Pasos siguientes

Agregue un enrutador lógico.

Perfiles de conmutación para conmutadores lógicos y puertos lógicos

Los perfiles de conmutación incluyen detalles de configuración de redes de Capa 2 para conmutadores lógicos y puertos lógicos. NSX Manager es compatible con varios tipos de perfiles de conmutación y mantiene uno o varios perfiles de conmutación predeterminados definidos por el sistema para cada tipo de perfil.

Los siguientes tipos de perfiles de conmutación están disponibles.

- Calidad del servicio (Quality of Service, QoS)
- Reflejo del puerto
- Detección de IP
- SpoofGuard
- Seguridad de conmutadores

■ Administración de MAC

Nota No puede editar ni eliminar los perfiles de conmutación predeterminados en NSX Manager. En su lugar, puede crear perfiles de conmutación predeterminados.

Antes de usar un perfil predeterminado, asegúrese de que la configuración sea la que necesita. Al crear un perfil personalizado, algunos ajustes tienen valores predeterminados. No asuma que esta configuración tendrá los valores predeterminados en el perfil predeterminado.

Cada perfil de conmutación predeterminado o personalizado tiene un identificador reservado único. Este identificador se utiliza para asociar el perfil de conmutación a un conmutador lógico o a un puerto lógico. Por ejemplo, el identificador de perfil de conmutación de calidad de servicio predeterminado es f313290b-eba8-4262-bd93-fab5026e9495.

Un conmutador lógico o puerto lógico puede asociarse a un perfil de conmutación de cada tipo. No puede tener, por ejemplo, dos perfiles de conmutación diferentes de calidad de servicio asociados a un conmutador lógico o puerto lógico.

Si no asocia un tipo de perfil de conmutación al crear o actualizar un conmutador lógico, NSX Manager asocia un correspondiente perfil de conmutación definido por el sistema predeterminado. Los puertos lógicos secundarios heredan el perfil de conmutación definido por el sistema predeterminado del conmutador lógico principal.

Cuando crea o actualiza un conmutador lógico o puerto lógico puede elegir asociar un perfil de conmutación predeterminado o uno personalizado. Cuando el perfil de conmutación se asocia o disocia de un conmutador lógico, se aplica el perfil de conmutación para puertos lógicos secundarios basándose en los siguientes criterios.

- Si el conmutador lógico principal tiene un perfil asociado a él, el puerto lógico secundario hereda el perfil de conmutación del principal.
- Si el conmutador lógico principal no tiene un perfil de conmutación asociado a él, el perfil de conmutación predeterminado se asigna al conmutador lógico y el puerto lógico hereda dicho perfil de conmutación predeterminado.
- Si asocia explícitamente un perfil personalizado a un puerto lógico, este perfil personalizado anula el perfil de conmutación existente.

Nota Si asoció un perfil de conmutación personalizado a un conmutador lógico, pero quiere conservar el perfil de conmutación predeterminado para uno de los puertos lógicos secundarios, debe realizar una copia del perfil de conmutación predeterminado y asociarlo al puerto lógico específico.

No puede eliminar un perfil de conmutación personalizado si está asociado a un conmutador lógico o a un puerto lógico. Puede averiguar si hay asociado algún conmutador lógico o puerto lógico al perfil de conmutación personalizado accediendo a la sección Asignado a de la vista Resumen y haciendo clic en los conmutadores y puertos lógicos enumerados.

Información sobre el perfil de conmutación de QoS

QoS proporciona un rendimiento de red dedicado y de gran calidad para el tráfico preferido que necesita un gran ancho de banda. Para ello, el mecanismo de QoS prioriza ancho de banda suficiente, controla la latencia y la vibración, y disminuye la pérdida de datos de los paquetes preferidos incluso cuando se produce una congestión de red. Este nivel del servicio de red se proporciona mediante los recursos de red existentes de manera eficiente.

Esta versión permite moldear y marcar el tráfico específicamente, así como admite CoS y DSCP. La clase de servicio (CoS) de Capa 2 le permite especificar la prioridad de los paquetes de datos cuando el tráfico se almacena en búfer en el conmutador lógico por una congestión. El punto de código de servicios diferenciados (DSCP) de Capa 3 detecta los paquetes en función de sus valores DSCP. CoS siempre se aplica al paquete de datos independientemente del modo de confianza.

NSX-T Data Center confía en la configuración DSCP aplicada por una máquina virtual o en la modificación y configuración del valor DSCP en el nivel del conmutador lógico. En cada caso, el valor DSCP se propaga al encabezado de IP externo de los marcos encapsulados. Esto permite que la red física externa priorice el tráfico en función de la configuración DSCP del encabezado externo. Cuando DSCP está en el modo de confianza, el valor DSCP se copia del encabezado interno. En este modo, el valor DSCP no se conserva para el encabezado interno.

Nota La configuración DSCP solo funciona en el tráfico de túnel. Esta configuración no se aplica al tráfico del mismo hipervisor.

Puede utilizar el perfil de conmutación de QoS para configurar los valores del ancho de banda de entrada y de salida para establecer la frecuencia del límite de transmisión. La frecuencia del pico de ancho de banda se utiliza para soportar el tráfico de ráfaga que un conmutador lógico tiene permitido para evitar la congestión en los vínculos de red ascendente. Esta configuración no garantiza el ancho de banda, pero permite limitar el uso del ancho de banda de la red. El ancho de banda real que observará se determina en función de la velocidad de vínculo del puerto o de los valores en el perfil de conmutación, el valor que sea menor.

La configuración del perfil de conmutación de QoS se aplica al conmutador lógico y el puerto de conmutador lógico secundario la hereda.

Configurar un perfil de conmutación de calidad de servicio personalizado

Puede definir el valor DSCP y configurar las opciones de entrada y salida para crear un perfil de conmutación de calidad de servicio personalizado.

Requisitos previos

- Familiarícese con el concepto de perfil de conmutación de calidad de servicio. Consulte [Información sobre el perfil de conmutación de QoS](#).
- Identifique el tráfico de red que desea priorizar.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccionar **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Perfiles de conmutación > Agregar**
- 3 Seleccione **Calidad de servicio** y complete los detalles del perfil de conmutación de calidad de servicio.

Opción	Descripción
Nombre y descripción	<p>Asigne un nombre al perfil de conmutación de calidad de servicio personalizado.</p> <p>Opcionalmente, puede describir la opción de configuración que modificó en el perfil.</p>
Modo	<p>Seleccione la opción de Modo De confianza o No de confianza en el menú desplegable.</p> <p>Si selecciona el modo Confianza, el valor DSCP del encabezado interno se aplica al encabezado de IP externa en el tráfico IP/IPv6. Para tráfico que no sea IP/IPv6, el encabezado de IP externa toma el valor predeterminado. El modo Confianza no es compatible con un puerto lógico basado en superposiciones. El valor predeterminado es 0.</p> <p>El modo no de confianza no es compatible con puertos lógicos basados en superposiciones o VLAN. Para un puerto lógico basado en superposiciones, el valor DSCP del encabezado IP saliente se establece con el valor configurado al margen del tipo de paquete interno para el puerto lógico. Para el puerto lógico basado en VLAN, el valor DSCP del paquete IP/IPv6 se establece con el valor configurado. El rango de valores DSCP para el modo no de confianza se encuentra entre 0 y 63.</p> <p>Nota La configuración DSCP solo funciona en el tráfico de túnel. Esta configuración no se aplica al tráfico del mismo hipervisor.</p>
Prioridad	<p>Establezca el valor de DSCP.</p> <p>Los valores de prioridad oscilan entre 0 y 63.</p>
Clase de servicio	<p>Establezca el valor de la clase de servicio.</p> <p>La clase de servicio es compatible con puertos lógicos basados en VLAN. La clase de servicio agrupa tipos similares de tráfico en la red y cada tipo de tráfico se trata como una clase con su propio nivel de prioridad de servicio. El tráfico con menor prioridad se ralentiza o, en algunos casos, se descarta para proporcionar mejor rendimiento al tráfico con mayor prioridad. La clase de servicio también puede configurarse para el ID de VLAN con paquete cero.</p> <p>El rango de valores de clase de servicio se encuentra entre 0 y 7, siendo 0 el servicio de mejor esfuerzo.</p>

Opción	Descripción
Entrada	<p>Establezca valores personalizados para el tráfico de red saliente de la máquina virtual a la red lógica.</p> <p>Puede utilizar el ancho medio de banda para reducir la congestión de red. El valor máximo de ancho de banda se utiliza para soportar tráfico a ráfagas, y el tamaño de las ráfagas se basa en la duración con el ancho de banda máximo. La duración de la ráfaga se establece en la opción Tamaño de ráfaga. No se puede garantizar el ancho de banda. Sin embargo, puede configurar los valores de tamaño medio, máximo y de ráfaga para limitar el ancho de banda de red.</p> <p>Por ejemplo, si el ancho de banda medio es de 30 Mbps, el ancho de banda máximo es de 60 Mbps y la duración permitida es 0,1 segundos, el tamaño de ráfaga será $60 * 1000000 * 0,10/8 = 750000$ bytes.</p> <p>El valor predeterminado 0 deshabilita el límite del tráfico de entrada.</p>
Difusión de entrada	<p>Establezca valores personalizados para el tráfico de red saliente de la máquina virtual a la red lógica en base a la difusión.</p> <p>Establezca valores personalizados para el tráfico de red saliente de la máquina virtual a la red lógica en base a la difusión. Por ejemplo, si establece el ancho de banda medio de un conmutador lógico en 3000 Kbps, el ancho de banda máximo es 6000 Kbps y la duración permitida es 0,1 segundos, el tamaño de ráfaga será $6000 * 1000 * 0,10/8 = 75000$ bytes.</p> <p>El valor predeterminado 0 deshabilita el límite del tráfico de difusión de entrada.</p>
Saliente	<p>Establezca valores personalizados para el tráfico de red entrante de la red lógica a la máquina virtual.</p> <p>El valor predeterminado 0 deshabilita el límite del tráfico de salida.</p>

Si no están configuradas las opciones de entrada, difusión de entrada y salida, los valores predeterminados se utilizan.

4 Haga clic en **Guardar**.

Resultados

El perfil de conmutación de calidad de servicio personalizado aparece como un vínculo.

Pasos siguientes

Asocie el perfil personalizado de conmutación de calidad de servicio a un conmutador lógico o a un puerto lógico para que los parámetros modificados en el perfil de conmutación se apliquen al tráfico de red. Consulte [Asociar un perfil personalizado a un conmutador lógico](#) o [Asociar un perfil personalizado a un puerto lógico](#).

Información sobre el perfil de conmutación de creación de reflejo del puerto

La creación de reflejo del puerto lógico le permite replicar y redireccionar todo el tráfico entrante y saliente de un puerto de conmutador lógico asociado a un puerto VIF de la máquina virtual. El tráfico reflejado se envía encapsulado dentro de un túnel de encapsulación de enrutamiento

genérico (GRE) a un recopilador para que toda la información del paquete original se conserve mientras atraviesa la red hacia un destino remoto.

Le recomendamos que utilice la creación de reflejo del puerto solo para solucionar problemas.

Nota No se recomienda la creación de reflejo del puerto para la supervisión, ya que si se utiliza durante períodos más largos, el rendimiento se vería afectado.

En comparación con la creación de reflejo del puerto físico, la creación de reflejo del puerto lógico garantiza la captura de todo el tráfico de red de la máquina virtual. Si solo implementa la creación de reflejo del puerto en la red física, alguna parte del tráfico de red de la máquina virtual no podrá reflejarse. Esto sucede porque la comunicación entre la máquina virtual situada en el mismo host nunca entra a la red física y, por tanto, no se refleja. La creación de reflejo del puerto lógico le permite seguir reflejando el tráfico de la máquina virtual incluso cuando esa máquina virtual se migre a otro host.

El proceso de creación de reflejo del puerto es similar para ambos puertos de la máquina virtual en los puertos y el dominio de NSX-T Data Center de las aplicaciones físicas. Puede reenviar el tráfico que captura una carga de trabajo conectada a una red lógica y reflejar ese tráfico a un recopilador. Se debe poder acceder a la dirección IP desde la dirección IP de invitado en la que esté alojada la máquina virtual. Este proceso también se aplica a las aplicaciones físicas conectadas a los nodos de puerta de enlace.

Configurar un perfil personalizado de conmutación de creación de reflejo del puerto

Es posible crear un perfil personalizado de conmutación de creación de reflejo del puerto con un destino y valor de clave distintos.

Requisitos previos

- Familiarícese con el concepto de perfil de conmutación de creación de reflejo del puerto. Consulte [Información sobre el perfil de conmutación de creación de reflejo del puerto](#).
- Identifique la dirección IP del ID del puerto lógico de destino al que desea redirigir el tráfico de red.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccionar **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Perfiles de conmutación > Agregar**

- 3 Seleccione **Reflejo del puerto** y complete los detalles del perfil de conmutación de reflejos del puerto.

Opción	Descripción
Nombre y descripción	<p>Asigna un nombre al perfil personalizado de conmutación de creación de reflejo del puerto.</p> <p>Opcionalmente, puede describir la opción de configuración que modificó para personalizar el perfil.</p>
Dirección	<p>Seleccione una opción en el menú desplegable para utilizar dicho origen para tráfico de Entrada, Salida o Bidireccional.</p> <p>Entrada corresponde al tráfico de red saliente de la máquina virtual a la red lógica.</p> <p>Salida corresponde al tráfico de red entrante de la red lógica a la máquina virtual.</p> <p>Bidireccional corresponde al tráfico bidireccional de la máquina virtual a la red lógica y viceversa. Esta es la opción predeterminada.</p>
Truncamiento de paquete	Opcional. El rango es 60 - 65.535.
Clave	<p>Introduzca un valor aleatorio de 32 bits para identificar los paquetes reflejados del puerto lógico.</p> <p>Este valor se copia al campo de la clave en el encabezado GRE de cada paquete reflejado. Si el valor es 0, la definición predeterminada se copia al campo de la clave en el encabezado GRE.</p> <p>El valor predeterminado de 32 bits está compuesto por los siguientes valores.</p> <ul style="list-style-type: none"> ■ El primer valor de 24 bits es un valor VNI. VNI es parte del encabezado IP de los marcos encapsulados. ■ El bit número 25 indica si el primer valor de 24 bits es un valor VNI válido. Uno representa un valor válido y cero representa un valor no válido. ■ El bit número 26 indica la dirección del tráfico reflejado. Uno representa una dirección de entrada y cero una dirección de salida. ■ Los seis bits restantes no se utilizan.
Destinos	<p>Introduzca el ID de destino del recopilador de la sesión reflejada.</p> <p>El ID de la dirección IP de destino solo puede ser una dirección IPv4 dentro de la red o una dirección IPv4 remota que NSX-T Data Center no administre. Puede agregar hasta tres direcciones IP de destino separadas por comas.</p>

- 4 Haga clic en **Guardar**.

Resultados

Un perfil personalizado de conmutación de creación de reflejo del puerto aparece como un vínculo.

Pasos siguientes

Asocie el perfil de conmutación a un conmutador lógico o a un puerto lógico. Consulte [Asociar un perfil personalizado a un conmutador lógico](#) o [Asociar un perfil personalizado a un puerto lógico](#).

Compruebe que el perfil personalizado de conmutación de creación de reflejo del puerto funciona. Consulte [Comprobar el perfil personalizado de conmutación de creación de reflejo del puerto](#).

Comprobar el perfil personalizado de conmutación de creación de reflejo del puerto

Antes de empezar a utilizar el perfil personalizado de conmutación de creación de reflejo del puerto, compruebe que la personalización funcione correctamente.

Requisitos previos

- Compruebe que el perfil personalizado de conmutación de creación de reflejo del puerto esté configurado. Consulte [Configurar un perfil personalizado de conmutación de creación de reflejo del puerto](#).
- Compruebe que el perfil personalizado de conmutación de creación de reflejo del puerto esté asociado a un conmutador lógico. Consulte [Asociar un perfil personalizado a un conmutador lógico](#).

Procedimiento

- 1 Localice las dos máquinas virtuales con una VIF adjunta al puerto lógico configurado para crear el reflejo del puerto.

Por ejemplo, la máquina virtual 1 10.70.1.1 y la máquina virtual 2 10.70.1.2 incluyen VIF adjuntas y están situadas en la misma red lógica.

- 2 Ejecute el comando `tcpdump` en una dirección IP de destino.

```
sudo tcpdump -n -i eth0 dst host destination_IP_address and proto gre
```

Por ejemplo, la dirección IP de destino es 10.24.123.196.

- 3 Inicie sesión en la primera máquina virtual y haga ping a la segunda para comprobar que las respuestas y solicitudes eco correspondientes se reciban en la dirección de destino.

Pasos siguientes

Asocie este perfil personalizado de conmutación de creación de reflejo del puerto a un conmutador lógico para que los parámetros modificados del perfil de conmutación se apliquen al tráfico de red. Consulte [Asociar un perfil personalizado a un conmutador lógico](#).

Información sobre el perfil de conmutación de detección de direcciones IP

La detección de IP utiliza la intromisión de DHCP y DHCPv6, la intromisión de protocolo de resolución de direcciones (Address Resolution Protocol, ARP), la intromisión de detección de vecinos (Neighbor Discovery, ND) y VM Tools para aprender las direcciones IP y MAC.

Las direcciones MAC e IP detectadas se utilizan para conseguir la supresión de ARP/ND, lo que minimiza el tráfico entre las máquinas virtuales conectadas al mismo conmutador lógico. Las direcciones también las utilizan SpoofGuard y los componentes de firewall distribuido (DFW). DFW utiliza los enlaces de direcciones para determinar la dirección IP de los objetos en las reglas de firewall.

La intromisión de DHCP/DHCPv6 inspecciona los paquetes de DHCP/DHCPv6 que se intercambian entre el servidor y el cliente de DHCP/DHCPv6 para aprender las direcciones IP y MAC.

La intromisión de ARP inspecciona los paquetes de ARP y de ARP innecesario (Gratuitous ARP, GARP) salientes de una máquina virtual para aprender las direcciones IP y MAC.

VM Tools es el software que se ejecuta en las máquinas virtuales alojadas en ESXi y que puede proporcionar información de configuración de las máquinas virtuales, como las direcciones MAC, IP o IPv6. Este método de detección de direcciones IP está disponible para máquinas virtuales que se ejecutan solo en hosts ESXi.

La intromisión de ND es el equivalente IPv6 de la intromisión de ARP. Examina los mensajes de solicitud de equipos vecinos (NS) y de anuncio de equipos vecinos (NA) para aprender las direcciones IP y MAC.

Con la detección de direcciones duplicadas se comprueba si una dirección IP recién detectada ya figura en la lista de enlaces aplicada de otro puerto. Esta comprobación se realiza para los puertos en el mismo segmento. Si se detecta una dirección duplicada, la dirección recién detectada se agrega a la lista descubierta, pero no se agrega a la lista de enlaces aplicada. Todas las direcciones IP duplicadas tienen una marca de tiempo de detección asociada. Si se quita la dirección IP que se encuentra en la lista de enlaces, ya sea porque se agrega a la lista de enlaces ignorados o porque se deshabilita la intromisión, la dirección IP duplicada con la marca de tiempo más antigua se moverá a la lista de enlaces. La información de la dirección duplicada está disponible a través de una llamada de API.

De forma predeterminada, los métodos de detección intromisión de ARP y de ND funcionan en un modo denominado Confianza desde el primer uso (Trust On First Use, TOFU). En el modo TOFU, cuando se detecta una dirección y se agrega a la lista de enlaces realizados, ese enlace permanece en la lista aplicada para siempre. TOFU se aplica a los primeros enlaces 'n' únicos <IP, MAC, VLAN> detectados mediante la intromisión ARP/ND, donde 'n' es el límite de enlace que puede configurar. Puede deshabilitar TOFU para la intromisión de ARP/ND. Los métodos seguirán funcionando en el modo de confianza en cada uso (TOEU). En el modo TOEU, cuando se detecta una dirección, se agrega a la lista de enlaces aplicados y, cuando se elimina o caduca, se elimina de la lista de enlaces aplicados. La intromisión de DHCP y VM Tools siempre funciona en el modo TOEU.

Para cada puerto, NSX Manager mantiene una lista de enlaces ignorados, que contiene las direcciones IP que no se pueden enlazar al puerto. Si accede a **Redes y seguridad > Conmutación > Puertos** y selecciona un puerto, puede agregar enlaces detectados a la lista de enlaces omitidos. También puede eliminar un enlace detectado o aplicado existente copiándolos en **Enlaces omitidos**.

Nota TOFU no es igual que SpoofGuard y no bloquea el tráfico de la misma forma. Para obtener más información, consulte [Información sobre el perfil de segmentos de Spoofguard](#).

Para las máquinas virtuales Linux, el problema de flujo de ARP puede provocar que la intromisión de ARP obtenga información incorrecta. Puede evitar el problema con un filtro ARP. Para obtener más información, consulte <http://linux-ip.net/html/ether-arp.html#ether-arp-flux>.

Configurar perfiles de conmutación de detección de IP

NSX-T Data Center tiene varios perfiles de conmutación de detección de IP predeterminados. También puede crear otros perfiles adicionales.

Requisitos previos

Familiarícese con los conceptos del perfil de conmutación de detección de IP. Consulte [Información sobre el perfil de conmutación de detección de direcciones IP](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Perfiles de conmutación > Agregar**.
- 3 Seleccione **Detección de IP** y especifique los detalles del perfil de conmutación de detección de IP.

Opción	Descripción
Nombre y descripción	Introduzca un nombre y, si lo desea, una descripción.
Intromisión de ARP	Para un entorno IPv4. Aplica si las máquinas virtuales tienen direcciones IP estáticas.
Límite de enlace de ARP	El número máximo de direcciones IP IPv4 que se pueden enlazar a un puerto. El mínimo permitido es 1 (el valor predeterminado) y el máximo es 256.
Tiempo de espera del límite de enlace de ND de ARP	El valor de tiempo de espera, en minutos, para direcciones IP en la tabla de enlace de ARP/ND si TOFU está deshabilitado. Si se agota el tiempo de espera de una dirección, la reemplazará una nueva dirección detectada.
Intromisión de DHCP	Para un entorno IPv4. Aplica si las máquinas virtuales tienen direcciones IPv4.
Intromisión de DHCP V6	Para un entorno IPv6. Aplica si las máquinas virtuales tienen direcciones IPv6.
VM Tools	Disponible solo para las máquinas virtuales alojadas en ESXi.

Opción	Descripción
VM Tools para IPv6	Disponible solo para las máquinas virtuales alojadas en ESXi.
Intromisión de detección de vecinos	Para un entorno IPv6. Aplica si las máquinas virtuales tienen direcciones IP estáticas.
Límite de enlace de detección de vecinos	El número máximo de direcciones IPv6 que se pueden enlazar a un puerto.
Confiar en el primer uso	Aplicable a intromisión de ND y ARP.
Detección de direcciones IP duplicadas	Para todos los métodos de intromisión y los entornos IPv4 e IPv6.

4 Haga clic en **Agregar**.

Pasos siguientes

Asocie el perfil personalizado de conmutación de detección de IP a un conmutador lógico o a un puerto lógico para que los parámetros modificados en el perfil de conmutación se apliquen al tráfico de red. Consulte [Asociar un perfil personalizado a un conmutador lógico](#) o [Asociar un perfil personalizado a un puerto lógico](#).

Información sobre SpoofGuard

SpoofGuard ayuda a evitar un ataque malicioso denominado "suplantación de páginas web" o "suplantación de identidad". Una directiva SpoofGuard bloquea el tráfico que se determina que se va a suplantar.

SpoofGuard es una herramienta diseñada para evitar que las máquinas virtuales de su entorno alteren su dirección IP actual. En el caso de que una dirección IP de la máquina virtual no coincida con la dirección IP del puerto lógico y los enlaces de direcciones del conmutador correspondientes de SpoofGuard, la vNIC de la máquina virtual no podrá acceder a la red por completo. SpoofGuard se puede configurar en el nivel del puerto o del conmutador. Hay varias razones por las que podría utilizar SpoofGuard en su entorno:

- Evitar que una máquina virtual no autorizada suplante la dirección IP de una máquina virtual existente.
- Garantizar que las direcciones IP de las máquinas virtuales no se puedan modificar sin intervención. En algunos entornos, es preferible que las máquinas virtuales no puedan modificar sus direcciones IP sin cambiar correctamente la revisión de control. Para ello, SpoofGuard garantiza que el propietario de la máquina virtual no pueda modificar la dirección IP y seguir trabajando sin impedimentos.
- Garantizar que las reglas de Distributed Firewall (DFW) no se omitan involuntariamente (o deliberadamente). En el caso de las reglas de DFW que se creen con conjuntos de direcciones IP como orígenes o destinos, siempre cabe la posibilidad de que una máquina virtual pueda tener su dirección IP falsificada en el encabezado del paquete y, por tanto, se omitan las reglas en cuestión.

La configuración de SpoofGuard de NSX-T Data Center incluye lo siguiente:

- SpoofGuard de direcciones MAC: autentica la dirección MAC del paquete.
- SpoofGuard de direcciones IP: autentica las direcciones IP y MAC del paquete.
- Inspección del protocolo de resolución de direcciones dinámicas (ARP), es decir, la validación de SpoofGuard de descubrimiento cercano (ND) y de SpoofGuard del protocolo de resolución de direcciones gratuito (GARP) y del ARP contradice la asignación del origen de direcciones IP-MAC, el origen de direcciones MAC y el origen de direcciones IP en la carga de ARP/GARP/ND.

En el nivel del puerto, la lista de MAC/VLAN/IP permitidas se proporciona a través de la propiedad de enlaces de direcciones del puerto. Cuando la máquina virtual envía tráfico, se descarta si su IP/MAC/VLAN no coincide con las propiedades de IP/MAC/VLAN del puerto. SpoofGuard del nivel del puerto se ocupa de la autenticación del tráfico (por ejemplo, la consistencia del tráfico con la configuración VIF).

En el nivel del conmutador, la lista de MAC/VLAN/IP permitidas se proporciona a través de la propiedad de enlaces de direcciones del conmutador. Suele ser una subred o un rango de IP permitidos del conmutador, mientras que el SpoofGuard del nivel del conmutador se ocupa de la autorización del tráfico.

SpoofGuard del nivel del conmutador Y del nivel del puerto deben permitir el tráfico antes de que se permita en el conmutador. Puede controlar si activa o desactiva Spoofguard del nivel del conmutador o del puerto con el perfil de conmutador de SpoofGuard.

Configurar asociaciones de direcciones de puertos

Los enlaces de direcciones especifican las direcciones IP y MAC de un puerto lógico y se utilizan para especificar la lista blanca del puerto en Spoofguard.

Los enlaces de direcciones de puertos especifican las direcciones IP y MAC, y en el caso de VLAN, del puerto lógico. Si Spoofguard está habilitado, se garantiza que los enlaces de direcciones determinados se apliquen en la ruta de datos. Además de Spoofguard, los enlaces de direcciones de puertos se utilizan para la traducción de reglas DFW.

Procedimiento

- 1 En NSX Manager, seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos**.
- 2 Haga clic en el puerto lógico al que desea aplicar el enlace de direcciones.
Aparece el resumen del puerto lógico.
- 3 En la pestaña **Información general**, expanda **Enlaces de direcciones > Enlaces manuales**.
- 4 Haga clic en **Agregar**.

El cuadro de diálogo Agregar enlace de direcciones (Add Address Binding) aparece.

- 5 Especifique la dirección IP (dirección IPv4 o IPv6, o bien subred IPv6) y MAC del puerto lógico al que desea aplicar el enlace de direcciones. Por ejemplo, en IPv6, 2001::/64 es una subred IPv6 y 2001::1 es una dirección IP de host, mientras que 2001::1/64 no es una entrada válida. También puede especificar un identificador de VLAN.

- 6 Haga clic en **Agregar**.

Pasos siguientes

Utilice los enlaces de direcciones de puertos cuando [Configurar un perfil de conmutación de Spoofguard](#).

Configurar un perfil de conmutación de Spoofguard

Al configurar Spoofguard, si la dirección IP de la máquina virtual cambia, el tráfico de la máquina virtual puede bloquearse hasta que los enlaces de direcciones de puerto/conmutador configurados se actualicen con la nueva dirección IP.

Habilite Spoofguard para los grupos de puertos que incluyan invitados. Si se habilita en cada adaptador de red, Spoofguard inspecciona los paquetes para la dirección MAC preestablecida y su correspondiente dirección IP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Perfiles de conmutación > Agregar**.
- 3 Seleccione **Spoofguard**.
- 4 Introduzca un nombre y, si lo desea, una descripción.
- 5 Para habilitar el nivel del puerto Spoofguard, establezca **Enlaces de puertos** en **Habilitado**.
- 6 Haga clic en **Agregar**.

Resultados

Se crea un nuevo perfil de conmutación con un perfil Spoofguard.

Pasos siguientes

Asocie el perfil de Spoofguard a un conmutador lógico o un puerto lógico. Consulte [Asociar un perfil personalizado a un conmutador lógico](#) o [Asociar un perfil personalizado a un puerto lógico](#).

Información sobre el perfil de conmutación de seguridad del conmutador

La seguridad del conmutador ofrece seguridad de Capa 2 y de Capa 3 sin estado. Para ello, comprueba el tráfico de entrada al conmutador lógico y descarta los paquetes no autorizados que se envían desde máquinas virtuales comparando la dirección IP, la dirección MAC y los

protocolos con un conjunto de direcciones y protocolos permitidos. Puede utilizar la seguridad del conmutador para proteger la integridad del conmutador lógico mediante el filtrado de los ataques maliciosos de la máquina virtual de la red.

Puede configurar el filtro Unidad de datos de protocolo de puente (BDPU), la búsqueda DHCP, el bloqueo de servidores DHCP y las opciones de limitación de frecuencia para personalizar el perfil de conmutación de seguridad del conmutador en un conmutador lógico.

Configurar un perfil de conmutación de seguridad del conmutador personalizado

Es posible crear un perfil de conmutación de seguridad del conmutador personalizado con direcciones MAC de destino de la lista permitida BPDU y configurar el límite de frecuencia.

Requisitos previos

Familiarícese con el concepto de perfil de conmutación de seguridad del conmutador. Consulte [Información sobre el perfil de conmutación de seguridad del conmutador](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación**.
- 3 Haga clic en la pestaña **Perfiles de conmutación**.
- 4 Haga clic en **Agregar** y seleccione **Seguridad de conmutadores**.
- 5 Complete los detalles del perfil de conmutación de seguridad del conmutador.

Opción	Descripción
Nombre y descripción	Asigne un nombre al perfil de seguridad del conmutador personalizado. Opcionalmente, puede describir la opción de configuración que modificó en el perfil.
Filtro de BPDU	Alterne el botón Filtro BPDU para habilitar el filtro BPDU. Deshabilitado de forma predeterminada. Al habilitar el filtro BPDU, todo el tráfico a la dirección MAC de destino BPDU se bloquea. El filtro BPDU habilitado también deshabilita STP en los puertos de conmutadores lógicos, ya que dichos puertos no deberían formar parte de STP.
Lista de permitidos de filtro de BPDU	Haga clic en la dirección MAC de destino de la lista de direcciones MAC de destino BPDU para permitir el tráfico al destino seleccionado. Debe habilitar el Filtro de BPDU para poder seleccionar un elemento de esta lista.
Filtro de DHCP	Alterne el botón Bloqueo de servidores y Bloqueo de clientes para habilitar el filtro DHCP. Ambas opciones están deshabilitadas de forma predeterminada. La opción Bloqueo de servidores bloquea el tráfico de un servidor DHCP a un cliente DHCP. Tenga en cuenta que esto no bloquea el tráfico de un servidor DHCP a un agente de retransmisión DHCP. La opción Bloqueo de clientes de DHCP evita que una máquina virtual adquiera una dirección IP de DHCP bloqueando las solicitudes de DHCP.

Opción	Descripción
Filtro DHCPv6	<p>Alterne el botón Bloquear servidor V6 y Bloquear cliente V6 para habilitar el filtro DHCP. Ambas opciones están deshabilitadas de forma predeterminada.</p> <p>La opción Bloquear servidor DHCPv6 bloquea el tráfico que procede de un servidor DHCPv6 y se dirige a un cliente DHCPv6. Tenga en cuenta que esto no bloquea el tráfico de un servidor DHCP a un agente de retransmisión DHCP. Se filtran los paquetes cuyo número de puerto UDP de origen es 547.</p> <p>La opción Bloquear cliente DHCPv6 evita que una máquina virtual adquiera una dirección IP de DHCP al bloquear las solicitudes de DHCP. Se filtran los paquetes cuyo número de puerto UDP de origen es 546.</p>
Bloquear tráfico que no usa IP	<p>Alterne el botón Bloquear tráfico que no usa IP para permitir solo el tráfico de IPv4, IPv6, ARP y BPDU.</p> <p>Se bloqueará el resto de tráfico que no use IP. El tráfico IPv4, IPv6, ARP, GARP y BPDU permitido se basa en otro conjunto de directivas de la configuración de los enlaces de dirección y Spoofguard.</p> <p>De forma predeterminada, esta opción se deshabilita para permitir que el tráfico que no usa IP se gestione como tráfico estándar.</p>
Protección de RA	<p>Alterne el botón Protección de RA para filtrar los anuncios de entrada del enrutador IPv6. Se filtran los 134 paquetes del tipo ICMPv6. Esta opción está habilitada de forma predeterminada.</p>
Límites de velocidad	<p>Establezca un límite de transmisión para el tráfico de difusión y multidifusión. Esta opción está habilitada de forma predeterminada.</p> <p>Los límites de transmisión se pueden utilizar para proteger el conmutador lógico o las máquinas virtuales de eventos como las tormentas de difusión.</p> <p>Para evitar problemas de conectividad, el valor mínimo de límite de frecuencia debe ser ≥ 10 pps.</p>

6 Haga clic en **Agregar**.

Resultados

Un perfil de seguridad del conmutador personalizado aparece como un vínculo.

Pasos siguientes

Asocie el perfil personalizado de conmutación de seguridad del conmutador a un conmutador lógico o a un puerto lógico para que los parámetros modificados en el perfil de conmutación se apliquen al tráfico de red. Consulte [Asociar un perfil personalizado a un conmutador lógico](#) o [Asociar un perfil personalizado a un puerto lógico](#).

Información sobre el perfil de conmutación de gestión de direcciones MAC

El perfil de conmutación de gestión de direcciones MAC admite dos funciones: el cambio de direcciones MAC y el aprendizaje de estas direcciones.

La función para cambiar de dirección MAC permite que una máquina virtual cambie su dirección MAC. Una máquina virtual conectada a un puerto puede ejecutar un comando administrativo para cambiar la dirección MAC de su vNIC y seguir enviando y recibiendo el tráfico en dicha vNIC. Esta función solo es compatible con ESXi y no con KVM. Esta propiedad estará deshabilitada de forma predeterminada, excepto cuando la máquina virtual invitada se implementa mediante VMware Integrated OpenStack, en cuyo caso la propiedad estará habilitada de forma predeterminada.

El aprendizaje de direcciones MAC proporciona conectividad de red a las implementaciones en las que varias direcciones MAC están configuradas detrás de una vNIC, por ejemplo, en una implementación de hipervisor anidado en el que una máquina virtual ESXi se ejecuta en un host ESXi y varias máquinas virtuales se ejecutan dentro de la máquina virtual ESXi. Sin el aprendizaje de direcciones MAC, cuando la vNIC de la máquina virtual ESXi se conecta a un puerto del conmutador, su dirección MAC es estática. Las máquinas virtuales que se ejecutan dentro de la máquina virtual ESXi no tienen conectividad de red debido a que sus paquetes tienen distintas direcciones MAC de origen. Con el aprendizaje de direcciones MAC, el vSwitch inspecciona la dirección MAC de origen de cada paquete que provenga de la vNIC, aprende la dirección MAC y permite la transmisión del paquete. Si una dirección MAC aprendida no se usa durante un periodo de tiempo, esta se eliminará. Esta propiedad de caducidad no se puede configurar.

El aprendizaje de direcciones MAC también admite la inundación de unidifusión desconocida. Normalmente, cuando un puerto recibe un paquete con una dirección MAC de destino desconocido, el paquete se descarta. Cuando el desbordamiento de unidifusión desconocida está habilitado, el puerto envía el tráfico de unidifusión desconocida a cada puerto del conmutador que tenga habilitadas las opciones de desbordamiento de unidifusión desconocida y de aprendizaje de direcciones MAC. Esta propiedad está habilitada de forma predeterminada, pero solo si el aprendizaje de direcciones MAC está habilitado.

El número de direcciones MAC que se pueden aprender se puede configurar. El valor máximo es 4096, que es el valor predeterminado. También puede establecer la directiva para cuando se alcance el límite. Las opciones son:

- **Anular:** Se descartan los paquetes de direcciones MAC de origen desconocido. Los paquetes entrantes dirigidos a esta dirección MAC se tratarán como unidifusión desconocida. El puerto recibirá los paquetes solo si tiene habilitado el desbordamiento de unidifusión desconocida.
- **Permitir:** Los paquetes procedentes de una dirección MAC de origen desconocido se reenvían, aunque no se conocerá la dirección. Los paquetes entrantes dirigidos a esta dirección MAC se tratarán como unidifusión desconocida. El puerto recibirá los paquetes solo si tiene habilitado el desbordamiento de unidifusión desconocida.

Si habilita el aprendizaje de direcciones MAC o el cambio de estas direcciones, también deberá configurar SpoofGuard para mejorar la seguridad.

Configurar el perfil de conmutación de administración de direcciones MAC

Puede crear un perfil de conmutación de administración de direcciones MAC para administrarlas.

Requisitos previos

Familiarícese con el concepto de perfil de conmutación de administración de direcciones MAC. Consulte [Información sobre el perfil de conmutación de gestión de direcciones MAC](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Perfiles de conmutación > Agregar**.
- 3 Seleccione **Administración de direcciones MAC** y complete los detalles del perfil de administración de direcciones MAC.

Opción	Descripción
Nombre y descripción	Asigne un nombre al perfil de administración de direcciones MAC. Opcionalmente, puede describir la opción de configuración que modificó en el perfil.
Cambio de dirección MAC	Habilite o deshabilite la función para cambiar de dirección MAC. Esta opción está deshabilitada de forma predeterminada.
Estado	Habilite o deshabilite la función para detectar la dirección MAC. Esta opción está deshabilitada de forma predeterminada.
Desborde de unidif. desconocido	Habilite o deshabilite la función de desbordamiento de unidifusión desconocida. Esta opción está habilitada de forma predeterminada. Esta opción está disponible si habilita el aprendizaje de direcciones MAC.
Límite de MAC	Configure el número máximo de direcciones MAC. El valor predeterminado es 4096. Esta opción está disponible si habilita el aprendizaje de direcciones MAC.
Directiva de límite de MAC	Seleccione Permitir o Anular . La opción predeterminada es Permitir . Esta opción está disponible si habilita el aprendizaje de direcciones MAC.

- 4 Haga clic en **Agregar**.

Pasos siguientes

Asocie el perfil de conmutación a un conmutador lógico o a un puerto lógico. Consulte [Asociar un perfil personalizado a un conmutador lógico](#) o [Asociar un perfil personalizado a un puerto lógico](#).

Asociar un perfil personalizado a un conmutador lógico

Puede asociar un perfil de conmutación personalizado a un conmutador lógico, de forma que el perfil se aplique a todos los puertos del conmutador.

Cuando se adjuntan perfiles de conmutación personalizados a un conmutador lógico, invalidan los perfiles de conmutación predeterminados existentes. El perfil de conmutación personalizado es heredado por puertos de conmutadores lógicos secundarios.

Nota Si asoció un perfil de conmutación personalizado a un conmutador lógico, pero quiere conservar el perfil de conmutación predeterminado para uno de los puertos de conmutadores lógicos secundarios, debe realizar una copia del perfil de conmutación predeterminado y asociarlo al puerto de conmutador lógico específico.

Requisitos previos

- Compruebe que se configuró un conmutador lógico. Consulte [Crear un conmutador lógico](#).
- Compruebe que se configuró un perfil de conmutación personalizado. Consulte [Perfiles de conmutación para conmutadores lógicos y puertos lógicos](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Conmutadores**.
- 3 Haga clic en el conmutador lógico para aplicar el perfil de conmutación personalizado.
- 4 Haga clic en la pestaña **Administrar**.
- 5 Seleccione el tipo de perfil de conmutación personalizado en el menú desplegable.
 - **Calidad de servicio**
 - **Reflejo del puerto**
 - **Detección de IP**
 - **Spoofguard**
 - **Seguridad de conmutadores**
 - **Administración de MAC**
- 6 Haga clic en **Cambiar**.
- 7 Seleccione el perfil de conmutación personalizado creado previamente en la lista desplegable.
- 8 Haga clic en **Guardar**.
El conmutador lógico queda ahora asociado al perfil de conmutación personalizado.
- 9 Compruebe que el nuevo perfil de conmutación personalizado con la configuración modificada aparezca bajo la pestaña **Administrar**.
- 10 (opcional) Haga clic en la pestaña **Relacionado** y seleccione **Puertos** en el menú desplegable para comprobar que se aplique el perfil de conmutación personalizado a puertos lógicos secundarios.

Pasos siguientes

Si no quiere utilizar el perfil de conmutación heredado desde un conmutador lógico, puede aplicar un perfil de conmutación personalizado al puerto de conmutador lógico secundario. Consulte [Asociar un perfil personalizado a un puerto lógico](#).

Asociar un perfil personalizado a un puerto lógico

Un puerto lógico proporciona un punto de conectividad lógica a un VIF, una conexión de revisión a un enrutador o una conexión de puerta de enlace de Capa 2 a una red externa. Los puertos lógicos también exponen los perfiles de conmutación, contadores de estadísticas de puertos y un estado de vínculo lógico.

Puede cambiar el perfil de conmutación heredado del conmutador lógico a otro perfil de conmutación personalizado para el puerto lógico secundario.

Requisitos previos

- Compruebe que se configuró un puerto lógico. Consulte [Conectar una VM a un conmutador lógico](#).
- Compruebe que se configuró un perfil de conmutación personalizado. Consulte [Perfiles de conmutación para conmutadores lógicos y puertos lógicos](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación > Puertos**.
- 3 Haga clic en el puerto lógico para aplicar el perfil de conmutación personalizado.
- 4 Haga clic en la pestaña **Administrar**.
- 5 Seleccione el tipo de perfil de conmutación personalizado en el menú desplegable.
 - Calidad de servicio
 - Reflejo del puerto
 - Detección de IP
 - Spoofguard
 - Seguridad de conmutadores
 - Administración de MAC
- 6 Haga clic en **Cambiar**.
- 7 Seleccione el perfil de conmutación personalizado creado previamente en la lista desplegable.
- 8 Haga clic en **Guardar**.

El puerto lógico queda ahora asociado al perfil de conmutación personalizado.

- 9 Compruebe que el nuevo perfil de conmutación personalizado con la configuración modificada aparezca bajo la pestaña **Administrar**.

Pasos siguientes

Puede supervisar la actividad en el puerto del conmutador lógico para solucionar problemas. Consulte "Supervisar la actividad de un puerto del conmutador lógico" en *Guía de administración de NSX-T Data Center*.

Pila de red mejorada

La ruta de datos mejorada es un modo de pila de red que, cuando está configurado, proporciona un rendimiento superior de red. Está dirigido principalmente a cargas de trabajo NFV, que requieren las ventajas de rendimiento que ofrece este modo.

El conmutador de N-VDS solo se puede configurar en el modo de ruta de datos mejorada en un host ESXi. ENS también admite el tráfico que fluye a través de las máquinas virtuales de Edge. En el modo de ruta de datos mejorada, puede configurar el tráfico de superposición y el tráfico de VLAN.

Asignar automáticamente núcleos lógicos de ENS

Asigne automáticamente núcleos lógicos a las vNIC para que los núcleos lógicos dedicados administren el tráfico entrante y saliente de las vNIC.

Al configurar el conmutador N-VDS en el modo Ruta de datos mejorada, si se asocia un solo núcleo lógico a una vNIC, ese núcleo lógico procesará el tráfico bidireccional entrante y saliente de una vNIC. Si se configuran varios núcleos lógicos, el host determinará automáticamente qué núcleo lógico debe procesar el tráfico de una vNIC.

Asigne núcleos lógicos a las vNIC según uno de los siguientes parámetros.

- **vNIC-Count:** el host asume que la transmisión del tráfico entrante o saliente para una dirección de las vNIC requiere la misma cantidad de recursos de CPU. A cada núcleo lógico se le asigna el mismo número de vNIC según el grupo de núcleos lógicos disponibles. Este es el modo predeterminado. El modo vNIC-count es fiable, pero no es el más adecuado para el tráfico asimétrico.
- **CPU-usage:** el host utiliza estadísticas internas para predecir el uso de CPU necesario para transmitir el tráfico entrante o saliente en cada dirección de las vNIC. Según el uso de CPU necesario, el host cambiará las asignaciones de núcleos lógicos para equilibrar la carga entre ellos. El modo CPU-usage es más adecuado que vNIC-count, pero no es fiable cuando el tráfico no es estable.

En el modo CPU-usage, si el tráfico que se transmite cambia con frecuencia, los recursos de CPU previstos requeridos y la asignación de vNIC también pueden cambiar con frecuencia. Los cambios de asignación demasiado frecuentes pueden provocar que se anulen paquetes.

Si los patrones de tráfico son simétricos entre las vNIC, la opción vNIC-count proporciona un comportamiento fiable, que es menos vulnerable a los cambios frecuentes. Sin embargo, si los patrones de tráfico son asimétricos, la opción vNIC-count puede provocar que anulen paquetes, ya que no distingue la diferencia de tráfico entre las vNIC.

En el modo vNIC-count, se recomienda configurar la cantidad adecuada de núcleos lógicos para que se asigne el mismo número de vNIC a cada núcleo lógico. Si se asigna un número de vNIC diferente a cada núcleo lógico, la asignación de CPU no será equilibrada y el rendimiento no será determinista.

Cuando una vNIC está conectada o desconectada, o cuando se agrega o se elimina un núcleo lógico, los hosts detectan automáticamente los cambios y los vuelven a equilibrar.

Procedimiento

- ◆ Para cambiar de un modo a otro, ejecute el siguiente comando:

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

Donde *<ens-lc-mode>* se puede establecer en el modo **vNIC-count** o **cpu-usage**.

vNIC-count es la asignación de núcleos lógicos según el recuento de vNIC o direcciones.

cpu-usage es la asignación de núcleos lógicos según el uso de CPU.

Configurar el enrutamiento entre VLAN invitadas

En redes superpuestas, NSX-T admite el enrutamiento del tráfico entre VLAN de un dominio de Capa 3. Durante el enrutamiento, el enrutador distribuido virtual (Virtual Distributed Router, VDR) utiliza el identificador de VLAN para enrutar paquetes entre las subredes VLAN.

En el enrutamiento entre VLAN, se pueden utilizar más de 10 vNIC por máquina virtual. Gracias a que NSX-T admite el enrutamiento entre VLAN, podrá crear en la vNIC y consumir muchas subinterfaces de VLAN para servicios de red diferentes. Por ejemplo, una vNIC de una máquina virtual puede dividirse en varias subinterfaces. Cada subinterfaz pertenece a una subred, que puede alojar un servicio de red, como SNMP o DHCP. Con el enrutamiento entre VLAN, por ejemplo, una subinterfaz en VLAN-10 puede alcanzar una subinterfaz en VLAN-10 o en cualquier otra VLAN.

Cada vNIC de una máquina virtual se conecta al N-VDS a través del puerto lógico principal, que administra paquetes sin etiquetar.

Para crear una subinterfaz, en el conmutador N-VDS mejorado, cree un puerto secundario mediante la API con una VIF asociada mediante la llamada API descrita en el procedimiento. La subinterfaz marcada con un identificador de VLAN está asociada a un nuevo conmutador lógico (por ejemplo, VLAN10 está conectado al conmutador lógico LS-VLAN-10). Todas las subinterfaces de VLAN10 tiene que estar asociadas a LS-VLAN-10. Esta asignación 1-1 entre el identificador

de VLAN de la subinterfaz y su conmutador lógico asociado constituye un requisito previo importante. Por ejemplo, si se agrega un puerto secundario con VLAN20 al conmutador lógico LS-VLAN-10 asignado a VLAN-10, el enrutamiento de paquetes entre VLAN no funcionará. Estos errores de configuración hacen que el enrutamiento entre VLAN no sea funcional.

Requisitos previos

- Antes de asociar una subinterfaz de VLAN a un conmutador lógico, asegúrese de que este no esté asociado a otra subinterfaz de VLAN. Si se produce un error de coincidencia, es posible que el enrutamiento entre VLAN en redes superpuestas no funcione.
- Asegúrese de que los hosts ejecuten ESXi 6.7 U2 o versiones posteriores.

Procedimiento

- 1 Si desea crear subinterfaces para una vNIC, asegúrese de que dicha vNIC se haya actualizado a un puerto principal. Realice la siguiente llamada REST API.

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "vif_type": "PARENT"
    },
    "id" : "<Attachment UUID of the vNIC>"
  },
  "admin_state" : "UP",
  "logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
  "_revision" : 0
}
```

- 2 Si desea crear puertos secundarios para un puerto vNIC principal en el N-VDS asociado a las subinterfaces en una máquina virtual, realice la llamada API. Antes de realizar la llamada API, compruebe que existe un conmutador lógico para conectar los puertos secundarios con las subinterfaces de la máquina virtual.

```
POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
      "traffic_tag" : <VLAN ID>,
      "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be unique.
    }
  }
}
```



```

    "vif_type" : "CHILD"
  },
  "id" : "<ID of the CHILD port>"
},

  "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
to which Child port would be connected to>",
  "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
  "admin_state" : "UP"
}

```

Resultados

NSX-T Data Center crea subinterfaces en máquinas virtuales.

Puente de Capa 2

Cuando un conmutador lógico de NSX-T Data Center requiere una conexión de Capa 2 a un grupo de puertos respaldados por VLAN o necesita llegar a otro dispositivo, como una puerta de enlace situada fuera de una implementación de NSX-T Data Center, puede utilizar un puente de Capa 2 de NSX-T Data Center. El puente de Capa 2 es especialmente útil en un escenario de migraciones, en el que necesita dividir una subred en las cargas de trabajo virtuales y físicas.

Los conceptos de NSX-T Data Center que forma parte del puente de Capa 2 son los perfiles de clústeres de Edge y de puente de Edge. Puede configurar el puente de Capa 2 mediante nodos de transporte de NSX Edge. Para usar los nodos de transporte de NSX Edge para el puente, cree un perfil de puente de Edge. Un perfil de puente de Edge especifica qué clúster de Edge se utilizará para el puente y qué nodo de transporte de Edge actuará como puente principal y de copia de seguridad.

El perfil de puente de Edge está conectado a un conmutador lógico, y la asignación especifica el vínculo superior físico en la instancia de Edge utilizada para el puente y el identificador de VLAN que se asociará al conmutador lógico. Un conmutador lógico se puede asociar a varios perfiles de puente.

Crear un perfil de puente Edge

Un perfil de puente Edge hace posible que un clúster de NSX Edge pueda proporcionar un puente de Capa 2 a un conmutador lógico.

Cuando se crea un perfil de puente de Edge, si se configura el modo de conmutación por error como preferente y se produce una conmutación por error, el nodo en espera se convierte en el nodo activo. Una vez que se recupera el nodo en el que se produjo el error, se volverá a convertir en el nodo activo. Si se configura el modo de conmutación por error como no preferente y se produce una conmutación por error, el nodo en espera se convertirá en el nodo activo. Una vez que se recupera el nodo en el que se produjo el error, se convertirá en el nodo en espera. Puede establecer manualmente el nodo de Edge en espera para que sea el nodo activo ejecutando el comando de CLI `set l2bridge-port <uuid> state active` en el nodo de Edge en espera.

El comando solo se puede aplicar en modo no preferente. De lo contrario, se producirá un error. En el modo no preferente, el comando activará una conmutación por error de HA cuando se aplique a un nodo en espera, y se omitirá cuando se aplique a un nodo activo. Para obtener más información, consulte la *Referencia de la interfaz de línea de comandos de NSX-T Data Center*.

Requisitos previos

- Compruebe que tenga un clúster de NSX Edge con dos nodos de transporte de NSX Edge.

Procedimiento

- 1 Seleccione **Sistema > Tejido > Perfiles > Perfiles de puente de Edge > Agregar**.
- 2 Escriba un nombre para el perfil de puente Edge y, opcionalmente, una descripción.
- 3 Seleccione un clúster de NSX Edge.
- 4 Seleccione un nodo principal.
- 5 Seleccione un nodo de respaldo.
- 6 Seleccione un modo de conmutación por error.

Las opciones son **Preferente** y **No preferente**.

- 7 Haga clic en el botón **Agregar**.

Pasos siguientes

Ahora puede asociar un conmutador lógico al perfil de puente.

Configurar el puente basado en Edge

Cuando se configura el puente basado en Edge, después de crear un perfil de puente de Edge para un clúster de Edge, se requieren algunas configuraciones adicionales.

Tenga en cuenta que no puede conectar un conmutador lógico con puente dos veces en el mismo nodo de Edge. Sin embargo, sí puede conectar dos VLAN al mismo conmutador lógico en dos nodos de Edge diferentes.

Hay tres opciones de configuración.

Opción 1: Configurar el modo promiscuo

- Establezca el modo promiscuo en el grupo de puertos.
- Permita la transmisión falsificada en el grupo de puertos.
- Ejecute el siguiente comando para habilitar el filtro inverso en el host ESXi en el que se ejecuta la máquina virtual de Edge:

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```

A continuación, deshabilite y habilite el modo promiscuo en la puertos siguiendo estos pasos:

- Edite la configuración del grupo de puertos.

- Deshabilite el modo promiscuo y guarde la configuración.
- Vuelva a editar la configuración del grupo de puertos.
- Habilite el modo promiscuo y guarde la configuración.
- Compruebe que no haya otros grupos de puertos en el modo promiscuo en el mismo host donde se comparte el conjunto de VLAN.
- Las máquinas virtuales de Edge activas y en espera deben estar en hosts diferentes. Si están en el mismo host, es posible que el rendimiento disminuya porque el tráfico de VLAN se debe reenviar a ambas máquinas virtuales en modo promiscuo.

Opción 2: Configurar el aprendizaje de direcciones MAC

Si la instancia de Edge se implementa en un host con NSX-T instalado, puede conectarse a un segmento o conmutador lógico de VLAN. El conmutador lógico debe tener un perfil de administración de MAC con el aprendizaje de direcciones MAC habilitado. De forma similar, el segmento debe tener un perfil de descubrimiento de MAC con el aprendizaje de direcciones MAC habilitado.

Opción 3: Configurar un puerto de recepción

- 1 Recupere el número de puerto del tronco vNIC que quiera configurar como el puerto de recepción.
 - a Inicie sesión en vSphere Web Client y acceda a **Inicio > Redes**.
 - b Haga clic en el grupo de puertos distribuidos al que está conectada la interfaz troncal de NSX Edge, y haga clic en **Puertos** para ver los puertos y las máquinas virtuales conectadas. Anote el número de puerto asociado a la interfaz troncal. Utilice este número de puerto cuando recupere y actualice datos opacos.
- 2 Recupere el valor dvsUuid para vSphere Distributed Switch.
 - a Inicie sesión en la interfaz de usuario de vCenter Mob en `https://<ip-vc>/mob`.
 - b Haga clic en **content** (contenido).
 - c Haga clic en el vínculo asociado con **rootFolder** (por ejemplo, *grupo-d1 [Centrosdedatos]*).
 - d Haga clic en el vínculo asociado con **childEntity** (por ejemplo: *centrodedatos-1*).
 - e Haga clic en el vínculo asociado con **networkFolder** (por ejemplo: *grupo-n6*).
 - f Haga clic en el vínculo del nombre de DVS para el conmutador vSphere Distributed Switch asociado con las instancias de NSX Edge (por ejemplo: *dvs-1 [Mgmt_ VDS]*).
 - g Copie el valor de la cadena uuid. Utilice este valor de dvsUuid cuando recupere y actualice datos opacos.
- 3 Compruebe si los datos opacos existen para el puerto especificado.
 - a Acceda a `https://<ip-vc> /mob/?moid=DVSManager&vmodl=1`.
 - b Haga clic en **fetchOpaqueDataEx**.

- c En el cuadro del valor **selectionSet**, pegue la siguiente entrada de XML:

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Utilice el número de puerto y el valor dvsUuid que recuperó para la interfaz troncal de NSX Edge.

- d Establezca `isRuntime` como `false`.
- e Haga clic en **Invocar método** (Invoke Method). Si el resultado muestra valores para `vim.dvs.OpaqueData.ConfigInfo`, significa que ya hay un conjunto de datos opacos, por lo que debe usar la operación `edit` cuando establezca el puerto de recepción. Si el valor de `vim.dvs.OpaqueData.ConfigInfo` está vacío, use la operación `add` cuando establezca el puerto de recepción.
- 4 Configure el puerto de recepción en el navegador de objeto administrado (MOB) de vCenter
- a Acceda a `https://<ip-vc> /mob/?moid=DVSManger&vmodl=1`.
- b Haga clic en **updateOpaqueDataEx**.
- c En el cuadro del valor **selectionSet**, pegue la siguiente entrada de XML. Por ejemplo,

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Utilice el valor dvsUuid que recuperó de vCenter MOB.

- d En el cuadro del valor `opaqueDataSpec`, pegue una de las siguientes entradas XML.

Use esta entrada para habilitar un puerto de recepción si no se configuraron los datos opacos (`operation` está establecido como `add`):

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmodl.Binary">AAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

Use esta entrada para habilitar un puerto de recepción si ya se configuraron los datos opacos (operation está establecido como edit):

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmobl.Binary">AAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    </opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

Utilice esta entrada para deshabilitar un puerto de recepción:

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmobl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    </opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

- e Establezca isRuntime como false.
- f Haga clic en **Invocar método** (Invoke Method).

Crear un conmutador lógico respaldado por puentes de Capa 2

Cuando haya máquinas virtuales conectadas a la superposición de NSX-T Data Center, podrá configurar un conmutador lógico respaldado por un puente para proporcionar conectividad de Capa 2 a otros dispositivos o máquinas virtuales que estén fuera de la implementación de NSX-T Data Center.

Requisitos previos

- Compruebe que tiene un perfil de puente de Edge.
- Al menos un host ESXi o KVM como nodo de transporte regular. Este nodo tiene máquinas virtuales alojadas que necesitan conectarse con dispositivos fuera de una implementación de NSX-T Data Center.
- Una máquina virtual u otro dispositivo final fuera de la implementación de NSX-T Data Center. Este dispositivo final se debe asociar a un puerto VLAN que coincida con el ID de VLAN del conmutador lógico respaldado por puentes.

- Un conmutador lógico en una zona de transporte de superposición como el conmutador lógico respaldado por puentes.

Procedimiento

- 1 Desde un explorador, inicie sesión en un NSX Manager en `https://<nsx-mgr>`.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación**.
- 3 Haga clic en el nombre de un conmutador de superposición (tipo de tráfico: superposición).
- 4 Haga clic en **Relacionados > Perfiles de puente de Edge**.
- 5 Haga clic en **Asociar**.
- 6 Para asociar a un perfil de puente de Edge,
 - a Seleccione un perfil de puente de Edge.
 - b Seleccione una zona de transporte.
 - c Escriba un identificador de VLAN.
 - d Haga clic en **Guardar**.
- 7 Conecte las máquinas virtuales al conmutador lógico (si aún no están conectadas).
 Las máquinas virtuales deben encontrarse en nodos de transporte de la misma zona de transporte que el perfil de puente de Edge.

Resultados

Puede probar la funcionalidad del puente. Para ello, envíe un ping desde la máquina virtual interna de NSX-T Data Center a un nodo externo a NSX-T Data Center.

Para supervisar el tráfico del conmutador de puente, haga clic en la pestaña **Supervisar**.

También puede consultar el tráfico del puente con la llamada de API GET `https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics:`


```
{
  "tx_packets": {
    "total": 134416,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "rx_bytes": {
    "total": 22164,
    "multicast_broadcast": 0
  },
  "tx_bytes": {
    "total": 8610134,
    "multicast_broadcast": 0
  },
  "rx_packets": {
    "total": 230,
```

```
    "dropped": 0,  
    "multicast_broadcast": 0  
  },  
  "last_update_timestamp": 1454979822860,  
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"  
}
```

NSX-T Data Center admite un modelo de enrutamiento de dos niveles.

En el nivel superior está el enrutador lógico de nivel 0. En dirección norte, el enrutador lógico de nivel 0 se conecta a uno o varios enrutadores físicos o conmutadores de capa 3, y funciona como una puerta de enlace a la infraestructura física. En dirección sur, el enrutador lógico de nivel 0 se conecta a uno o varios enrutadores lógicos de nivel 1 o directamente a uno o varios conmutadores lógicos.

En el nivel inferior está el enrutador lógico de nivel 1. En dirección norte, el enrutador lógico de nivel 1 se conecta a un enrutador lógico de nivel 0. En dirección sur, se conecta a uno o varios conmutadores lógicos.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Este capítulo incluye los siguientes temas:

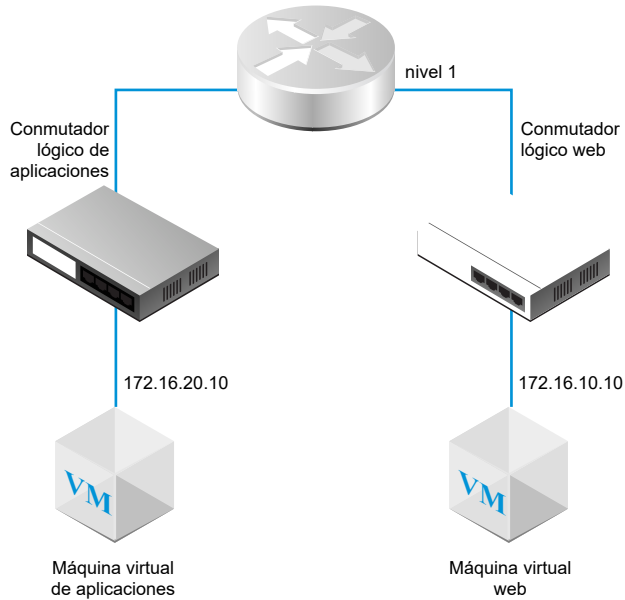
- [Enrutador lógico de nivel 1](#)
- [Enrutador lógico de nivel 0](#)

Enrutador lógico de nivel 1

Los enrutadores lógicos de nivel 1 tienen puertos de vínculo superior para conectarse a conmutadores lógicos y puertos de vínculo de descarga para conectarse a los enrutadores lógicos de nivel 0.

Al agregar un enrutador lógico, es importante que planifique la topología de red que crea.

Figura 14-1. Topología del enrutador lógico de nivel 1



Por ejemplo, esta topología sencilla muestra dos conmutadores lógicos conectados a un enrutador lógico de nivel 1. Cada conmutador lógico tiene una única máquina virtual conectada. Las dos máquinas virtuales pueden estar en hosts diferentes o en el mismo host, en clústeres de hosts diferentes o en el mismo clúster de hosts. Si un enrutador lógico no separa las máquinas virtuales, las direcciones IP subyacentes configuradas en las máquinas virtuales deben estar en la misma subred. Si un enrutador lógico las separa, las direcciones IP de las máquinas virtuales deben estar en subredes diferentes.

En algunos casos, los clientes externos envían consultas de ARP para direcciones MAC enlazadas a puertos VIP de equilibrador de carga. Sin embargo, los puertos VIP de equilibrador de carga no tienen direcciones MAC y no pueden procesar estas consultas. Se debe implementar ARP de proxy en los puertos de servicio centralizado de un enrutador lógico de nivel 1 para procesar las consultas de ARP en nombre de los puertos VIP de equilibrador de carga.

Al configurar un enrutador lógico de nivel 1 con DNAT, el firewall de Edge y el equilibrador de carga, el tráfico dirigido a otro enrutador lógico de nivel 1 y procedente de este se procesa en este orden: primero DNAT, segundo el firewall de Edge y, por último, el equilibrador de carga. El tráfico interno del enrutador lógico de nivel 1 se procesa primero a través de DNAT y, a continuación, mediante el equilibrador de carga. Se omite el procesamiento a través del firewall de Edge.

En un enrutador lógico de nivel 0 o 1, puede configurar diferentes tipos de puertos. Un tipo se denomina puerto de servicio centralizado (CSP). Debe configurar un CSP en un enrutador lógico de nivel 0 en modo activo-en espera, o bien en un enrutador lógico de nivel 1 para conectarse a un conmutador lógico respaldado por VLAN o para crear un enrutador lógico de nivel 1 independiente. Un CSP es compatible con los siguientes servicios en un enrutador lógico de nivel 0 en modo activo-en espera o en un enrutador lógico de nivel 1:

- NAT

- Equilibrio de carga
- Firewall con estado
- VPN (IPsec y L2VPN)

Crear un enrutador lógico de nivel 1

El enrutador lógico de nivel 1 debe estar conectado al enrutador lógico de nivel 0 para obtener el acceso al enrutador físico en dirección norte.

Requisitos previos

- Compruebe que se configuraron los conmutadores lógicos. Consulte [Crear un conmutador lógico](#).
- Compruebe que se implementó un clúster de NSX Edge para realizar la configuración de traducción de direcciones de red (NAT). Consulte la *Guía de instalación de NSX-T Data Center*.
- Familiarícese con la topología del enrutador lógico de nivel 1. Consulte [Enrutador lógico de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Enrutadores > Enrutadores > Agregar**.
- 3 Seleccione **Enrutador de nivel 1** y escriba un nombre para el enrutador lógico y, opcionalmente, una descripción.
- 4 (opcional) Seleccione un enrutador lógico de nivel 0 para conectarlo a este enrutador lógico de nivel 1.

Si aún no tiene configurado ningún enrutador lógico de nivel 0, puede dejar este campo en blanco de momento y editar la configuración del enrutador más adelante.

- 5 (opcional) Seleccione un clúster de NSX Edge.

Para anular la selección de un clúster seleccionado, haga clic en el icono **x**. Si se va a utilizar el enrutador lógico de nivel 1 para la configuración NAT, debe conectarse a un clúster de NSX Edge. Si aún no tiene configurado ningún clúster de NSX Edge, puede dejar este campo en blanco por el momento y editar la configuración del enrutador más adelante.

- 6 (opcional) Haga clic en el botón de alternancia **Reubicación en espera** para habilitar o deshabilitar la reubicación en espera.

La reubicación en espera significa que si se produce un error en el nodo de Edge en el que se ejecuta el enrutador lógico activo o en espera, se creará un nuevo enrutador lógico en espera en otro nodo de Edge para mantener la alta disponibilidad. Si el nodo de Edge en el que se

produce el error ejecuta el enrutador lógico activo, el enrutador lógico en espera original se convertirá en el enrutador lógico activo y se creará un nuevo enrutador lógico en espera. Si el nodo de Edge en el que se produce el error ejecuta el enrutador lógico en espera, el nuevo enrutador lógico en espera lo reemplazará.

- 7 (opcional) Si seleccionó un clúster de NSX Edge, seleccione un modo de conmutación por error.

Opción	Descripción
Preferente	Si se produce un error en el nodo preferente y se soluciona, reemplazará al nodo del mismo nivel y se convertirá en el nodo activo. El estado de este nodo cambiará a en espera. Esta es la opción predeterminada.
No preferente	Si se produce un error en el nodo preferente y se soluciona, comprobará si el nodo del mismo nivel es el activo. Si es así, el nodo preferente no reemplazará al nodo del mismo nivel y será el nodo que esté en espera.

- 8 (opcional) Haga clic en la pestaña **Avanzado** e introduzca un valor para **Subred de tránsito intranivel 1**.

- 9 Haga clic en **Agregar**.

Resultados

Después de crear el enrutador lógico, si desea quitar el clúster de Edge de la configuración del enrutador, siga estos pasos:

- Haga clic en el nombre del enrutador para ver los detalles de configuración.
- Seleccione **Servicios > Firewall de Edge**.
- Haga clic en **Deshabilitar firewall**.
- Haga clic en la pestaña **Información general** y, a continuación, en **Editar**.
- En el campo **Clúster de Edge**, haga clic en el icono **x**.
- Haga clic en **Guardar**.

Si este enrutador lógico admite más de 5.000 máquinas virtuales, debe ejecutar los siguientes comandos en cada nodo del clúster de NSX Edge para aumentar el tamaño de la tabla ARP.

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

Debe volver a ejecutar los comandos después de reiniciar dataplane o de reiniciar el nodo porque los cambios no son persistentes.

Pasos siguientes

Cree puertos de vínculo inferior para su enrutador lógico de nivel 1. Consulte [Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1](#).

Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1

Si crea un puerto de vínculo inferior en un enrutador lógico de nivel 1, el puerto funciona como una puerta de enlace predeterminada para las máquinas virtuales que se encuentren en la misma subred.

Requisitos previos

Compruebe que el enrutador lógico de nivel 1 esté configurado. Consulte [Crear un enrutador lógico de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el nombre de un enrutador.
- 4 Haga clic en la pestaña **Configuración** y seleccione **Puertos del enrutador**.
- 5 Haga clic en **Agregar**.
- 6 Escriba un nombre para el puerto de enrutador y, opcionalmente, una descripción.
- 7 En el campo **Tipo**, seleccione **Vínculo inferior**.
- 8 En **Modo URPF**, seleccione **Estricto** o **Ninguno**.
El reenvío de ruta inversa de unidifusión (Unicast Reverse Path Forwarding, URPF) es una función de seguridad.
- 9 (opcional) Seleccione un conmutador lógico.
- 10 Seleccione si desea que esta conexión cree un puerto de conmutador o actualice un puerto de conmutador existente.
Si la conexión es para un puerto de conmutador existente, seleccione el puerto en el menú desplegable.
- 11 Introduzca la dirección IP del puerto del enrutador en notación CIDR.
Por ejemplo, la dirección IP puede ser 172.16.10.1/24.
- 12 (opcional) Seleccione un servicio de retransmisión DHCP.
- 13 Haga clic en **Agregar**.

Pasos siguientes

Habilite el anuncio de enrutadores para facilitar la conectividad de Norte a Sur entre las máquinas virtuales y las redes físicas externas o entre diferentes enrutadores lógicos de nivel 1 que estén conectados al mismo enrutador lógico de nivel 0. Consulte [Configurar anuncios de rutas en un enrutador lógico de nivel 1](#).

Agregar un puerto de VLAN en un enrutador lógico de nivel 0 o de nivel 1

Si tiene solo conmutadores lógicos respaldados por VLAN, puede conectar los conmutadores a los puertos de VLAN en un enrutador de nivel 0 o de nivel 1 para que NSX-T Data Center pueda suministrar servicios de capa 3.

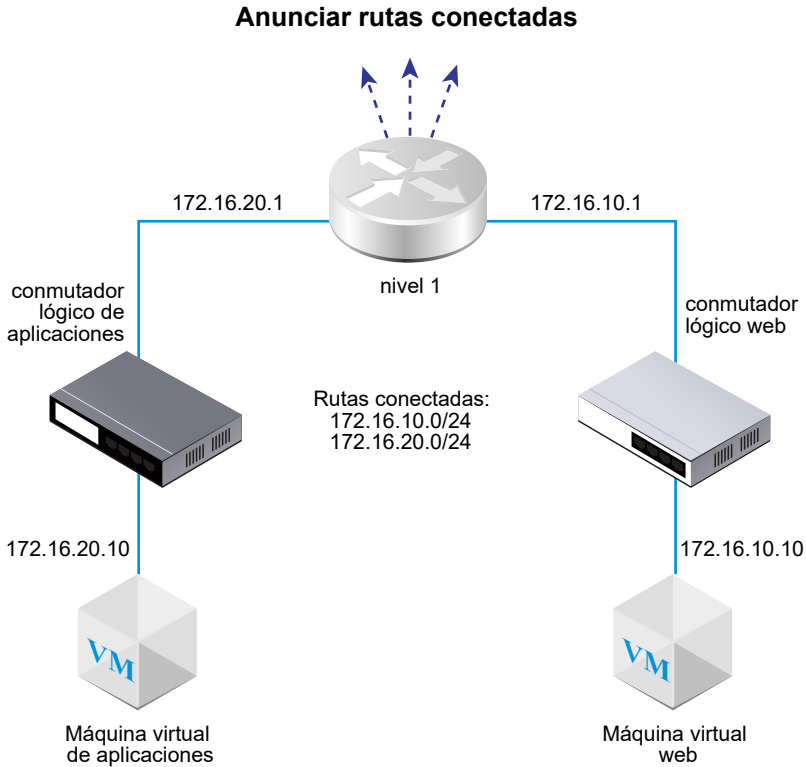
Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el nombre de un enrutador.
- 4 Haga clic en la pestaña **Configuración** y seleccione **Puertos del enrutador**.
- 5 Haga clic en **Agregar**.
- 6 Escriba un nombre para el puerto de enrutador y, opcionalmente, una descripción.
- 7 En el campo **Tipo**, seleccione **Centralizado**.
- 8 En **Modo URPF**, seleccione **Estricto** o **Ninguno**.
El reenvío de ruta inversa de unidifusión (Unicast Reverse Path Forwarding, URPF) es una función de seguridad.
- 9 (Requerido) Seleccione un conmutador lógico.
- 10 Seleccione si desea que esta conexión cree un puerto de conmutador o actualice un puerto de conmutador existente.
Si la conexión es para un puerto de conmutador existente, seleccione el puerto en el menú desplegable.
- 11 Introduzca la dirección IP del puerto del enrutador en notación CIDR.
- 12 Haga clic en **Agregar**.

Configurar anuncios de rutas en un enrutador lógico de nivel 1

Para proporcionar conectividad de Capa 3 entre máquinas virtuales conectadas a conmutadores lógicos adjuntos a otros enrutadores lógicos de nivel 1, es necesario habilitar el anuncio de rutas de nivel 1 a nivel 0. No es necesario configurar un protocolo de enrutamiento o rutas estáticas entre enrutadores lógicos de nivel 1 y 0. NSX-T Data Center crea rutas estáticas NSX-T Data Center de manera automática al habilitar el anuncio de rutas.

Por ejemplo, para proporcionar conectividad desde y hacia las máquinas virtuales a través de enrutadores emparejados, el enrutador de nivel 1 debe estar configurado con anuncios de rutas para aquellas conectadas. Si no desea anunciar todas las rutas conectadas, puede especificar cuáles desea anunciar.



Requisitos previos

- Compruebe que las máquinas virtuales estén conectadas a conmutadores lógicos. Consulte [Capítulo 13 Conmutadores lógicos](#).
- Compruebe que los puertos de vínculos inferiores para el enrutamiento lógico de nivel 1 estén configurados. Consulte [Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el nombre de un enrutador de nivel 1.
- 4 Seleccione **Anuncio de rutas** en el menú desplegable **Enrutamiento**.
- 5 Haga clic en **Editar** para editar la configuración de anuncio de rutas.

Puede activar o desactivar los siguientes conmutadores:

- **Estado**
- **Anunciar rutas conectadas de NSX**
- **Anunciar todas las rutas de NAT**
- **Anunciar todas las rutas estáticas**

- **Anunciar rutas de VIP del LB**
- **Anunciar rutas de IP de SNAT del LB**
- **Anunciar todas las rutas de reenviador de DNS**

a Haga clic en **Guardar**.

6 Haga clic en **Agregar** para anunciar las rutas.

- a Introduzca un nombre y, si lo desea, una descripción.
- b Introduzca un prefijo de ruta con el formato CIDR.
- c Haga clic en **Aplicar filtro** para configurar las opciones siguientes:

Acción	Especifique Permitir o Denegar .
Hacer coincidir tipos de ruta	Seleccione una o varias de las siguientes opciones: <ul style="list-style-type: none"> ■ Cualquiera ■ NSX conectado ■ VIP de equilibrador de carga de nivel 1 ■ Estático ■ NAT de nivel 1 ■ SNAT de equilibrador de carga de nivel 1
Operador de prefijo	Seleccione GE o EQ .

d Haga clic en **Agregar**.

Pasos siguientes

Familiarícese con la topología de enrutadores lógicos de nivel 0 y cree uno. Consulte [Enrutador lógico de nivel 0](#).

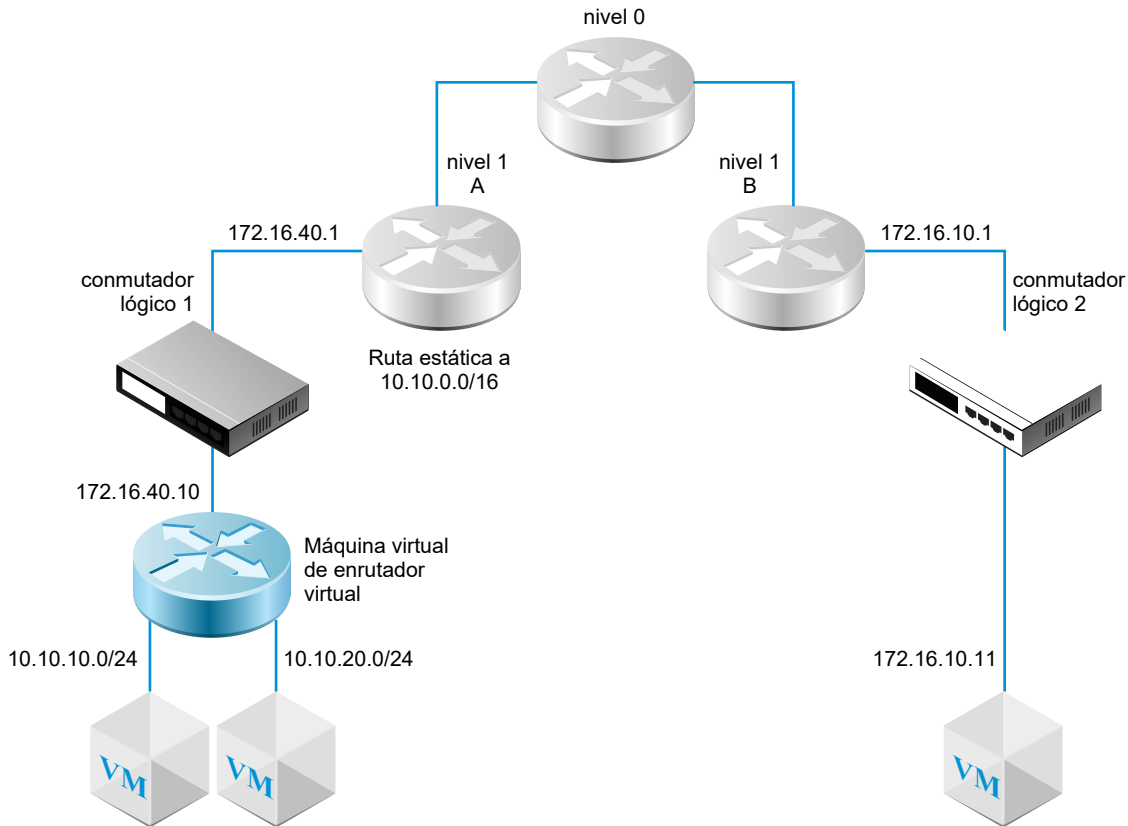
Si el enrutador lógico de nivel 0 ya está conectado al de nivel 1, compruebe que el enrutador de nivel 0 está aprendiendo las rutas conectadas del enrutador de nivel 1. Consulte [Comprobar que un enrutador de nivel 0 aprendió las rutas de un enrutador de nivel 1](#).

Configurar una ruta estática de enrutador lógico de nivel 1

Puede configurar una ruta estática en un enrutador lógico de nivel 1 para proporcionar conectividad desde NSX-T Data Center hasta un conjunto de redes a las que se puede acceder a través de un enrutador virtual.

Por ejemplo, en el siguiente diagrama, el enrutador lógico de nivel 1 A tiene un puerto de vínculo inferior a un conmutador lógico de NSX-T Data Center. Este puerto de vínculo inferior (172.16.40.1) sirve la puerta de enlace predeterminada para la VM del enrutador virtual. El enrutador virtual VM y el nivel 1 A están conectados a través del mismo conmutador lógico de NSX-T Data Center. El enrutador lógico de nivel 1 tiene una ruta estática 10.10.0.0/16 que resume las redes disponibles mediante el enrutador virtual. El nivel 1 A entonces tiene el anuncio de ruta configurado para anunciar la ruta estática al nivel 1 B.

Figura 14-2. Topología de ruta estática de enrutador lógico de nivel 1



Se admiten las rutas estáticas recursivas.

Requisitos previos

Compruebe que se configuró un puerto de vínculo inferior. Consulte [Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el nombre de un enrutador de nivel 1.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **Rutas estáticas** en el menú desplegable.
- 5 Haga clic en **Agregar**.
- 6 Introduzca una dirección de red en formato CIDR.

Se admite la ruta estática en función de IPv6. Los prefijos de IPv6 solo pueden tener un próximo salto de IPv6.

Por ejemplo, 10.10.10.0/16 o una dirección IPv6.

- 7 Haga clic en **Agregar** para agregar una dirección IP de próximo salto.

Por ejemplo, 172.16.40.10. También puede especificar una ruta nula haciendo clic en el icono de lápiz y seleccionando **NULO** en el desplegable. Para agregar otras direcciones de próximo salto, haga clic en **Agregar**.

- 8 Haga clic en **Agregar** en la parte inferior del cuadro de diálogo.

La dirección de red de la ruta estática recién creada aparece en la fila.

- 9 Desde el enrutador lógico de nivel 1, seleccione **Enrutamiento > Anuncio de ruta**.

- 10 Haga clic en **Editar** y seleccione **Anunciar todas las rutas estáticas**.

- 11 Haga clic en **Guardar**.

La ruta estática se propaga por toda la superposición de NSX-T Data Center.

Crear un enrutador lógico de nivel 1 independiente

Un enrutador lógico de nivel 1 independiente no tiene vínculos inferiores ni conexiones con un enrutador de nivel 0. Tiene un enrutador de servicio, pero no cuenta con ningún enrutador distribuido. El enrutador de servicio puede implementarse en un nodo de NSX Edge o dos nodos de NSX Edge en modo activo-en espera.

Un enrutador lógico de nivel 1 independiente:

- No debe estar conectado a un enrutador lógico de nivel 0.
- No debe tener un vínculo inferior.
- Solo puede tener un puerto de servicio centralizado (Centralized Service Port, CSP) si se usa para asociar un servicio de equilibrador de carga (Load Balancer, LB).
- Puede conectarse a un conmutador lógico superpuesto o a un conmutador lógico de VLAN.
- Admite cualquier combinación de los servicios IPSec, DNAT, firewall, equilibrador de carga e inserción de servicios. Para la entrada, el orden de procesamiento es: IPSec, DNAT, firewall, equilibrador de carga e inserción de servicios. Para la salida, el orden de procesamiento es inserción de servicio, equilibrador de carga, firewall, DNAT e IPSec.

Por lo general, un enrutador lógico de nivel 1 independiente está conectado a un conmutador lógico al que también está conectado un enrutador lógico de nivel 1 típico. El enrutador lógico de nivel 1 independiente puede comunicarse con otros dispositivos mediante el enrutador lógico de nivel 1 típico tras configurar las rutas estáticas y los anuncios de rutas.

Antes de utilizar el enrutador lógico de nivel 1 independiente, tenga en cuenta lo siguiente:

- Para especificar la puerta de enlace predeterminada para el enrutador lógico de nivel 1 independiente, debe agregar una ruta estática. La subred debe ser 0.0.0.0/0 y el próximo salto es la dirección IP de un enrutador de nivel 1 típico conectado al mismo conmutador.

- Se admite el proxy ARP en el enrutador independiente. Puede configurar una dirección IP de servidor virtual de equilibrador de carga, o bien una dirección IP de SNAT de equilibrador de carga en la subred del CSP. Por ejemplo, si la dirección IP del CSP es 1.1.1.1/24, la dirección IP virtual puede ser 1.1.1.2. También puede ser una dirección IP de otra subred, como 2.2.2.2, si se configura correctamente el enrutamiento para que el tráfico de 2.2.2.2 pueda llegar al enrutador independiente.
- Para una máquina virtual de NSX Edge, no puede tener más de una instancia de CSP conectada al mismo conmutador lógico respaldado por VLAN o diferentes conmutadores lógicos respaldados por VLAN que tengan el mismo identificador de VLAN.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Enrutadores > Enrutadores > Agregar**.
- 3 Seleccione **Enrutador de nivel 1** y escriba un nombre para el enrutador lógico y, opcionalmente, una descripción.
- 4 (Requerido) Seleccione un clúster de NSX Edge para conectarlo a este enrutador lógico de nivel 1.
- 5 (Requerido) Seleccione miembros de clúster y un modo de conmutación por error.

Opción	Descripción
Preferente	Si se produce un error en el nodo preferente y se soluciona, reemplazará al nodo del mismo nivel y se convertirá en el nodo activo. El estado de este nodo cambiará a en espera. Esta es la opción predeterminada.
No preferente	Si se produce un error en el nodo preferente y se soluciona, comprobará si el nodo del mismo nivel es el activo. Si es así, el nodo preferente no reemplazará al nodo del mismo nivel y será el nodo que esté en espera.

- 6 Haga clic en **Agregar**.
- 7 Haga clic en el nombre del enrutador que acaba de crear.
- 8 Haga clic en la pestaña **Configuración** y seleccione **Puertos del enrutador**.
- 9 Haga clic en **Agregar**.
- 10 Escriba un nombre para el puerto de enrutador y, opcionalmente, una descripción.
- 11 En el campo **Tipo**, seleccione **Centralizado**.
- 12 En **Modo URPF**, seleccione **Estricto** o **Ninguno**.
El reenvío de ruta inversa de unidifusión (Unicast Reverse Path Forwarding, URPF) es una función de seguridad.
- 13 (Requerido) Seleccione un conmutador lógico.

- 14 Seleccione si desea que esta conexión cree un puerto de conmutador o actualice un puerto de conmutador existente.
- 15 Introduzca la dirección IP del puerto del enrutador en notación CIDR.
- 16 Haga clic en **Agregar**.

Enrutador lógico de nivel 0

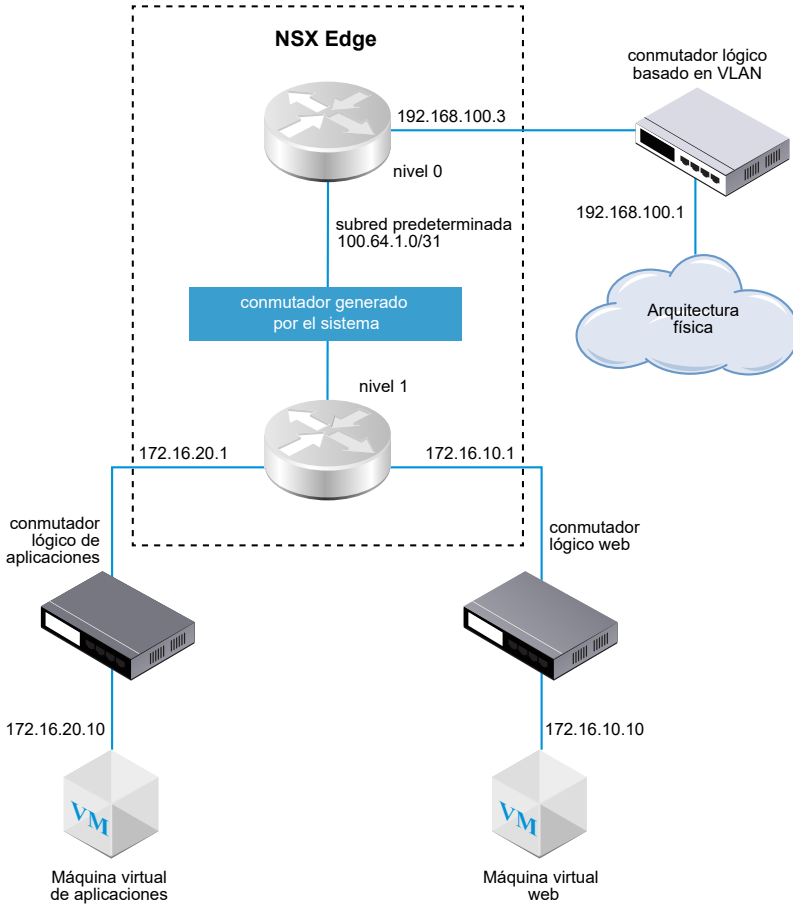
Un enrutador lógico de nivel 0 proporciona un servicio de puerta de enlace entre la red física y lógica.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

Un nodo de Edge solo es compatible con una puerta de enlace o un enrutador lógico de nivel 0. Al crear una puerta de enlace o un enrutador lógico de nivel 0, asegúrese de no crear un número de puertas de enlace o enrutadores lógicos de nivel 0 superior al número de nodos de Edge del clúster de NSX Edge.

Al agregar un enrutador lógico de nivel 0, es importante que planifique la topología de red que crea.

Figura 14-3. Topología del enrutador lógico de nivel 0



Para simplificar el ejemplo de topología, en él se muestra un único enrutador lógico de nivel 1 conectado a un único enrutador lógico de nivel 0 alojado en un único nodo de NSX Edge. Tenga en cuenta que esta no es una topología recomendada. Lo ideal es tener un mínimo de dos nodos de NSX Edge para aprovechar al máximo el diseño del enrutador lógico.

El enrutador lógico de nivel 1 tiene un conmutador lógico web y un conmutador lógico de aplicaciones con sus respectivas máquinas virtuales asociadas. El conmutador enrutador-vínculo entre el enrutador de nivel 1 y el de nivel 0 se crea automáticamente al asociar el enrutador de nivel 1 al de nivel 0. Por lo tanto, este conmutador se califica como generado por el sistema.

En algunos casos, los clientes externos envían consultas de ARP para las direcciones MAC enlazadas a puertos IP de IKE o de bucle invertido. Sin embargo, los puertos IP de IKE o de bucle invertido no tienen direcciones MAC y no pueden gestionar estas consultas. El proxy ARP se implementa en el enlace ascendente y los puertos de servicio centralizados de un enrutador lógico de nivel 0 para controlar las consultas de ARP en nombre de los puertos IP de IKE o de bucle invertido.

Al configurar un enrutador lógico de nivel 0 con DNAT, IPSec y el firewall de Edge, el tráfico se procesa en este orden: primero IPSec, segundo DNAT y, por último, el firewall de Edge.

En un enrutador lógico de nivel 0 o 1, puede configurar diferentes tipos de puertos. Un tipo se denomina puerto de servicio centralizado (CSP). Debe configurar un CSP en un enrutador lógico de nivel 0 en modo activo-en espera, o bien en un enrutador lógico de nivel 1 para conectarse a un conmutador lógico respaldado por VLAN o para crear un enrutador lógico de nivel 1 independiente. Un CSP es compatible con los siguientes servicios en un enrutador lógico de nivel 0 en modo activo-en espera o en un enrutador lógico de nivel 1:

- NAT
- Equilibrio de carga
- Firewall con estado
- VPN (IPsec y L2VPN)

Crear un enrutador lógico de nivel 0

Los enrutadores lógicos de nivel 0 tienen puertos de vínculo de descarga para conectarse a enrutadores lógicos de nivel 1 de NSX-T Data Center y puertos de vínculo superior para conectarse a redes externas.

Requisitos previos

- Compruebe que al menos un NSX Edge esté instalado. Consulte la *Guía de instalación de NSX-T Data Center*.
- Compruebe que haya un clúster de NSX Edge configurado. Consulte la *Guía de instalación de NSX-T Data Center*.
- Familiarícese con la topología de red del enrutador lógico de nivel 0. Consulte [Enrutador lógico de nivel 0](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Enrutadores > Enrutadores > Agregar**.
- 3 Seleccione **Enrutador de nivel 0** en el menú desplegable.
- 4 Asigne un nombre al enrutador lógico de nivel 0.
- 5 En el menú desplegable, seleccione un clúster de NSX Edge ya creado para respaldar este enrutador lógico de nivel 0.
- 6 (opcional) Seleccione un modo de alta disponibilidad.

El modo activo/activo se utiliza de forma predeterminada. En el modo activo/activo, la carga del tráfico se equilibra en todos los miembros. En el modo activo/espera, un miembro activo elegido procesa todo el tráfico. Si el miembro activo no realiza este proceso, se elige otro nuevo miembro para que sea activo.

- 7 (opcional) Haga clic en la pestaña **Avanzado** para introducir una subred para la subred de tránsito de internivel 0.

Esta es la subred que conecta el enrutador de los servicios de nivel 0 a su enrutador distribuido. Si deja este campo en blanco, se utilizará la subred predeterminada 169.0.0.0/28.

- 8 (opcional) Haga clic en la pestaña **Avanzado** para introducir una subred para la subred de tránsito entre el nivel 0 y nivel 1.

Esta es la subred que conecta el enrutador de nivel 0 a cualquier enrutador de nivel 1 conectado a este enrutador de nivel 0. Si deja este campo en blanco, el espacio de dirección para estas conexiones entre el nivel 0 y nivel 1 es 100.64.0.0/16. A cada conexión del mismo nivel de nivel 0 a nivel 1 se le proporciona una subred /31 dentro del espacio de direcciones 100.64.0.0/16.

- 9 Haga clic en **Guardar**.

El nuevo enrutador lógico de nivel 0 aparecerá en forma de vínculo.

- 10 (opcional) Haga clic en este vínculo para consultar el resumen.

Pasos siguientes

Asocie los enrutadores lógicos de nivel 1 a este enrutador lógico de nivel 0.

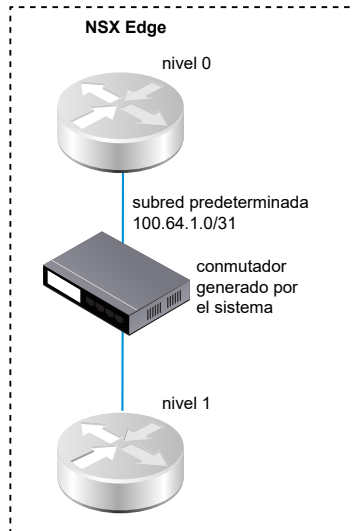
Configure el enrutador lógico de nivel 0 para conectarlo a un conmutador lógico VLAN y crear un vínculo superior a una red externa. Consulte [Conectar un enrutador lógico de nivel 0 a un conmutador lógico VLAN para el vínculo superior de NSX Edge](#).

Adjuntar nivel 0 y nivel 1

Es posible adjuntar el enrutador lógico de nivel 0 al de nivel 1, de tal modo que este último obtenga conectividad de red de Norte a Sur y Este a Oeste.

Al conectar un enrutador lógico de nivel 1 a uno de nivel 0, se crea un conmutador de vínculo de enrutador entre los dos. Este conmutador se etiqueta como generado por el sistema en la topología. El espacio de dirección predeterminado asignado para dichas conexiones nivel-0-a-nivel-1 es 100.64.0.0/16. A cada conexión del mismo nivel de nivel 0 a nivel 1 se le proporciona una subred /31 dentro del espacio de direcciones 100.64.0.0/16. También puede configurar el espacio de direcciones en la configuración del nivel 0 **Resumen > Avanzado**.

La siguiente cifra muestra una topología como ejemplo.



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 1.
- 4 De la pestaña **Resumen**, haga clic en **Editar**.
- 5 Seleccione el enrutador lógico de nivel 0 en el menú desplegable.
- 6 (opcional) Seleccione un clúster de NSX Edge del menú desplegable.
 Debe realizarse una copia de seguridad del enrutador de nivel 1 en un dispositivo Edge si el enrutador se utilizará para servicios, como NAT. Si no selecciona un clúster de NSX Edge, el enrutador de nivel 1 no puede realizar el servicio NAT.
- 7 Especifique los miembros y el miembro preferido.
 Si selecciona un clúster de NSX Edge y deja los campos de miembros y el miembro preferido en blanco, NSX-T Data Center establece el dispositivo de copia de seguridad del clúster especificado.
- 8 Haga clic en **Guardar**.
- 9 Haga clic en la pestaña **Configuración** del enrutador de nivel 1 para comprobar que se creó la dirección IP del puerto con vinculación punto a punto.
 Por ejemplo, la dirección IP del puerto vinculado puede ser 100.64.1.1/31.
- 10 Seleccione el enrutador lógico de nivel 0 en el panel de navegación.
- 11 Haga clic en la pestaña **Configuración** del enrutador de nivel 0 para comprobar que se creó la dirección IP del puerto con vinculación punto a punto.
 Por ejemplo, la dirección IP del puerto vinculado puede ser 100.64.1.1/31.

Pasos siguientes

Compruebe que el enrutador de nivel 0 aprenda acerca de rutas anunciadas por enrutadores de nivel 1.

Comprobar que un enrutador de nivel 0 aprendió las rutas de un enrutador de nivel 1

Cuando un enrutador lógico de nivel 1 anuncia las rutas a un enrutador lógico de nivel 0, las rutas se incluyen en la tabla de enrutamiento del enrutador de nivel 0 como rutas estáticas de NSX-T Data Center.

Procedimiento

- 1 En NSX Edge, ejecute el comando `get logical-routers` para encontrar el número de VRF del enrutador de servicio de nivel 0.

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 0
type          : TUNNEL

Logical Router
UUID          : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf           : 5
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf           : 6
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf           : 7
type          : SERVICE_ROUTER_TIER1

Logical Router
UUID          : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf           : 8
type          : DISTRIBUTED_ROUTER
```

- 2 Ejecute el comando `vrf <number>` para introducir el contexto del enrutador de servicios de nivel 0.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```


- 3 En el enrutador de servicios de nivel 0, ejecute el comando `get route` y compruebe que las rutas esperadas aparezcan en la tabla de enrutamiento.

Tenga en cuenta que el enrutador de nivel 0 aprende las rutas estáticas (ns) de NSX-T Data Center porque el enrutador de nivel 1 anuncia las rutas.

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

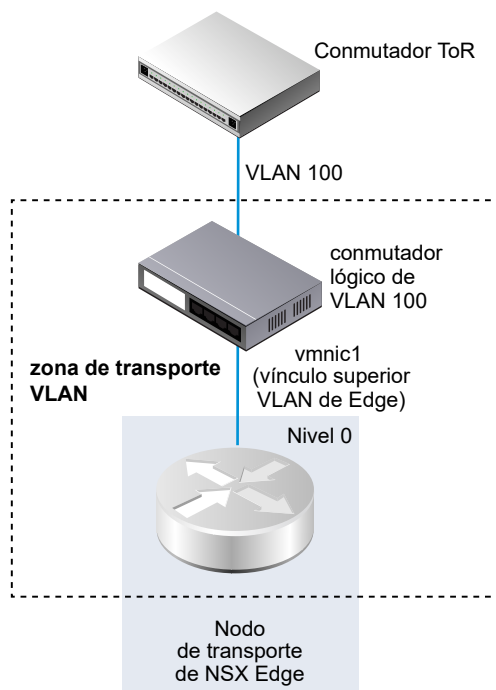
Total number of routes: 7

b    10.10.10.0/24      [20/0]      via 192.168.100.254
rl   100.91.176.0/31   [0/0]      via 169.254.0.1
c    169.254.0.0/28    [0/0]      via 169.254.0.2
ns   172.16.10.0/24    [3/3]      via 169.254.0.1
ns   172.16.20.0/24    [3/3]      via 169.254.0.1
c    192.168.100.0/24  [0/0]      via 192.168.100.2
```

Conectar un enrutador lógico de nivel 0 a un conmutador lógico VLAN para el vínculo superior de NSX Edge

Para crear un vínculo superior de NSX Edge, debe conectar un enrutador de nivel 0 al conmutador VLAN.

La siguiente topología sencilla muestra un conmutador lógico VLAN dentro de una zona de transporte VLAN. El conmutador lógico VLAN tiene un ID de VLAN que coincide con el del puerto TOR para el vínculo superior de la VLAN de Edge.



Requisitos previos

Cree un conmutador lógico VLAN. Consulte [Crear un conmutador lógico VLAN para el vínculo superior de NSX Edge](#).

Cree un enrutador de nivel 0.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 En la pestaña **Configuración**, agregue un puerto nuevo para el enrutador lógico.
- 5 Escriba un nombre para el puerto, por ejemplo "vínculo superior".
- 6 Seleccione el tipo **Vínculo superior**.
- 7 Seleccione un nodo de transporte de Edge.
- 8 Seleccione un conmutador lógico VLAN.
- 9 Escriba una dirección IP con el formato CIDR en la misma subred que el puerto conectado en el conmutador TOR.

Resultados

Se agrega un vínculo superior nuevo para el enrutador de nivel 0.

Pasos siguientes

Configure BGP o una ruta estática.

Comprobar la conexión del enrutador lógico de nivel 0 y TOR

Para que el enrutamiento funcione en el vínculo superior desde el enrutador de nivel 0, se debe disponer de conectividad con el dispositivo para parte superior de bastidor.

Requisitos previos

- Compruebe que el enrutador lógico de nivel 0 esté conectado a un conmutador lógico de VLAN. Consulte [Conectar un enrutador lógico de nivel 0 a un conmutador lógico VLAN para el vínculo superior de NSX Edge](#).

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager.

- 2 En NSX Edge, ejecute el comando `get logical-routers` para encontrar el número de VRF del enrutador de servicio de nivel 0.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 3 Ejecute el comando `vrf <number>` para introducir el contexto del enrutador de servicios de nivel 0.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4 En el enrutador de servicio de nivel 0, ejecute el comando `get route` y asegúrese de que la ruta prevista se muestra en la tabla de enrutamiento.

Tenga en cuenta que la ruta al TOR aparece como conectado (c).

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]       via 169.254.0.1
```

```

c    169.254.0.0/28      [0/0]      via 169.254.0.2
ns   172.16.10.0/24     [3/3]      via 169.254.0.1
ns   172.16.20.0/24     [3/3]      via 169.254.0.1
c    192.168.100.0/24   [0/0]      via 192.168.100.2

```

5 Haga ping al TOR.

```

nsx-edge1(tier0_sr)> ping      192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms

```

Resultados

Los paquetes se envían entre el enrutador lógico de nivel 0 y el enrutador físico para verificar una conexión.

Pasos siguientes

Dependiendo de sus requisitos de red, puede configurar una ruta estática o BGP. Consulte [Configurar una ruta estática](#) o [Configurar BGP en un enrutador lógico de nivel 0](#).

Agregar un puerto de bucle invertido al enrutador

Puede agregar un puerto de bucle invertido a un enrutador lógico de nivel 0.

El puerto de bucle invertido se puede usar con los siguientes propósitos:

- ID del enrutador para los protocolos de enrutamiento
- NAT
- BDF
- Dirección de origen de los protocolos de enrutamiento

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Seleccione **Configuración > Puertos del enrutador**.
- 5 Haga clic en **Agregar**.

- 6 Introduzca un nombre y, si lo desea, una descripción.
- 7 Seleccione el tipo **Bucle invertido**.
- 8 Seleccione un nodo de transporte de Edge.
- 9 Introduzca una dirección IP en formato CIDR.

Resultados

Se agrega un puerto nuevo para el enrutador de nivel 0.

Agregar un puerto de VLAN en un enrutador lógico de nivel 0 o de nivel 1

Si tiene solo conmutadores lógicos respaldados por VLAN, puede conectar los conmutadores a los puertos de VLAN en un enrutador de nivel 0 o de nivel 1 para que NSX-T Data Center pueda suministrar servicios de capa 3.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el nombre de un enrutador.
- 4 Haga clic en la pestaña **Configuración** y seleccione **Puertos del enrutador**.
- 5 Haga clic en **Agregar**.
- 6 Escriba un nombre para el puerto de enrutador y, opcionalmente, una descripción.
- 7 En el campo **Tipo**, seleccione **Centralizado**.
- 8 En **Modo URPF**, seleccione **Estricto** o **Ninguno**.
El reenvío de ruta inversa de unidifusión (Unicast Reverse Path Forwarding, URPF) es una función de seguridad.
- 9 (Requerido) Seleccione un conmutador lógico.
- 10 Seleccione si desea que esta conexión cree un puerto de conmutador o actualice un puerto de conmutador existente.
Si la conexión es para un puerto de conmutador existente, seleccione el puerto en el menú desplegable.
- 11 Introduzca la dirección IP del puerto del enrutador en notación CIDR.
- 12 Haga clic en **Agregar**.

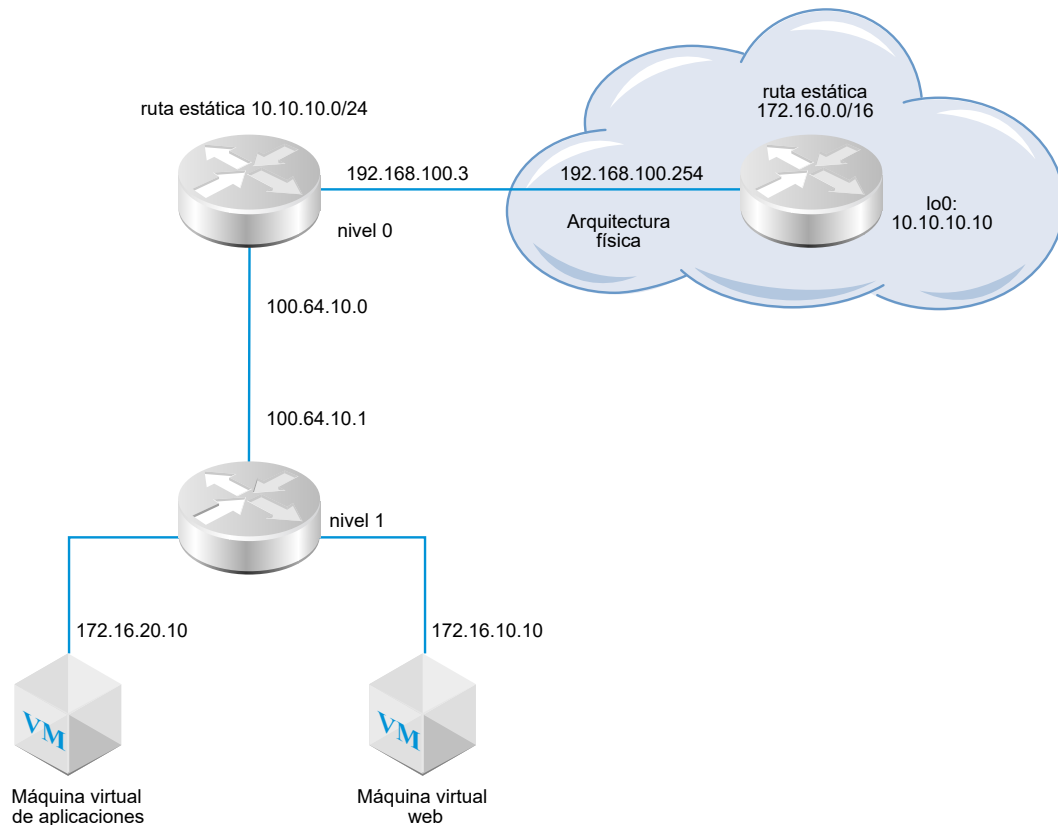
Configurar una ruta estática

Puede configurar una ruta estática en el enrutador de nivel 0 para redes externas. Tras configurar la ruta estática, no es necesario anunciar la ruta de nivel 0 a nivel 1, ya que los enrutadores de

nivel 1 poseen de forma automática una ruta estática predeterminada hacia el enrutador de nivel 0 al que están conectados.

La topología de la ruta estática muestra un enrutador lógico de nivel 0 con una ruta estática al prefijo 10.10.10.0/24 en la arquitectura física. A modo de prueba, la dirección 10.10.10.10/32 se configura en la interfaz de bucle invertido del enrutador externo. El enrutador externo posee una ruta estática al prefijo 172.16.0.0/16 para alcanzar la aplicación y web de las máquinas virtuales.

Figura 14-4. Topología de la ruta estática



Se admiten las rutas estáticas recursivas.

Requisitos previos

- Compruebe que el enrutador físico y el enrutador lógico de nivel 0 están conectados. Consulte [Comprobar la conexión del enrutador lógico de nivel 0 y TOR](#).
- Compruebe que el enrutador de nivel 1 está configurado para anunciar las rutas conectadas. Consulte [Crear un enrutador lógico de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.

- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **Ruta estática** en el menú desplegable.
- 5 Seleccione **Agregar**.
- 6 Introduzca una dirección de red en formato CIDR.
Por ejemplo, 10.10.10.0/24.
- 7 Haga clic en **+ Agregar** para agregar una dirección IP de próximo salto.
Por ejemplo, 192.168.100.254. También puede especificar una ruta nula haciendo clic en el icono de lápiz y seleccionando **NULO** en el menú desplegable.
- 8 Especifique la distancia administrativa.
- 9 Seleccione un puerto de enrutador lógico en la lista desplegable.
La lista incluye los puertos de la interfaz de túnel virtual (VTI) de IPsec.
- 10 Haga clic en el botón **Agregar**.

Pasos siguientes

Compruebe que la ruta estática está configurada correctamente. Consulte [Comprobar la ruta estática](#).

Comprobar la ruta estática

Utilice la CLI para comprobar que la ruta estática esté conectada. También debe comprobar que el enrutador externo pueda hacer ping a las máquinas virtuales internas y viceversa.

Requisitos previos

Compruebe que una ruta estática esté configurada. Consulte [Configurar una ruta estática](#).

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager.

2 Confirme la ruta estática.

- a Obtenga la información de UUID del enrutador de servicios.

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

- b Localice la información de UUID de la salida.

```
Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0
```

- c Compruebe que la ruta estática funcione.

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 route static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s    10.10.10.0/24      [1/1]      via 192.168.100.254
rl   100.64.1.0/31     [0/0]      via 169.0.0.1
ns   172.16.10.0/24    [3/3]      via 169.0.0.1
ns   172.16.20.0/24    [3/3]      via 169.0.0.1
```


- 3 En el enrutador externo, haga ping a las máquinas virtuales internas para confirmar que se puede acceder a ellas a través de la superposición de NSX-T Data Center.

- a Conéctese al enrutador externo.

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- b Pruebe la conectividad de red.

```
tracert 172.16.10.10
```

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.64.1.1 (100.64.1.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4 En las máquinas virtuales, haga ping a la dirección IP externa.

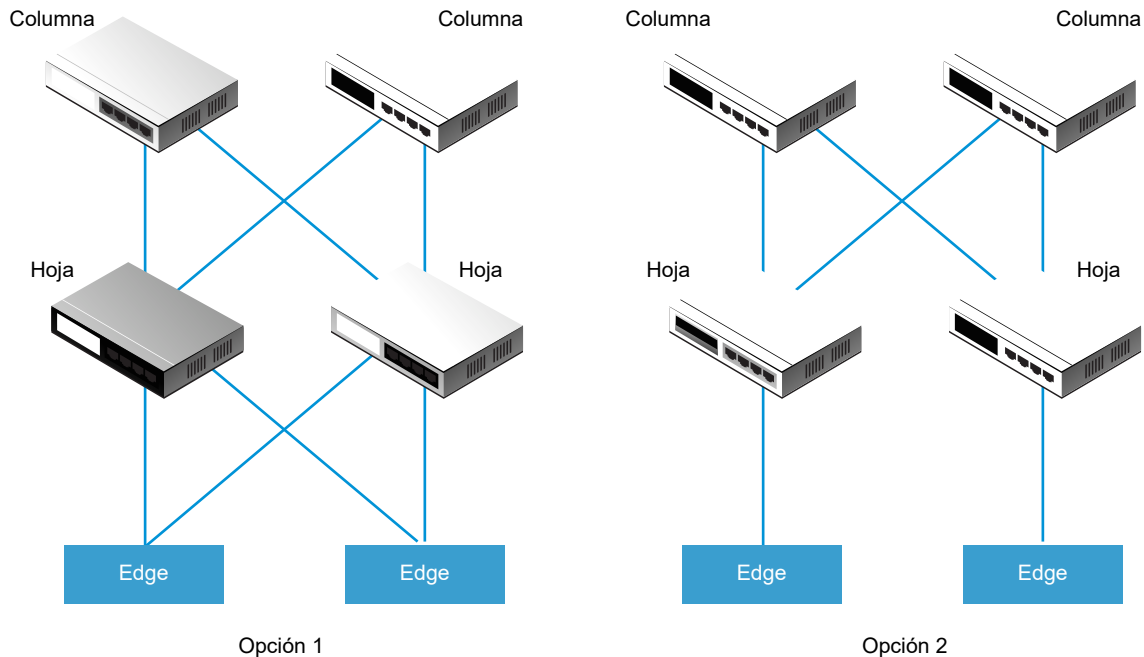
```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

Opciones de configuración de BGP

Para sacar pleno provecho del enrutador lógico de nivel 0, se debe configurar la topología con redundancia y simetría con BGP entre los enrutadores de nivel 0 y los elementos del mismo nivel externos de la parte superior del rack. Este diseño ayuda a garantizar la conectividad en caso de que el vínculo o el nodo fallen.

Existen dos modos de configuración: activo-activo y activo-espera. El siguiente diagrama muestra dos opciones de configuración simétrica. Hay dos nodos NSX Edge en cada topología. En el caso de una configuración activo-activo, al crear puertos de vínculo superior de nivel 0, puede asociar cada uno de ellos con hasta ocho nodos de transporte NSX Edge. Cada nodo NSX Edge puede poseer dos puertos de vínculo superior.



Para la opción 1, cuando se configuran los enrutadores físicos de nodo hoja, deben poseer vecinos BGP con NSX Edge. La redistribución de rutas debe incluir los mismos prefijos de red con métricas BGP similares para todos los vecinos BGP. En la configuración de enrutadores lógicos de nivel 0, todos los enrutadores deben configurarse como vecinos BGP.

Cuando esté configurando los vecinos BGP del enrutador de nivel 0, si no especifica una dirección local (la dirección IP de origen), la configuración de vecino BGP se envía a todos los nodos NSX Edge asociados con los vínculos superiores de enrutadores lógicos de nivel 0. Si configura una dirección local, la configuración pasa al nodo NSX Edge con el vínculo superior que posea dicha dirección IP.

En el caso de la opción 1, si los vínculos superiores se encuentran en la misma subred de los nodos NSX Edge, resulta lógico omitir la dirección local. Si los vínculos superiores en los nodos NSX Edge se encuentran en distintas subredes, la dirección local debe especificarse en la configuración del vecino BGP del enrutador de nivel 0 para evitar que la configuración se aplique a todos los nodos NSX Edge asociados.

Para la opción 2, compruebe que la configuración del enrutador lógico de nivel 0 incluya la dirección IP local del enrutador de servicios con nivel 0. Los enrutadores de nodo hoja están solo configurados con las instancias de NSX Edge que estén directamente conectadas, como el vecino BGP.

Configurar BGP en un enrutador lógico de nivel 0

Para habilitar el acceso entre las máquinas virtuales y el mundo exterior, puede configurar una conexión BGP externa o interna (eBGP o iBGP) entre el enrutador lógico de nivel 0 y el enrutador de la infraestructura física.

La función iBGP presenta las siguientes capacidades y restricciones:

- Se admite la redistribución, las listas de prefijos y los mapas de rutas.
- No se admiten los reflectores de ruta.
- No se admite la confederación BGP.

Al configurar BGP, debe configurar un número local de sistema autónomo (Autonomous System, AS) para el enrutador lógico de nivel 0. Por ejemplo, la siguiente topología muestra que el número local del AS es 64510. También debe configurar el número de AS remoto. Los vecinos de EBGP deben estar conectados directamente y en la misma subred que el vínculo superior de nivel 0. Si no están en la misma subred, se deberá utilizar los saltos múltiples BGP.

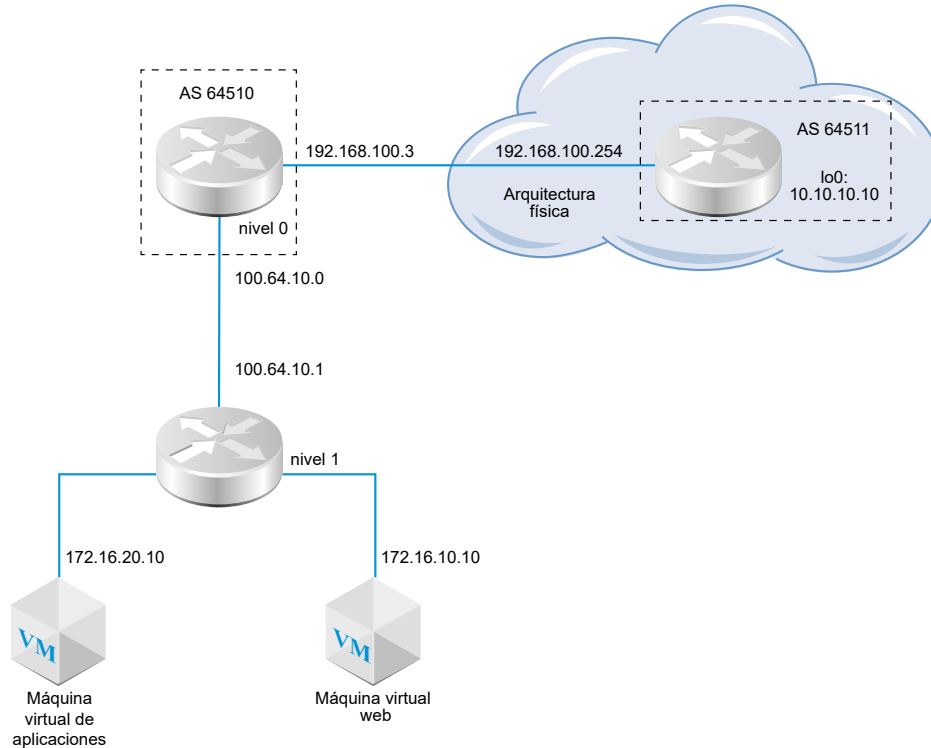
Un enrutador lógico de nivel 0 en modo activo/activo es compatible con el enrutamiento entre-SR (enrutador de servicio). Si el enrutador n.º 1 no puede comunicarse con un enrutador físico en dirección norte, el tráfico se vuelve a enrutar al enrutador n.º 2 en el clúster activo/activo. Si el enrutador n.º 2 puede comunicarse con el enrutador físico, el tráfico entre el enrutador n.º 1 y el enrutador físico no se verá afectado.

En una topología con un enrutador lógico de nivel 0 en modo activo-activo conectado a un enrutador lógico de nivel 1 en modo activo-en espera, debe habilitar el enrutamiento inter-SR para gestionar el enrutamiento asimétrico. Si configura una ruta estática en uno de los SR o si uno de los SR necesita comunicarse con el vínculo superior de otro SR, entonces tiene un enrutamiento asimétrico. Además, tenga en cuenta lo siguiente:

- En el caso de una ruta estática configurada en una instancia de SR (por ejemplo, SR1 en el nodo de Edge1), es posible que otro SR (por ejemplo, SR2 en el nodo de Edge2) obtenga la misma ruta de un eBGP del mismo nivel y prefiera esta ruta a la ruta estática de SR1, que puede resultar más eficaz. Para asegurarse de que SR2 utilice la ruta estática configurada en SR1, configure el enrutador lógico de nivel 1 en modo preferente y configure el nodo de Edge1 como nodo de preferencia.
- Si el enrutador lógico de nivel 0 tiene un puerto de vínculo superior en el nodo de Edge1 y otro en el nodo de Edge2, el tráfico de ping de las máquinas virtuales de tenant a los vínculos superiores funciona si los dos vínculos superiores se encuentran en subredes diferentes. Si los dos vínculos superiores están en la misma subred, se producirá un error en el tráfico de ping.

Nota El ID del enrutador utilizado para crear sesiones BGP en un nodo Edge se selecciona automáticamente a partir de las direcciones IP configuradas en los vínculos superiores de un enrutador lógico de nivel 0. Las sesiones BGP en un nodo Edge pueden oscilar cuando la ID del enrutador cambia. Esto puede suceder cuando se eliminan la dirección IP autoseleccionada para un ID del enrutador o el puerto del enrutador lógico al que esta IP está asignada.

Figura 14-5. Topología de conectividad BGP



Tenga en cuenta los siguientes escenarios cuando se produzcan errores de conexión relacionados con BGP o BFD:

- Cuando solo se configura BGP y se desactivan todos los vecinos BGP, el estado del enrutador de servicio será inactivo.
- Cuando solo se configura BFD y se desactivan todos los vecinos BFD, el estado del enrutador de servicio será inactivo.
- Cuando se configuran BGP y BFD y se desactivan todos los vecinos BGP y BFD, el estado del enrutador de servicio será inactivo.
- Cuando se configuran BGP y rutas estáticas y se desactivan todos los vecinos BGP, el estado del enrutador de servicio será inactivo.
- Cuando solo se configuran rutas estáticas, el estado del enrutador de servicio siempre será activo a menos que el nodo sufra algún error o esté en modo de mantenimiento.

Requisitos previos

- Compruebe que el enrutador de nivel 1 está configurado para anunciar las rutas conectadas. Consulte [Configurar anuncios de rutas en un enrutador lógico de nivel 1](#). Esto no es un requisito obligatorio de la configuración BGP, pero si posee una topología de dos niveles y planea volver a distribuir las redes de nivel 1 en BGP, si es necesario.
- Compruebe que el enrutador de nivel 0 esté configurado. Consulte [Crear un enrutador lógico de nivel 0](#).

- Compruebe que el enrutador de nivel 0 aprendió las rutas del enrutador lógico de nivel 1. Consulte [Comprobar que un enrutador de nivel 0 aprendió las rutas de un enrutador de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **BGP** en el menú desplegable.
- 5 Haga clic en **Editar**.
 - a Introduzca el número del AS local.
Por ejemplo, 64510.
 - b Haga clic en el botón de alternancia **Estado** para habilitar o deshabilitar BGP.
 - c Haga clic en el botón de alternancia **ECMP** para habilitar o deshabilitar ECMP.
 - d Haga clic en el botón de alternancia **Reinicio estable** para habilitar o deshabilitar el reinicio estable.

El reinicio estable solo es compatible si el clúster de NSX Edge asociado con el enrutador de nivel 0 solo posee un nodo de Edge.
 - e Si este enrutador lógico se encuentra en modo activo/activo, haga clic en el botón de alternancia **Enrutamiento entre SR** para habilitar o deshabilitar el enrutamiento entre SR.
 - f Configure la agregación de rutas.
 - g Haga clic en **Guardar**.
- 6 Haga clic en **Agregar** para agregar un vecino BGP.
- 7 Introduzca la dirección IP de vecino.
Por ejemplo, 192.168.100.254.
- 8 Especifique el límite de salto máximo.
El valor predeterminado es 1.
- 9 Introduzca el número del AS remoto.
Por ejemplo, 64511 (vecino eBGP) o 64510 (vecino iBGP).
- 10 Configure los temporizadores (mantenimiento y supresión) y una contraseña.
- 11 Haga clic en la pestaña **Dirección local** para seleccionar una dirección local.
 - a (opcional) Desactive **Todos los vínculos superiores** para ver los puertos de bucles invertidos, así como los puertos de enlaces ascendentes.

- 12 Haga clic en la pestaña **Familias de direcciones** para agregar una familia de direcciones.
- 13 Haga clic en la pestaña **Configuración de BFD** para habilitar BFD.
- 14 Haga clic en **Guardar**.

Pasos siguientes

Compruebe que BGP esté funcionando correctamente. Consulte [Comprobar las conexiones BGP desde un enrutador de servicios de nivel 0](#).

Comprobar las conexiones BGP desde un enrutador de servicios de nivel 0

Utilice la CLI para comprobar desde el enrutador de servicios de nivel 0 que se estableció una conexión BGP a un vecino.

Requisitos previos

Compruebe que BGP esté configurado. Consulte [Configurar BGP en un enrutador lógico de nivel 0](#).

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager.
- 2 En NSX Edge, ejecute el comando `get logical-routers` para encontrar el número de VRF del enrutador de servicio de nivel 0.

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 0
type          : TUNNEL

Logical Router
UUID          : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf           : 5
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf           : 6
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf           : 7
type          : SERVICE_ROUTER_TIER1

Logical Router
UUID          : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf           : 8
type          : DISTRIBUTED_ROUTER
```

- 3 Ejecute el comando `vrf <number>` para introducir el contexto del enrutador de servicios de nivel 0.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4 Compruebe que el estado de BGP sea `Established, up` (Establecido, activo).

```
get bgp neighbor
```

```
BGP neighbor: 192.168.100.254    Remote AS: 64511
BGP state: Established, up
Hold Time: 180s    Keepalive Interval: 60s
Capabilities:
    Route Refresh: advertised and received
    Address Family: IPv4 Unicast:advertised and received
    Graceful Restart: none
    Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received
    Route Refresh: 0 received, 0 sent
    Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044
```

Pasos siguientes

Compruebe la conexión BGP desde el enrutador externo. Consulte [Comprobar la conectividad en dirección norte y la redistribución de rutas](#).

Configurar BFD en un enrutador lógico de nivel 0

El protocolo de detección de envío bidireccional (Bidirectional Forwarding Detection, BFD) puede detectar los errores de envío de rutas.

Nota En esta versión, no se admite la BFD sobre puertos de interfaz virtual de túnel (VTI).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **BFD** del menú desplegable.
- 5 Haga clic en **Editar** para configurar BFD.

- 6 Haga clic en el botón de alternancia **Estado** para habilitar BFD.

De forma opcional, es posible cambiar las propiedades BFD globales **Recibir intervalo**, **Transmitir intervalo** y **Declarar intervalo inactivo**.

- 7 (opcional) Haga clic en **Agregar** en Elementos BFD del mismo nivel para próximos saltos de rutas estáticas para agregar un elemento BFD del mismo nivel.

Especifique la dirección IP del elemento y establezca el estado de administrador como **Habilitado**. De forma opcional, es posible sobrescribir las propiedades BFD globales **Recibir intervalo**, **Transmitir intervalo** y **Declarar intervalo inactivo**.

Habilitar la redistribución de rutas en el enrutador lógico de nivel 0

Cuando habilita la redistribución de rutas, el enrutador lógico de nivel 0 comienza a compartir rutas especificadas con su enrutador en dirección norte.

Requisitos previos

- Compruebe que los enrutadores lógicos de nivel 0 y 1 estén conectados para que pueda anunciar las redes del enrutador lógico de nivel 1 para redistribuirlas en el enrutador lógico de nivel 0. Consulte [Adjuntar nivel 0 y nivel 1](#).
- Si quiere filtrar direcciones IP específicas de la redistribución de rutas, compruebe que estén configurados los mapas de rutas. Consulte [Crear un mapa de rutas](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **Redistribución de rutas** en el menú desplegable.
- 5 Haga clic en **Editar** para habilitar o deshabilitar la redistribución de rutas.

- 6 Haga clic en **Agregar** para agregar un conjunto de criterios de redistribución de rutas.

Opción	Descripción
Nombre y descripción	Asigne un nombre a la redistribución de rutas. Puede proporcionar una descripción de forma opcional. Un nombre de ejemplo sería advertise-to-bgp-neighbor.
Orígenes	<p>Seleccione uno o varios de los siguientes orígenes:</p> <ul style="list-style-type: none"> ■ Nivel 0 conectado ■ Vínculo superior de nivel 0 ■ Vínculo inferior de nivel 0 ■ CSP de nivel 0 ■ Bucle invertido de nivel 0 ■ Nivel 0 estático ■ NAT de nivel 0 ■ IP de reenviador de DNS de nivel 0 ■ IP local de IPSec de nivel 0 ■ Nivel 1 conectado ■ CSP de nivel 1 ■ Vínculo inferior de nivel 1 ■ Nivel 1 estático ■ SNAT de equilibrador de carga de nivel 1 ■ NAT de nivel 1 ■ VIP de equilibrador de carga de nivel 1 ■ IP de reenviador de DNS de nivel 1
Mapa de ruta	(Opcional) Asigne un mapa de rutas para filtrar una secuencia de direcciones IP de la redistribución de rutas.

Comprobar la conectividad en dirección norte y la redistribución de rutas

Use la CLI para comprobar que se aprendieron las rutas de BGP. También puede comprobar desde el enrutador externo que se pueda acceder a las VM conectadas a NSX-T Data Center.

Requisitos previos

- Compruebe que BGP esté configurado. Consulte [Configurar BGP en un enrutador lógico de nivel 0](#).
- Compruebe que las rutas estáticas de NSX-T Data Center estén configuradas para ser redistribuidas. Consulte [Habilitar la redistribución de rutas en el enrutador lógico de nivel 0](#).

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager.
- 2 Vea las rutas aprendidas desde el vecino BGP externo.

```
nsx-edge1(tier0_sr)> get route bgp
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

b    10.10.10.0/24          [20/0]          via 192.168.100.254
```

- 3 Desde el enrutador externo, compruebe que las rutas BGP se aprendieron y que se pueda acceder a las VM a través de la superposición de NSX-T Data Center.

- a Enumere las rutas BGP.

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

- b Desde el enrutador externo, haga ping en las VM conectadas a NSX-T Data Center.

ping 172.16.10.10

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- c Compruebe la ruta a través de la superposición de NSX-T Data Center.

traceroute 172.16.10.10

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.91.176.1 (100.91.176.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4 Desde las VM internas, haga ping en la dirección IP externa.

ping 10.10.10.10

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
```

```
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

Pasos siguientes

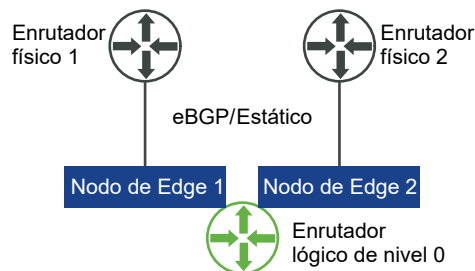
Configure funcionalidades de enrutamiento adicional, como ECMP.

Información sobre el enrutamiento ECMP

El protocolo de enrutamiento Multipath de igual coste (Equal cost multi-path, ECMP) aumenta el ancho de banda de la comunicación norte y sur al agregar un vínculo superior al enrutador lógico de nivel 0 y lo configura para cada nodo de Edge de un clúster de NSX Edge. Las rutas de enrutamiento ECMP se utilizan para equilibrar la carga del tráfico y para ofrecer una tolerancia a errores para las rutas con errores.

El enrutador lógico de nivel 0 debe estar en modo activo-activo para que el ECMP esté disponible. Se admite un máximo de ocho rutas ECMP. La implementación de ECMP en NSX Edge se basa en las 5 tuplas del número de protocolo, la dirección de origen, la dirección de destino, el puerto de origen y el puerto de destino. El algoritmo utilizado para distribuir los datos entre las rutas ECMP no es ROUND_ROBIN. Por lo tanto, algunas rutas pueden generar más tráfico que otras. Tenga en cuenta que si el protocolo es IPv6 y el encabezado IPv6 tiene más de un encabezado de extensión, ECMP se basará solo en las direcciones de origen y de destino.

Figura 14-6. Topología del enrutamiento ECMP



Por ejemplo, la topología anterior muestra un solo enrutador lógico de nivel 0 en modo activo-activo que se ejecuta en un clúster de NSX Edge de 2 nodos. Se configuran dos puertos de vínculo superior, uno en cada nodo de Edge.

Agregar un puerto de vínculo superior a un segundo nodo Edge

Antes de habilitar ECMP, debe configurar un vínculo superior para conectar el enrutador lógico de nivel 0 al conmutador lógico VLAN.

Requisitos previos

- Compruebe que la zona de transporte y los dos nodos de transporte estén configurados. Consulte la *Guía de instalación de NSX-T Data Center*.

- Compruebe que los dos nodos Edge y el clúster Edge estén configurados. Consulte la *Guía de instalación de NSX-T Data Center*.
- Compruebe que el conmutador lógico VLAN para el vínculo superior esté disponible. Consulte [Crear un conmutador lógico VLAN para el vínculo superior de NSX Edge](#).
- Compruebe que el enrutador lógico de nivel 0 esté configurado. Consulte [Crear un enrutador lógico de nivel 0](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Configuración** para agregar un puerto de enrutador.
- 5 Haga clic en **Agregar**.
- 6 Complete los detalles del puerto de enrutador.

Opción	Descripción
Nombre	Asigne un nombre al puerto de enrutador.
Descripción	Proporcione una descripción adicional que muestre que el puerto es para la configuración ECMP.
Tipo	Acepte el tipo predeterminado Vínculo superior .
MTU	Si deja este campo vacío, se usará 1.500 como valor predeterminado.
Nodo de transporte	Asigne el nodo de transporte de Edge en el menú desplegable.
Modo URPF	El reenvío de ruta inversa de unidifusión es una función de seguridad. Se recomienda que se establezca como Ninguno si tiene varios nodos de Edge activo-activo en el modo ECMP. El valor predeterminado es Estricto .
Conmutador lógico	Asigne el conmutador lógico del host en el menú desplegable.
Puerto de conmutador lógico	Asigne un nuevo nombre al puerto del conmutador. También puede utilizar un puerto del conmutador existente.
Dirección/máscara IP	Introduzca una dirección IP que se encuentre en la misma subred que el puerto conectado al conmutador ToR.

- 7 Haga clic en **Guardar**.

Resultados

Se agrega un nuevo puerto de vínculo superior al enrutador de nivel 0 y al conmutador lógico VLAN. El enrutador lógico de nivel 0 se configura en ambos nodos Edge.

Pasos siguientes

Cree una conexión BGP para el segundo vecino y habilite el enrutamiento ECMP. Consulte [Agregar un segundo vecino BGP y habilitar el enrutamiento ECMP](#).

Agregar un segundo vecino BGP y habilitar el enrutamiento ECMP

Antes de habilitar el enrutamiento ECMP, debe agregar un vecino BGP y configurarlo con la información del vínculo superior recién agregado.

Requisitos previos

Compruebe que un puerto de vínculo superior esté configurado en el segundo nodo Edge. Consulte [Agregar un puerto de vínculo superior a un segundo nodo Edge](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **BGP** en el menú desplegable.
- 5 Haga clic en **Agregar** en la sección Vecinos para agregar un vecino BGP.
- 6 Introduzca la dirección IP de vecino.
Por ejemplo, 192.168.200.254.
- 7 (opcional) Especifique el límite de salto máximo.
El valor predeterminado es 1.
- 8 Introduzca el número del AS remoto.
Por ejemplo, 64511.
- 9 (opcional) Haga clic en la pestaña **Dirección local** para seleccionar una dirección local.
 - a (opcional) Desactive **Todos los vínculos superiores** para ver los puertos de bucles invertidos, así como los puertos de enlaces ascendentes.
- 10 (opcional) Haga clic en la pestaña **Familias de direcciones** para agregar una familia de direcciones.
- 11 (opcional) Haga clic en la pestaña **Configuración de BFD** para habilitar BFD.
- 12 Haga clic en **Guardar**.
Aparece el vecino BGP recién agregado.
- 13 Haga clic en **Editar** junto a la sección Configuración BGP.
- 14 Haga clic en el botón de alternancia **ECMP** para habilitar ECMP.
El botón de Estado debe aparecer como Habilitado.

15 Haga clic en **Guardar**.

Resultados

Varias rutas de enrutamiento ECMP se conectan a las máquinas virtuales asociadas a los conmutadores lógicos y los dos nodos Edge en el clúster Edge.

Pasos siguientes

Verifique que las conexiones de enrutamiento ECMP funcionen de manera correcta. Consulte [Comprobar la conectividad del enrutamiento ECMP](#).

Comprobar la conectividad del enrutamiento ECMP

Utilice la CLI para comprobar si se estableció la conexión del enrutamiento ECMP al vecino.

Requisitos previos

Compruebe que el enrutamiento ECMP esté configurado. Consulte [Agregar un puerto de vínculo superior a un segundo nodo Edge](#) y [Agregar un segundo vecino BGP y habilitar el enrutamiento ECMP](#).

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager.
- 2 Obtenga la información de UUID del enrutador distribuido.

```
get logical-routers
```

```
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL

Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf           : 6
type          : DISTRIBUTED_ROUTER
```

3 Localice la información de UUID de la salida.

```
Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER
```

4 Escriba el VRF del enrutador distribuido de nivel 0.

```
vrf 5
```

5 Compruebe que el enrutador distribuido de nivel 0 esté conectado a los nodos de Edge.

```
get forwarding
```

Por ejemplo, edge-node-1 y edge-node-2.

6 Introduzca **exit** para dejar el contexto vrf.

7 Compruebe que el enrutador distribuido de nivel 0 esté conectado.

```
get logical-router <UUID> route
```

El tipo de ruta del UUID debe aparecer como NSX_CONNECTED.

8 Inicie una sesión SSH en los dos nodos de Edge.

9 Inicie una sesión para capturar paquetes.

```
set capture session 0 interface fp-eth1 dir tx
```

```
set capture session 0 expression src net <IP_Address>
```

10 Use cualquier herramienta que pueda generar tráfico desde una máquina virtual de origen conectada al enrutador de nivel 0 hasta una máquina virtual de destino.

11 Observe el tráfico en los dos nodos de Edge.

Crear una lista de prefijos IP

Una lista de prefijos IP contiene una o varias direcciones IP que tienen asignados permisos de acceso para anunciar rutas. Las direcciones IP de esta lista se procesan de forma secuencial. Las listas de prefijos IP se incluyen a través de los filtros de vecino BGP o los mapas de rutas con dirección entrante o saliente.

Por ejemplo, puede agregar la dirección IP 192.168.100.3/27 a la lista de prefijos IP y no permitir que la ruta se redistribuya al enrutador ascendente. También puede agregar una dirección IP con los modificadores "igual o inferior a" (le) y "igual o superior a" (ge) para permitir o limitar la redistribución de rutas. Por ejemplo, los modificadores le 30 y ge 24 de 192.168.100.3/27 coinciden con las máscaras de subred iguales o superiores a 24 bits, e iguales o inferiores a 30 bits de largo.

Nota La acción predeterminada de una ruta es **Denegar**. Cuando cree una lista de prefijos para denegar o permitir rutas específicas, asegúrese de crear un prefijo de IP sin una dirección de red específica (seleccione **Cualquiera** en la lista desplegable) y elegir la acción **Permitir** si desea permitir otras rutas.

Requisitos previos

Compruebe que tenga un enrutador lógico de nivel 0 configurado. Consulte [Crear un enrutador lógico de nivel 0](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **Listas de prefijos de IP** del menú desplegable.
- 5 Haga clic en **Agregar**.
- 6 Introduzca un nombre para la lista de prefijos de IP.
- 7 Haga clic en **Agregar** para especificar un prefijo.
 - a Introduzca una dirección IP en formato CIDR.
Por ejemplo, 192.168.100.3/27.
 - b Seleccione **Denegar** o **Permitir** en el menú desplegable.
 - c (opcional) Establezca un rango de números de dirección IP en los modificadores **le** o **ge**.
Por ejemplo, establezca el valor 30 para el modificador **le** y el valor 24 para el modificador **ge**.
- 8 Repita el paso anterior para especificar prefijos adicionales.
- 9 Haga clic en **Agregar** en la parte inferior de la ventana.

Crear una lista de comunidad

Puede crear listas de comunidad de BGP para configurar mapas de rutas en función de estas.

Requisitos previos

Compruebe que tenga un enrutador lógico de nivel 0 configurado. Consulte [Crear un enrutador lógico de nivel 0](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Haga clic en la pestaña **Enrutamiento** y seleccione **Listas de comunidad** en el menú desplegable.
- 5 Haga clic en **Agregar**.
- 6 Escriba un nombre para la lista de comunidad.
- 7 Especifique una comunidad con el formato aa:nn, por ejemplo, 300:500, y pulse Intro. Repita este procedimiento para agregar comunidades adicionales.

Además, puede hacer clic en la flecha desplegable y seleccionar una o varias de las siguientes opciones:

- NO_EXPORT_SUBCONFED: no anuncia a pares EGBP.
- NO_ADVERTISE: no anuncia a ningún par.
- NO_EXPORT: no anuncia fuera de la confederación BGP.

- 8 Haga clic en **Agregar**.

Crear un mapa de rutas

Un mapa de rutas es una secuencia de listas de prefijos IP, atributos de rutas BGP y una acción asociada. El enrutador analiza la secuencia para buscar una coincidencia de direcciones IP. Si hay alguna coincidencia, el enrutador realiza la acción y deja de analizar la secuencia.

Los mapas de rutas se pueden incluir en la redistribución de rutas y en el nivel de vecino BGP. Cuando las listas de prefijos IP se incluyen en mapas de rutas y la acción de los mapas de rutas para permitir o denegar direcciones IP se aplica, la acción especificada en la secuencia de los mapas de rutas anula la especificación de la lista de prefijos IP.

Requisitos previos

Compruebe que una lista de prefijos IP esté configurada. Consulte [Crear una lista de prefijos IP](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.

- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Seleccione **Enrutamiento > Mapas de rutas**.
- 5 Haga clic en **Agregar**.
- 6 Introduzca un nombre y una descripción opcional para el mapa de rutas.
- 7 Haga clic en **Agregar** para agregar una entrada al mapa de rutas.
- 8 Edite la columna **Hacer coincidir con la lista de comunidades o la lista de prefijos de IP** para seleccionar las listas de prefijos IP o las listas de comunidad, pero no ambas.
- 9 (opcional) Establezca atributos BGP.

Atributo BGP	Descripción
AS-path Prepend	Anteponga una ruta con uno o varios números de sistemas autónomos (autonomous system, AS) para que la ruta sea más larga y, por tanto, tenga menor preferencia.
MED	El atributo Discriminador de salida múltiple (Multi-Exit Discriminator, MED) indica a un par externo la ruta de preferencia a un AS.
Peso	Establece una ponderación que influye en la selección de las rutas. El rango es 0-65.535.
Comunidad	<p>Especifique una comunidad con el formato aa:nn, por ejemplo, 300:500. O utilice el menú desplegable para seleccionar uno de los siguientes atributos:</p> <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED: no anuncia a pares EBGP. ■ NO_ADVERTISE: no anuncia a ningún par. ■ NO_EXPORT: no anuncia fuera de la confederación BGP.

- 10 En la columna Acción, seleccione **Permitir** o **Denegar**.

Puede permitir o no que las direcciones IP de las listas de prefijos IP anuncien sus direcciones.

- 11 Haga clic en **Guardar**.

Configurar el temporizador de reenvíos


Puede configurar el temporizador de reenvíos para un enrutador lógico de nivel 0.

El temporizador de reenvíos define el tiempo en segundos que el enrutador debe esperar antes de enviar la notificación de activación después de que se establezca la primera sesión BGP. Este temporizador (antes conocido como retraso de reenvío) minimiza el periodo de inactividad si se producen conmutaciones por error en configuraciones activa-activa o activa-en espera de enrutadores lógicos de NSX Edge que usen un enrutamiento dinámico (BGP). Se debe configurar según el número de segundos que un enrutador externo (TOR) tarda en detectar todos los enrutadores después de la primera sesión BGP/BFD. El valor del temporizador debe ser directamente proporcional al número de enrutadores dinámicos en dirección norte que el enrutador debe conocer. Se debe configurar el temporizador a 0 en las configuraciones de nodos Edge únicos.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador lógico de nivel 0.
- 4 Seleccione **Enrutamiento > Configuración global**.
- 5 Haga clic en **Editar**.
- 6 Introduzca un valor para el temporizador de reenvíos.
- 7 Haga clic en **Guardar**.

Puede configurar NAT desde la pestaña **Opciones avanzadas de redes y seguridad**.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Este capítulo incluye los siguientes temas:

- [Traducción de direcciones de red](#)

Traducción de direcciones de red

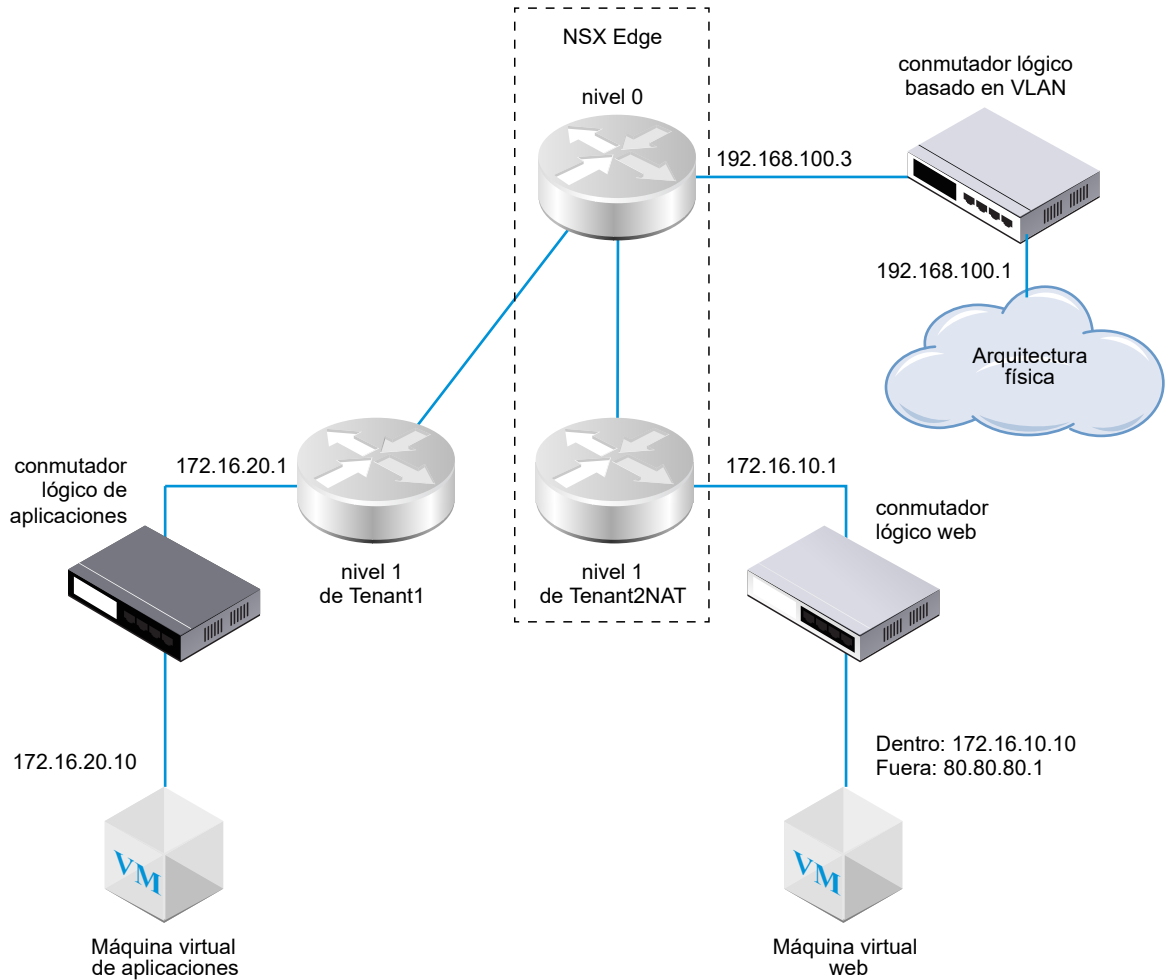
La traducción de direcciones de red (NAT) de NSX-T Data Center se puede configurar en los enrutadores lógicos de nivel 0 y nivel 1.

Por ejemplo, el siguiente diagrama muestra dos enrutadores lógicos de nivel 1 con NAT configurada en Tenant2NAT. La máquina virtual web se configura para utilizar 172.16.10.10 como dirección IP y 172.16.10.1 como puerta de enlace predeterminada.

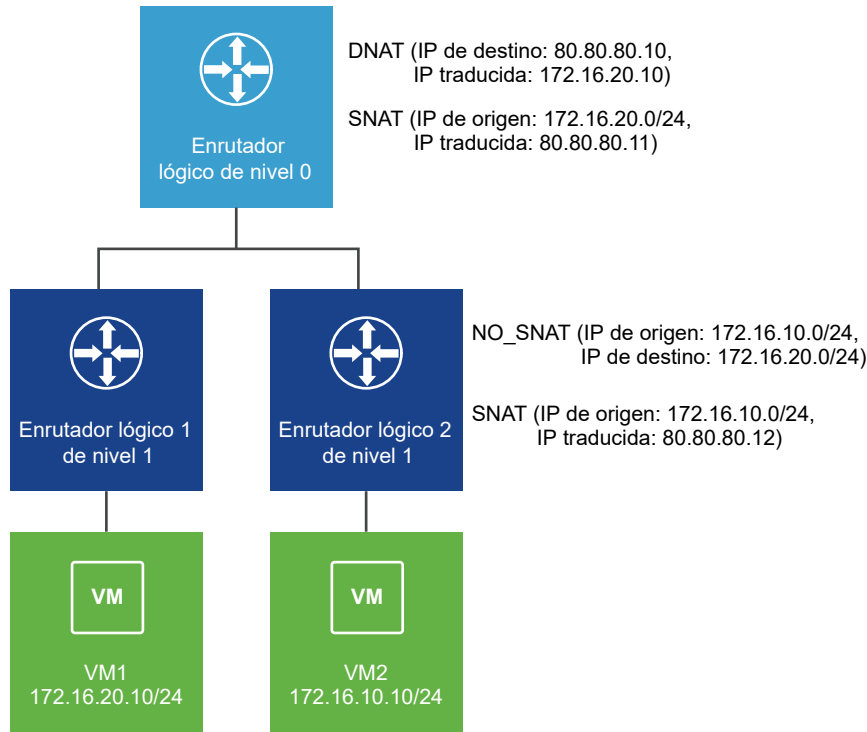
NAT se aplica al vínculo superior del enrutador lógico de Tenant2NAT en su conexión al enrutador lógico de nivel 0.

Para habilitar la configuración de NAT, Tenant2NAT debe tener un componente de servicio en un clúster de NSX Edge. Por tanto, Tenant2NAT se muestra dentro de NSX Edge. Para realizar comparativas, Tenant1 puede estar fuera de NSX Edge porque no utiliza ningún servicio de Edge.

Figura 15-1. Topología de NAT



Nota: En el siguiente escenario, no se admite la redirección al origen de NAT. El enrutador lógico de nivel 0 tiene configurados DNAT y SNAT. El enrutador lógico 2 de nivel 1 tiene configurados NO_SNAT y SNAT. VM2 no podrá acceder a VM1 con la dirección externa 80.80.80.10 de VM1.



En las siguientes secciones, se describe cómo crear reglas NAT mediante la interfaz de usuario de NSX Manager. También puede hacer una llamada API (`POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple`) para crear varias reglas NAT al mismo tiempo. Para obtener más información, consulte la *Guía de la API de NSX-T Data Center*.

NAT de nivel 1

Un enrutador lógico de nivel 1 es compatible con NAT de origen, NAT de destino y NAT reflexiva.

Configurar NAT de origen en un enrutador de nivel 1

Las reglas de NAT de origen (SNAT) cambian la dirección de origen en el encabezado IP del paquete. También puede cambiar el puerto de origen en los encabezados TCP/UDP. El uso general es cambiar una dirección o puerto privado (rfc1918) en uno público para los paquetes que abandonan la red.

Puede crear una regla para habilitar o deshabilitar la NAT de origen.

En este ejemplo, a medida que se reciben paquetes de la máquina virtual web, el enrutador de nivel 1 Tenant2NAT cambia la dirección IP de origen de los paquetes de 172.16.10.10 a 80.80.80.1. Una dirección IP de origen pública permite contar con destinos fuera de la red privada para volver a enrutar al primer origen.

Requisitos previos

- El enrutador de nivel 0 debe tener un vínculo superior conectado a un conmutador lógico basado en VLAN. Consulte [Conectar un enrutador lógico de nivel 0 a un conmutador lógico VLAN para el vínculo superior de NSX Edge](#).
- El enrutador de nivel 0 debe tener enrutamiento (estático o BGP) y la redistribución de rutas configurados en su vínculo superior a la arquitectura física. Consulte [Configurar una ruta estática](#), [Configurar BGP en un enrutador lógico de nivel 0](#) y [Habilitar la redistribución de rutas en el enrutador lógico de nivel 0](#).
- Cada uno de los enrutadores de nivel 1 debe tener configurado un vínculo superior a un enrutador de nivel 0. Un clúster de NSX Edge debe realizar una copia de seguridad de Tenant2NAT. Consulte [Adjuntar nivel 0 y nivel 1](#).
- Los enrutadores de nivel 1 deben tener configurados puertos de vínculo inferior y anuncio de ruta. Consulte [Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1](#) y [Configurar anuncios de rutas en un enrutador lógico de nivel 1](#).
- Las VM deben conectarse a los conmutadores lógicos pertinentes.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el enrutador lógico de nivel 1 sobre el que quiera configurar NAT.
- 4 Seleccione **Servicios > NAT**.
- 5 Haga clic en **AGREGAR**.
- 6 Especifique un valor de prioridad.
Un valor inferior significa una prioridad más alta para esta regla.
- 7 En **Acción**, seleccione **SNAT** para habilitar la NAT de origen o **NO_SNAT** para deshabilitarla.
- 8 Seleccione el tipo de protocolo.
De manera predeterminada, se encuentra seleccionada la opción **Cualquier protocolo**.
- 9 (opcional) Para **IP de origen**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.
Si deja este campo en blanco, todos los orígenes de los puertos de vínculo inferior del enrutador se traducirán. En este ejemplo, la dirección IP de origen es 172.16.10.10.
- 10 (opcional) Para **IP de destino**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.
Si deja este campo en blanco, la NAT se aplicará a todos los destinos fuera de la subred local.

- 11 Si **Acción** es **SNAT**, para la **IP traducida**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

En este ejemplo, la dirección IP traducida es 80.80.80.1.

- 12 (opcional) Para **Se aplica a**, seleccione un puerto de enrutador.

- 13 (opcional) Establezca el estado de la regla.

La regla está habilitada de forma predeterminada.

- 14 (opcional) Cambie el estado de registro.

De forma predeterminada, el registro está deshabilitado.

- 15 (opcional) Cambie el valor de omisión de firewall.

La opción está habilitada de manera predeterminada.

Resultados

La nueva regla se muestra bajo NAT. Por ejemplo:

Tenant2NAT

Información General

Configuración

Enrutamiento

Servicios

NAT

ACTUALIZAR

No se recopiló ninguna estadística

+ AGREGAR

EDITAR

ELIMINAR

Identificador	Acción	Hacer coincidir					Traducido		Se aplic	Estadís
		Protocolo	IP de origen	Puertos de origen	IP de destino	Puertos de destino	IP	Puertos		
Prioridad: 1024										
1036	SNAT	Cualq...	172.16.10.10	Cualquiera	Cualquiera	Cualquiera	80.80.80.1	Cual...		

Pasos siguientes

Configure el enrutador de nivel 1 para anunciar las rutas NAT.

Para anunciar las rutas NAT en sentido ascendente desde el enrutador de nivel 0 hasta la arquitectura física, configure el enrutador de nivel 0 para que anuncie las rutas NAT de nivel 1.

Configurar NAT de destino en un enrutador de nivel 1

El NAT de destino cambia la dirección de destino en el encabezado IP de un paquete. También puede cambiar el puerto de destino en los encabezados TCP/UDP. Su uso típico es el de redirigir los paquetes entrantes con un destino de una dirección/puerto público a una dirección IP/puerto privado dentro de su red.

Puede crear una regla para habilitar o deshabilitar la NAT de destino.

En este ejemplo, a medida que se reciben paquetes de la máquina virtual de aplicaciones, el enrutador de nivel 1 Tenant2NAT cambia la dirección IP de destino de los paquetes de 172.16.10.10 a 80.80.80.1. Una dirección IP de destino pública permite contar con un destino dentro de una red privada con el que se puede establecer contacto desde fuera de esta.

Requisitos previos

- El enrutador de nivel 0 debe tener un vínculo superior conectado a un conmutador lógico basado en VLAN. Consulte [Conectar un enrutador lógico de nivel 0 a un conmutador lógico VLAN para el vínculo superior de NSX Edge](#).
- El enrutador de nivel 0 debe tener enrutamiento (estático o BGP) y la redistribución de rutas configurados en su vínculo superior a la arquitectura física. Consulte [Configurar una ruta estática](#), [Configurar BGP en un enrutador lógico de nivel 0](#) y [Habilitar la redistribución de rutas en el enrutador lógico de nivel 0](#).
- Cada uno de los enrutadores de nivel 1 debe tener configurado un vínculo superior a un enrutador de nivel 0. Un clúster de NSX Edge debe realizar una copia de seguridad de Tenant2NAT. Consulte [Adjuntar nivel 0 y nivel 1](#).
- Los enrutadores de nivel 1 deben tener configurados puertos de vínculo inferior y anuncio de ruta. Consulte [Agregar un puerto de vínculo inferior en un enrutador lógico de nivel 1](#) y [Configurar anuncios de rutas en un enrutador lógico de nivel 1](#).
- Las VM deben conectarse a los conmutadores lógicos pertinentes.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el enrutador lógico de nivel 1 sobre el que quiera configurar NAT.
- 4 Seleccione **Servicios > NAT**.
- 5 Haga clic en **AGREGAR**.
- 6 Especifique un valor de prioridad.
Un valor inferior significa una prioridad más alta para esta regla.
- 7 En **Acción**, seleccione **DNAT** para habilitar la NAT de destino o **NO_DNAT** para deshabilitarla.
- 8 Seleccione el tipo de protocolo.
De manera predeterminada, se encuentra seleccionada la opción **Cualquier protocolo**.
- 9 (opcional) Para **IP de origen**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.
Si deja en blanco el campo IP de origen, NAT lo aplica a todos los orígenes externos a la subred local.
- 10 Para **IP de destino**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.
En este ejemplo, la dirección IP de destino es 80.80.80.1.

- 11 Si **Acción** es **DNAT**, para la **IP traducida**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

En este ejemplo, la dirección IP interna/traducida es 172.16.10.10.

- 12 (opcional) Si **Acción** es **DNAT**, para los **Puertos traducidos**, especifique los puertos traducidos.

- 13 (opcional) Para **Se aplica a**, seleccione un puerto de enrutador.

- 14 (opcional) Establezca el estado de la regla.

La regla está habilitada de forma predeterminada.

- 15 (opcional) Cambie el estado de registro.

De forma predeterminada, el registro está deshabilitado.

- 16 (opcional) Cambie el valor de omisión de firewall.

La opción está habilitada de manera predeterminada.

Resultados

La nueva regla se muestra bajo NAT. Por ejemplo:

Tenant2NAT

Información General Configuración Enrutamiento Servicios

NAT | ACTUALIZAR

No se recopiló ninguna estadística

+ AGREGAR EDITAR ELIMINAR

Identificador	Acción	Hacer coincidir					Traducido		Se aplica a	Estadística
		Protocolo	IP de origen	Puertos de origen	IP de destino	Puertos de destino	IP	Puertos		
Prioridad: 1024										
1034	DNAT	Cualq...	Cualque...	Cualquiera	80.80.80.1	Cualquiera	172.16.10.10	Cual...		

Pasos siguientes

Configure el enrutador de nivel 1 para anunciar las rutas NAT.

Para anunciar las rutas NAT en sentido ascendente desde el enrutador de nivel 0 hasta la arquitectura física, configure el enrutador de nivel 0 para que anuncie las rutas NAT de nivel 1.

Anunciar rutas NAT de nivel 1 para un enrutador ascendente de nivel 0

Anunciar rutas NAT de nivel 1 permite que el enrutador ascendente de nivel 0 aprenda acerca de dichas rutas.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.

- 3 Haga clic en un enrutador lógico de nivel 1 donde esté NAT configurado.
- 4 En el enrutador de nivel 1, seleccione **Enrutamiento > Anuncio de rutas**.
- 5 Haga clic en **Editar** para editar la configuración de anuncio de rutas.

Puede activar o desactivar los siguientes conmutadores:

- **Estado**
- **Anunciar rutas conectadas de NSX**
- **Anunciar todas las rutas de NAT**
- **Anunciar todas las rutas estáticas**
- **Anunciar rutas de VIP del LB**
- **Anunciar rutas de IP de SNAT del LB**
- **Anunciar todas las rutas de reenviador de DNS**

- 6 Haga clic en **Guardar**.

Pasos siguientes

Anuncie rutas NAT de nivel 1 del enrutador de nivel 0 para la arquitectura física ascendente.

Anunciar rutas NAT de nivel 1 para la arquitectura física

Anunciar rutas NAT de nivel 1 del enrutador de nivel 0 permite que la arquitectura física ascendente aprenda acerca de dichas rutas.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Enrutamiento**.
- 3 Haga clic en un enrutador lógico de nivel 0 conectado a un enrutador de nivel 1 donde NAT esté configurado.
- 4 En el enrutador de nivel 0, seleccione **Enrutamiento > Redistribución de rutas**.
- 5 Haga clic en **Editar** para habilitar o deshabilitar la redistribución de rutas.

- 6 Haga clic en **Agregar** para agregar un conjunto de criterios de redistribución de rutas.

Opción	Descripción
Nombre y descripción	Asigne un nombre a la redistribución de rutas. Puede proporcionar una descripción de forma opcional. Un nombre de ejemplo sería advertise-to-bgp-neighbor.
Orígenes	<p>Seleccione uno o varios de los siguientes orígenes:</p> <ul style="list-style-type: none"> ■ Nivel 0 conectado ■ Vínculo superior de nivel 0 ■ Vínculo inferior de nivel 0 ■ CSP de nivel 0 ■ Bucle invertido de nivel 0 ■ Nivel 0 estático ■ NAT de nivel 0 ■ IP de reenviador de DNS de nivel 0 ■ IP local de IPSec de nivel 0 ■ Nivel 1 conectado ■ CSP de nivel 1 ■ Vínculo inferior de nivel 1 ■ Nivel 1 estático ■ SNAT de equilibrador de carga de nivel 1 ■ NAT de nivel 1 ■ VIP de equilibrador de carga de nivel 1 ■ IP de reenviador de DNS de nivel 1
Mapa de ruta	(Opcional) Asigne un mapa de rutas para filtrar una secuencia de direcciones IP de la redistribución de rutas.

Comprobar la NAT de nivel 1

Compruebe que las reglas SNAT y DNAT funcionen correctamente.

Procedimiento

- 1 Inicie sesión en NSX Edge.
- 2 Ejecute el comando `get logical-routers` para determinar el número VRF del enrutador de servicios de nivel 0.
- 3 Ejecute el comando `vrf <number>` para introducir el contexto del enrutador de servicios de nivel 0.
- 4 Ejecute el comando `get route` y compruebe que la dirección de NAT de nivel 1 aparezca.

```
nsx-edge(tier0_sr)> get route
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
Total number of routes: 8

tln  80.80.80.1/32          [3/3]          via 169.0.0.1
...
```

- 5 Si la máquina virtual web está configurada para mostrar páginas web, compruebe que pueda abrir una página web en <http://80.80.80.1>.
- 6 Compruebe que el vecino en dirección ascendente del enrutador de nivel 0 de la arquitectura física pueda hacer ping a 80.80.80.1.
- 7 Mientras se esté ejecutando el ping, compruebe la columna de estadísticas de la regla DNAT. Debe haber una sesión activa.

NAT de nivel 0

Un enrutador lógico de nivel 0 en modo activo-en espera es compatible con NAT de origen, NAT de destino y NAT reflexiva. Un enrutador lógico de nivel 0 en modo activo-activo, admite solo NAT reflexivas.

Configurar NAT de origen y destino en un enrutador lógico de nivel 0

Es posible configurar NAT de origen y destino en un enrutador lógico de nivel 0 que se ejecuta en modo activo-en espera.

También se puede deshabilitar SNAT o DNAT para una dirección IP o un rango de direcciones. Si se aplican varias reglas NAT a una dirección, se aplicará la regla con la prioridad más alta.

La regla SNAT que se configura en el enlace ascendente de un enrutador lógico de nivel 0 procesará el tráfico desde un enrutador lógico de nivel 1 así como desde otro enlace ascendente en el enrutador lógico de nivel 0.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en un enrutador lógico de nivel 0.
- 4 Seleccione **Servicios > NAT**.
- 5 Haga clic en **AGREGAR** para agregar una regla NAT.
- 6 Especifique un valor de prioridad.
Un valor inferior significa una prioridad más elevada.
- 7 En **Acción**, seleccione **SNAT**, **DNAT**, **Sin Reflexivo**, **NO_SNAT** o **NO_DNAT**.
- 8 Seleccione el tipo de protocolo.
De manera predeterminada, se encuentra seleccionada la opción **Cualquier protocolo**.

- 9 (Requerido) Para **IP de origen**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

Si deja vacío este campo, esta regla NAT se aplicará a todos los orígenes fuera de la subred local.

- 10 Para **IP de destino**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

- 11 Para **IP traducida**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.

- 12 (opcional) Si **Acción** es **DNAT**, para los **Puertos traducidos**, especifique los puertos traducidos.

- 13 (opcional) Para **Se aplica a**, seleccione un puerto de enrutador.

- 14 (opcional) Establezca el estado de la regla.

La regla está habilitada de forma predeterminada.

- 15 (opcional) Cambie el estado de registro.

De forma predeterminada, el registro está deshabilitado.

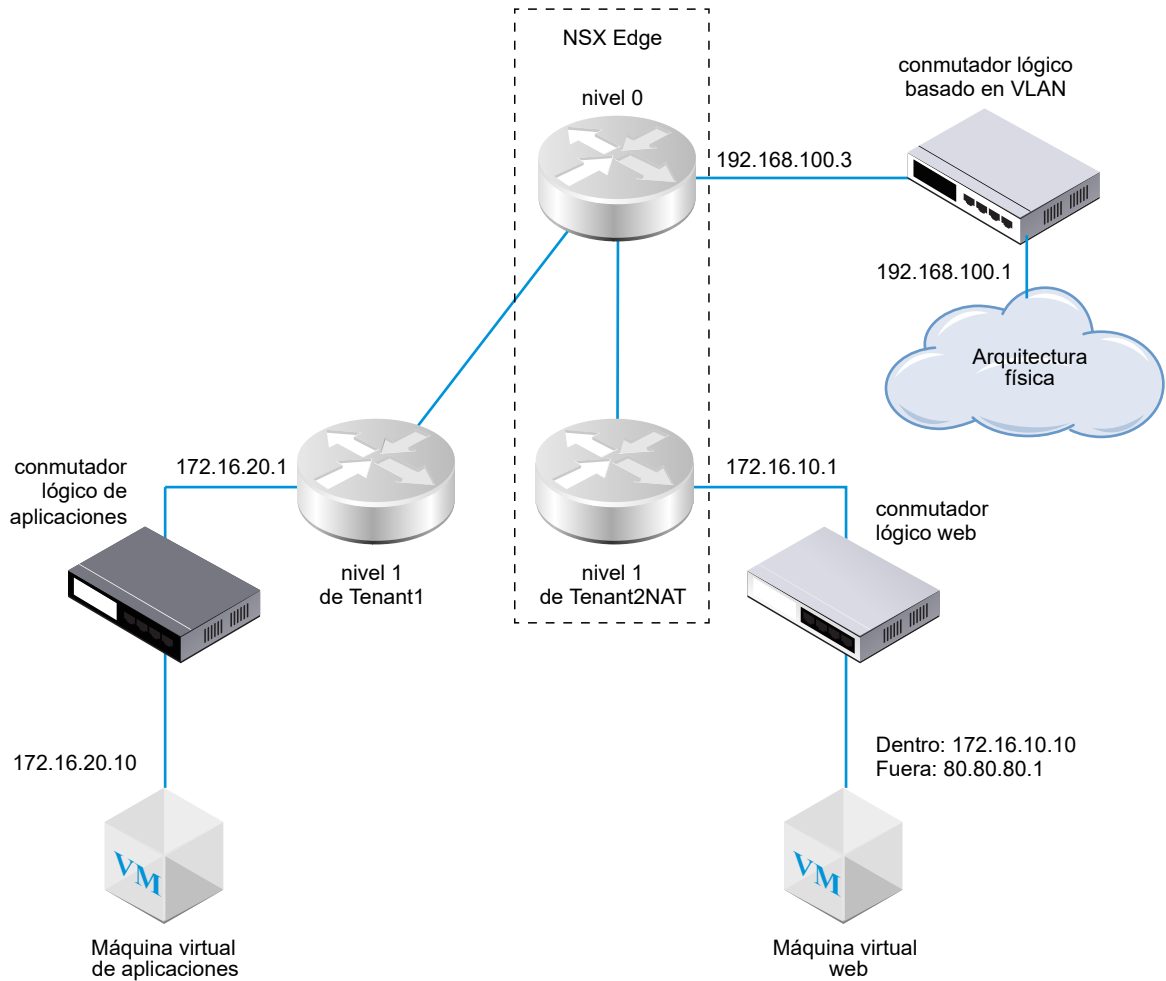
- 16 (opcional) Cambie el valor de omisión de firewall.

La opción está habilitada de manera predeterminada.

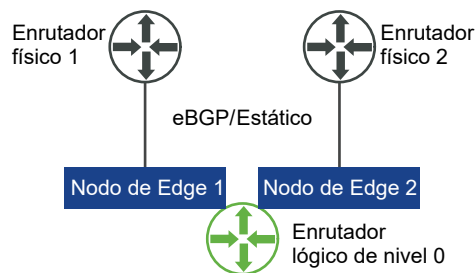
NAT reflexiva

Cuando un enrutador lógico de nivel 0 se ejecuta en modo activo-activo, no puede configurar la traducción de direcciones de red (Network Address Translation, NAT) con estado, ya que las rutas asimétricas podrían causar problemas. En el caso de los enrutadores con el modo activo-activo, puede configurar la NAT reflexiva (en ocasiones denominada NAT sin estado).

En este ejemplo, a medida que se reciben paquetes de la máquina virtual web, el enrutador de nivel 1 Tenant2NAT cambia la dirección IP de origen de los paquetes de 172.16.10.10 a 80.80.80.1. Una dirección IP de origen pública permite contar con destinos fuera de la red privada para volver a enrutar al primer origen.



Cuando participan dos enrutadores de nivel 0 con el modo activo-activo (como se muestra a continuación), se debe configurar la NAT reflexiva.



Configurar NAT reflexiva en un enrutador lógico de nivel 0 o nivel 1

Cuando un enrutador lógico de nivel 0 o nivel 1 se ejecuta en modo activo-activo, no puede configurar la traducción de direcciones de red (Network Address Translation, NAT) con estado, ya que las rutas asimétricas podrían causar problemas. En el caso de los enrutadores con el modo activo-activo, puede utilizar la NAT reflexiva, en ocasiones denominada NAT sin estado.

Para la NAT reflexiva, puede configurar que se traduzca una sola dirección de origen o un rango de direcciones. Si configura un rango de direcciones de origen, también debe configurar un rango de direcciones traducidas. El tamaño de los dos rangos debe ser el mismo. La traducción de direcciones será determinista, lo que significa que la primera dirección del rango de direcciones de origen se traducirá como la primera dirección en el rango de direcciones traducidas, la segunda dirección del rango de origen se traducirá como la segunda dirección del rango traducido, y así sucesivamente.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en el enrutador lógico de nivel 0 o nivel 1 donde desee configurar la NAT reflexiva.
- 4 Seleccione **Servicios > NAT**.
- 5 Haga clic en **AGREGAR**.
- 6 Especifique un valor de prioridad.
Un valor inferior significa una prioridad más alta para esta regla.
- 7 Para **Acción**, seleccione **Reflexivo**.
- 8 Para **IP de origen**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.
- 9 Para **IP traducida**, especifique una dirección IP o un rango de direcciones IP en formato CIDR.
- 10 (opcional) Establezca el estado de la regla.
La regla está habilitada de forma predeterminada.
- 11 (opcional) Cambie el estado de registro.
De forma predeterminada, el registro está deshabilitado.
- 12 (opcional) Cambie el valor de omisión de firewall.
La opción está habilitada de manera predeterminada.

Resultados

La nueva regla se muestra bajo NAT. Por ejemplo:

Tier0-LR-1 ×

[Información General](#)
[Configuración](#)
[Enrutamiento](#)
[Servicios](#)

NAT [ACTUALIZAR](#)

Total de estadísticas de regla | Última actualización: 6 de mar. de 2019 18:19:10

0 Sesiones activas
+ AGREGAR
EDITAR
ELIMINAR

0 Recuento de paquetes


0 Bytes Datos

Identificador	Acción	Coincide con					Traducido		Se aplica	Estadísticas
		Protocolo	IP de origen	Puertos de origen	IP de destino	Puertos de destino	IP	Puertos		
▼ Prioridad: 1024										
✓ 2048	Reflexivo	Cualquiera	80.80.80.1	Cualquiera	Cualquiera	Cualquiera	172.16.10....	Cualquiera		

Agrupación de objetos avanzada

16

Puede crear conjuntos de IP, grupos de IP, conjuntos de MAC, NSGroups y NSServices. Además, puede administrar las etiquetas de las máquinas virtuales.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Este capítulo incluye los siguientes temas:

- [Crear un conjunto de direcciones IP](#)
- [Crear un grupo de direcciones IP](#)
- [Crear un conjunto de direcciones MAC](#)
- [Crear un grupo NSGroup](#)
- [Configurar servicios y grupos de servicios](#)
- [Administrar las etiquetas de una máquina virtual](#)

Crear un conjunto de direcciones IP

Un conjunto de direcciones IP es un grupo de direcciones IP que se pueden utilizar como orígenes y destinos en reglas de firewall.

Un conjunto de direcciones IP puede contener una combinación de direcciones IP individuales, rangos de IP y subredes. Puede especificar direcciones IPv4 o IPv6, o ambas. Un conjunto de direcciones IP puede ser miembro de grupos NSGroup. Cualquier conjunto de direcciones IP creado con este método no será visible en el modo Directiva. En el modo Directiva, se puede crear un grupo y agregar miembros como direcciones IP, rangos, direcciones de red o direcciones MAC al navegar a **Inventario > Grupos > Establecer miembros** y especificar direcciones IP o MAC.

Nota Se admiten direcciones IPv4 y direcciones IPv6 para los rangos de origen o destino de las reglas de firewall.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Grupos > Conjuntos de direcciones IP > Agregar**.
- 3 Introduzca un nombre.
- 4 (opcional) Escriba una descripción.
- 5 En **Miembros**, introduzca las direcciones IP individuales, los rangos de IP y las subredes en una lista separada por comas.
- 6 Haga clic en **Guardar**.

Crear un grupo de direcciones IP

Puede utilizar un grupo de direcciones IP para asignar subredes o direcciones IP al crear subredes de Capa 3.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Grupos > Grupos de direcciones IP > Agregar**.
- 3 Escriba un nombre para el nuevo grupo de IP.
- 4 (opcional) Escriba una descripción.
- 5 Haga clic en **Agregar**.
- 6 Haga clic en la celda Rangos de IP e introduzca los rangos de IP.
Coloque el cursor del mouse sobre la esquina superior derecha de cualquier celda y haga clic en el icono de lápiz para editarla.
- 7 (opcional) Introduzca una puerta de enlace.
- 8 Introduzca una dirección IP de CIDR con sufijo.
- 9 (opcional) Introduzca servidores DNS.
- 10 (opcional) Introduzca un sufijo DNS.
- 11 Haga clic en **Guardar**.

Crear un conjunto de direcciones MAC

Un conjunto de direcciones MAC es un grupo de direcciones MAC que puede utilizar como origen y destino en reglas de firewall de Capa 2 y como miembro de un grupo NSGroup.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Grupos > Conjuntos de direcciones MAC > Agregar**.
- 3 Introduzca un nombre.
- 4 (opcional) Escriba una descripción.
- 5 Introduzca las direcciones MAC en una lista separada por comas.
- 6 Haga clic en **AGREGAR**.

Crear un grupo NSGroup

Los grupos NSGroup se pueden configurar para que contengan una combinación de conjuntos de direcciones IP, conjuntos de direcciones MAC, puertos lógicos, conmutadores lógicos y otros grupos NSGroup. Puede especificar grupos NSGroup con conmutadores lógicos, puertos lógicos y máquinas virtuales como orígenes y destinos, así como en el campo `Applied To` de una regla del firewall. Los grupos NSGroup con un conjunto de direcciones IP y un conjunto de direcciones MAC se omitirán en un campo `Applied To` del firewall distribuido.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

Un grupo NSGroup tiene las siguientes características:

- Un grupo NSGroup tiene miembros directos y efectivos. Entre los miembros efectivos, se incluyen los miembros que especifica con los criterios de pertenencia, así como todos los miembros efectivos y directos que pertenecen a los miembros de este grupo NSGroup. Por ejemplo, imaginemos que el grupo NSGroup-1 tiene el miembro directo LogicalSwitch-1. Agrega el grupo NSGroup-2 y especifica NSGroup-1 y LogicalSwitch-2 como miembros. Ahora NSGroup-2 tiene los miembros directos NSGroup-1 y LogicalSwitch-2, así como un miembro efectivo, LogicalSwitch-1. A continuación, agrega NSGroup-3 y especifica NSGroup-2 como miembro. NSGroup-3 ahora tiene el miembro directo NSGroup-2 y los miembros efectivos LogicalSwitch-1 y LogicalSwitch-2. En la tabla de grupos principal, al hacer clic en un grupo y seleccionar **Relacionado > Grupos NSGroup**, aparecería NSGroup-1, NSGroup-2 y NSGroup-3 debido a que LogicalSwitch-1 es miembro de estos tres de forma directa o indirecta.
- Un grupo NSGroup puede tener un máximo de 500 miembros directos.

- El límite recomendado para el número de miembros efectivos de un grupo NSGroup es 5.000. NSX Manager comprueba el límite de los grupos NSGroup dos veces al día, a las 7 de la mañana y a las 7 de la tarde. Si supera este límite, ninguna funcionalidad se verá afectada pero es posible que exista un impacto negativo en el rendimiento.
- Cuando el número de miembros efectivos de un grupo NSGroup supera el 80% de 5.000, se muestra el mensaje de advertencia `El grupo NSGroup xyz está a punto de superar el límite máximo de miembros. El número total de grupos NSGroup es... en el archivo de registro.` Cuando el número supera el límite de 5.000, aparece el mensaje de advertencia `El grupo NSGroup xyz alcanzó el límite máximo de números. Número total en el grupo NSGroup =`
- Cuando el número de direcciones MAC o IP, o de archivos VIF traducidos, supera el límite de 5.000, se muestra el mensaje de advertencia `El contenedor xyz alcanzó el límite máximo de traducciones de IP/MAC/VIF. Las traducciones actuales se incluyen en Contenedor: Direcciones IP:..., Direcciones MAC:..., Archivos VIF:... en el archivo de registro.`
- El número máximo de máquinas virtuales admitidas es 10.000.
- Puede crear un máximo de 10.000 grupos NSGroup.

Para todos los objetos que se pueden agregar a un grupo NSGroup como miembros, puede desplazarse hasta la pantalla de cualquiera de los objetos y seleccionar **Relacionado > Grupos NSGroup**.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Grupos > Agregar**.
- 3 Introduzca un nombre para el grupo NSGroup.
- 4 (opcional) Escriba una descripción.
- 5 (opcional) Haga clic en **Criterios de pertenencia**.

Para cada criterio, puede especificar hasta cinco reglas, que se combinen con el operador AND lógico. El criterio de miembro disponible puede aplicarse a lo siguiente:

- **Puerto lógico:** puede especificar una etiqueta y un ámbito opcional.
- **Conmutador lógico:** puede especificar una etiqueta y un ámbito opcional.
- **Máquina Virtual:** puede especificar un nombre, una etiqueta, un nombre de sistema operativo de equipo o un nombre de equipo que coincida con una cadena específica, que no coincida con ella, que la contenga, o que comience o termine con ella.
- **Nodo de transporte:** puede especificar un tipo de nodo que equivalga a un nodo de Edge o un nodo de host.
- **Conjunto de direcciones IP:** puede especificar una etiqueta y, opcionalmente, un ámbito.

6 (opcional) Haga clic en **Miembros** para seleccionar miembros.

Los tipos de miembro disponibles son:

- **Grupo de AD:** los grupos NSGroup con grupos ADGroup solo se pueden usar en el campo `extended_source` de una regla de firewall distribuido y deben ser los únicos miembros del grupo. Por ejemplo, no puede haber un grupo NSGroup con en el que ADGroup y IPSet sean miembros al mismo tiempo.
- **Conjunto de direcciones IP:** puede incluir direcciones IPv4 y direcciones IPv6.
- **Puerto lógico:** puede incluir direcciones IPv4 y direcciones IPv6.
- **Conmutador lógico:** puede incluir direcciones IPv4 y direcciones IPv6.
- **Conjunto de direcciones MAC**
- **Grupo NSGroup**
- **Nodo de transporte**
- **VIF**
- **Máquina virtual**

7 Haga clic en **AGREGAR**.

El grupo se agrega a la tabla de grupos. Haga clic en un nombre de grupo para que aparezca una descripción general y pueda editar la información de grupo, incluidos los criterios de pertenencia, los miembros, las aplicaciones y los grupos relacionados. Desplácese hasta la parte inferior de la pestaña **Información general** para agregar y eliminar etiquetas. Consulte [Agregar etiquetas a un objeto](#) para obtener más información. Al seleccionar **Relacionado> Grupos NSGroup**, se muestran todos los grupos NSGroup que tienen el grupo NSGroup seleccionado como miembro.

Configurar servicios y grupos de servicios

Puede configurar un servicio NSService y especificar parámetros del tráfico de red coincidente, como una vinculación de protocolos y puertos. También puede utilizar un servicio NSService para permitir o bloquear determinados tipos de tráfico en las reglas de firewall.

Un servicio NSService puede ser de los siguientes tipos:

- Ethernet
- IP
- IGMP
- ICMP
- ALG
- Conjunto de puertos de Capa 4

Un conjunto de puertos de Capa 4 admite la identificación de puertos de origen y de destino. Puede especificar puertos individuales o un rango de puertos con un máximo de 15 puertos.

Un servicio NSService también puede ser un grupo de otros servicios NSService. Un servicio NSService que sea un grupo puede ser de los siguientes tipos:

- Capa 2
- Capa 3 y superior

No puede cambiar el tipo después de crear un servicio NSService. Algunos servicios NSService están predefinidos. No puede modificarlos ni eliminarlos.

Crear un servicio NSService

Puede crear un servicio NSService para especificar las características que utiliza la búsqueda de coincidencias de red, o bien para definir el tipo de tráfico que se debe bloquear o permitir en las reglas de firewall.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Servicios > Agregar**.
- 3 Introduzca un nombre.
- 4 (opcional) Escriba una descripción.
- 5 Seleccione **Especificar un protocolo** para configurar un servicio individual, o bien haga clic en **Agrupar servicios existentes** para configurar un grupo de servicios NSService.
- 6 En el caso de un servicio individual, seleccione un tipo de servicio y un protocolo.
Los tipos disponibles son **Ethernet**, **IP**, **IGMP**, **ICMP**, **ALG** y **Conjunto de puertos de Capa 4**.
- 7 En el caso de un grupo de servicios, seleccione un tipo y los miembros del grupo.
Los tipos disponibles son **Capa 2** y **Capa 3 y superior**.
- 8 Haga clic en **AGREGAR**.

Administrar las etiquetas de una máquina virtual

Puede ver la lista de máquinas virtuales en el inventario. También puede agregar etiquetas a una máquina virtual para facilitar las búsquedas.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Máquinas virtuales** en el panel de navegación.

Se muestra la lista de máquinas virtuales con cuatro columnas: Máquina virtual, ID externo, Origen y Etiqueta. Haga clic en el icono de filtro del encabezado de las tres primeras columnas para filtrar la lista. Introduzca una cadena de caracteres para buscar una coincidencia parcial. Si la cadena en la columna contiene la cadena que introdujo, se muestra la entrada. Introduzca una cadena de caracteres entre comillas dobles para buscar una coincidencia exacta. Si la cadena en la columna coincide exactamente con la cadena que introdujo, se muestra la entrada.


- 3 Seleccione **Inventario > Máquinas virtuales** en el panel de navegación.
- 4 Seleccione una máquina virtual.
- 5 Haga clic en **ADMINISTRAR ETIQUETAS**.
- 6 Agregue o elimine etiquetas.

Opción	Acción
Agregar una etiqueta	Haga clic en AGREGAR para especificar una etiqueta y, de forma opcional, un ámbito.
Eliminar una etiqueta	Seleccione una etiqueta y haga clic en ELIMINAR .

El número máximo de etiquetas que se pueden asignar desde NSX Manager a una máquina virtual es de 25. El número máximo de etiquetas para todos los demás objetos administrados, como los conmutadores lógicos o puertos, es de 30.

- 7 Haga clic en **Guardar**.

Puede configurar DHCP desde la pestaña **Opciones avanzadas de redes y seguridad**.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Este capítulo incluye los siguientes temas:

- [DHCP](#)
- [Servidores proxy de metadatos](#)

DHCP

El Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) permite a los clientes obtener de forma automática la configuración de la red, como direcciones IP, máscara de subred, puerta de enlace predeterminada y configuración de DNS desde un servidor DHCP.

Puede crear servidores DHCP para gestionar solicitudes DHCP y crear servicios de retransmisión DHCP para retransmitir tráfico DHCP a servidores DHCP externos. Sin embargo, no debe configurar un servidor DHCP en un conmutador lógico y también configurar un servicio de retransmisión DHCP en el puerto de enrutador al que se conecta el mismo conmutador lógico. En tal caso, las solicitudes DHCP solo se dirigirían al servicio de retransmisión DHCP.

Si configura los servidores DHCP, para mejorar la seguridad, configure una regla DFW para permitir el tráfico en los puertos UDP 67 y 68 solo para direcciones IP de servidor DHCP.

Nota Una regla DFW que tenga `Logical Switch/Logical Port/NSGroup` como el origen, `Any` como el destino y se configura para colocar paquetes DHCP para los puertos 67 y 68, no podrá bloquear el tráfico DHCP. Para bloquear el tráfico DHCP, configure `Any` como origen y destino.

En esta versión, el servidor DHCP no admite el etiquetado de VLAN invitado.

Crear un perfil de servidor DHCP

Un perfil de servidor DHCP especifica un clúster de NSX Edge o miembros de un clúster de NSX Edge. Un servidor DHCP con este perfil atiende las solicitudes DHCP de las VM en conmutadores lógicos conectados a los nodos de NSX Edge que se especifican en el perfil.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Perfiles de servidor > Agregar**.
- 3 Escriba un nombre y una descripción opcional.
- 4 Seleccione un clúster de NSX Edge del menú desplegable.
- 5 (opcional) Seleccione miembros del clúster de NSX Edge.
Puede especificar hasta 2 miembros.

Pasos siguientes

Cree un servidor DHCP. Consulte [Crear un servidor DHCP](#).

Crear un servidor DHCP

Puede crear servidores DHCP para atender a las solicitudes DHCP de VM conectadas a conmutadores lógicos.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Servidores > Agregar**.
- 3 Escriba un nombre y una descripción opcional.
- 4 Introduzca la dirección IP del servidor DHCP y su máscara de subred en formato CIDR.
Por ejemplo, escriba `192.168.1.2/24`.
- 5 (Requerido) Seleccione un perfil DHCP en el menú desplegable.
- 6 (opcional) Introduzca las opciones comunes, como nombre de dominio, puerta de enlace predeterminada, servidores DNS y máscara de subred.
- 7 (opcional) Introduzca las opciones de ruta estática sin clase.
- 8 (opcional) Introduzca otras opciones.
- 9 Haga clic en **Guardar**.
- 10 Seleccione el servidor DHCP que se acaba de crear.

- 11 Expanda la sección Grupos de direcciones IP.
- 12 Haga clic en **Agregar** para agregar rangos de direcciones IP, puerta de enlace predeterminada, duración de la concesión, umbral de error, opción de ruta estática sin clase y otras opciones.
- 13 Expanda la sección Enlaces estáticos.
- 14 Haga clic en **Agregar** para agregar enlaces estáticos entre direcciones MAC y direcciones IP, puerta de enlace predeterminada, nombre de host, duración de la concesión, opción de ruta estática sin clase y otras opciones.

Pasos siguientes

Adjunte un servidor DHCP a un conmutador lógico. Consulte [Adjuntar un servidor DHCP a un conmutador lógico](#).

Adjuntar un servidor DHCP a un conmutador lógico

Debe adjuntar un servidor DHCP a un conmutador lógico antes que el servidor DHCP pueda procesar las solicitudes DHCP de las máquinas virtuales conectadas al conmutador.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación**.
 - a Haga clic en la casilla de verificación de un conmutador lógico.
 - b Haga clic en **Acciones > Adjuntar un servidor DHCP**.
- 3 También puede seleccionar **Opciones avanzadas de redes y seguridad > DHCP**.
 - a Haga clic en la pestaña **Servidores**.
 - b Haga clic en la casilla de verificación de un servidor DHCP.
 - c Haga clic en **Acciones > Asociar a conmutador lógico**.

Desasociar un servidor DHCP de un conmutador lógico

Puede desasociar un servidor DHCP de un conmutador lógico para volver a configurar el entorno.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Conmutación**.
- 3 Haga clic en el conmutador lógico del que quiera desasociar un servidor DHCP.
- 4 Haga clic en **Acciones > Desasociar servidor DHCP**.

Crear un perfil de retransmisión DHCP

Un perfil de retransmisión DHCP especifica uno o varios servidores DHCP o DHCPv6 externos. Al crear un servicio de retransmisión DHCP o DHCPv6, debe especificar un perfil de retransmisión DHCP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Perfiles de retransmisión > Agregar**.
- 3 Escriba un nombre y una descripción opcional.
- 4 Introduzca una o varias direcciones de servidores DHCP o DHCPv6 externos.

Pasos siguientes

Cree un servicio de retransmisión DHCP o DHCPv6. Consulte [Crear un servicio de retransmisión DHCP](#).

Crear un servicio de retransmisión DHCP

Puede crear un servicio de retransmisión DHCP para retransmitir el tráfico entre clientes y servidores DHCP que no se crearon en NSX-T Data Center.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Servicios de retransmisión > Agregar**.
- 3 Escriba un nombre y una descripción opcional.
- 4 Seleccione un perfil de retransmisión DHCP en el menú desplegable.

Pasos siguientes

Agregue un servicio DHCP a un puerto del enrutador lógico. Consulte [Agregar un servicio de retransmisión de DHCP a un puerto de enrutador lógico](#).

Agregar un servicio de retransmisión de DHCP a un puerto de enrutador lógico

Puede agregar un servicio de retransmisión de DHCP a un puerto del enrutador lógico. Las máquinas virtuales del conmutador lógico conectadas a ese puerto se pueden comunicar con los servidores DHCP configurados en el servicio de retransmisión.

Requisitos previos

- Compruebe que el servicio relé DHCP esté configurado. Consulte [Crear un servicio de retransmisión DHCP](#).
- Compruebe que el puerto del enrutador sea del tipo **Vínculo inferior**.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Seleccione el enrutador adecuado para mostrar más información y opciones de configuración.
- 4 Seleccione **Configuración > Puertos del enrutador**.
- 5 Seleccione el puerto de enrutador que esté conectado al conmutador lógico deseado y haga clic en **Editar**.
- 6 Seleccione un servicio relé DHCP en la lista desplegable **Servicio de retransmisión** y haga clic en **Guardar**.

También es posible seleccionar un servicio relé DHCP al agregar un puerto de enrutador lógico nuevo.

Eliminar una concesión de DHCP

Le recomendamos eliminar una concesión de DHCP en ciertos casos, como, por ejemplo, si quiere que un cliente DHCP obtenga una dirección IP diferente o si un cliente se desconecta sin emitir su dirección IP y quiere que esa dirección esté disponible para otros clientes.

Puede utilizar la siguiente API para eliminar una concesión de DHCP:

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```

Para asegurarse de eliminar la concesión correcta, utilice la siguiente llamada API antes y después de la API DELETE:

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

Después usar la llamada de API DELETE, asegúrese de que los resultados de la API GET no muestren la concesión eliminada.

Para obtener más información, consulte la *Referencia de API de NSX-T Data Center*.

Servidores proxy de metadatos

Un servidor proxy de metadatos permite a las instancias de la máquina virtual recuperar metadatos de instancias específicas de un servidor de la API OpenStack Nova.

Los siguientes pasos indican el funcionamiento de un servidor proxy de metadatos:

- 1 Una máquina virtual envía una solicitud HTTP GET a `http://169.254.169.254:80` para solicitar algunos metadatos.
- 2 El servidor proxy de metadatos conectado al mismo conmutador lógico que la máquina virtual lee la solicitud, realiza los cambios necesarios en los encabezados y reenvía la solicitud al servidor de la API Nova.
- 3 El servidor de la API Nova solicita y recibe información sobre la máquina virtual del servidor Neutron.
- 4 El servidor de la API Nova busca los metadatos y los envía al servidor proxy de metadatos.
- 5 El servidor proxy de metadatos reenvía los metadatos a la máquina virtual.

Un servidor proxy de metadatos se ejecuta en un nodo de NSX Edge. Para obtener una alta disponibilidad, puede configurar el servidor proxy de metadatos para que se ejecute en dos o más nodos de NSX Edge de un clúster de NSX Edge.

Agregar un servidor proxy de metadatos

Un servidor proxy de metadatos permite a las máquinas virtuales recuperar metadatos de un servidor API OpenStack Nova.

Requisitos previos

Compruebe que haya creado un clúster de NSX Edge. Para obtener más información, consulte *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Servidores proxy de metadatos > Agregar**.
- 3 Escriba un nombre para el servidor proxy de metadatos.
- 4 (opcional) Escriba una descripción.
- 5 Introduzca la URL y el puerto para el servidor Nova.
El rango de puerto válido se encuentra entre 3000 y 9000.
- 6 Introduzca un valor para **Secreto**.
- 7 Seleccione un clúster de NSX Edge de la lista desplegable.
- 8 (opcional) Seleccione miembros del clúster de NSX Edge.

Pasos siguientes

Adjunte el servidor proxy de metadatos a un conmutador lógico.

Asociar un servidor proxy de metadatos a un conmutador lógico

Para proporcionar servicios proxy de metadatos en máquinas virtuales conectadas a un conmutador lógico, debe adjuntar un servidor proxy de metadatos al conmutador.

Requisitos previos

Compruebe que creó un conmutador lógico. Para obtener más información, consulte [Crear un conmutador lógico](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Servidores proxy de metadatos**.
- 3 Seleccione un servidor proxy de metadatos.
- 4 Seleccione la opción en el menú **Acciones > Asociar a conmutador lógico**.
- 5 Seleccione un conmutador lógico de la lista desplegable.

Resultados

También es posible conectar un servidor proxy de metadatos a un conmutador lógico si se dirige a **Conmutación > Conmutadores**, seleccione un conmutador y la opción de menú **Acciones > Asociar servidor proxy de metadatos**.

Desconectar un servidor proxy de metadatos de un conmutador lógico

Para dejar de suministrar servicios de proxy de metadatos a máquinas virtuales conectadas a un conmutador lógico o utilizar un servidor proxy de metadatos diferente, puede desconectar un servidor proxy de metadatos desde un conmutador lógico.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > DHCP > Servidores proxy de metadatos**.
- 3 Seleccione un servidor proxy de metadatos.
- 4 Seleccione la opción de menú **Acciones > Desasociar de conmutador lógico**.
- 5 Seleccione un conmutador lógico de la lista desplegable.


Resultados

También puede desconectar un servidor proxy de metadatos de un conmutador lógico accediendo a **Conmutación > Conmutadores**, seleccionando un conmutador y a continuación seleccionando la opción de menú **Acciones > Desconectar servidor proxy de metadatos**.

Administración de direcciones IP avanzada

18

Gracias a la administración de direcciones IP (IP address management, IPAM), puede crear bloques de IP para admitir NSX Container Plug-in (NCP). Para obtener más información sobre NCP, consulte *Guía de instalación y administración de NSX-T Container Plug-in para Kubernetes*.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Este capítulo incluye los siguientes temas:

- [Administrar los bloques de IP](#)
- [Administrar subredes para bloques de IP](#)

Administrar los bloques de IP

Para configurar NSX Container Plug-in, es necesario que cree bloques de IP para los contenedores.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > IPAM**.
- 3 Para agregar un bloque de IP, haga clic en **Agregar**.
 - a Introduzca un nombre y, si lo desea, una descripción.
 - b Introduzca un bloque de IP en formato CIDR. Por ejemplo, 10.10.10.0/24.
- 4 Para editar un bloque de IP, haga clic en el nombre.
 - a En la pestaña **Información general**, haga clic en **Editar**.

Puede cambiar el nombre, la descripción o el valor del bloque de IP.

- 5 Para administrar las etiquetas de un bloque de IP, haga clic en el nombre.
 - a En la pestaña **Información general**, haga clic en **Administrar**.
Puede agregar o eliminar etiquetas.
- 6 Para eliminar uno o varios bloques de IP, selecciónelos.
 - a Haga clic en **Eliminar**.
No puede eliminar un bloque de IP que tenga una subred asignada.

Administrar subredes para bloques de IP

Puede agregar o eliminar subredes para bloques de IP.

Procedimiento


- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > IPAM**.
- 3 Haga clic en el nombre de un bloque de IP.
- 4 Haga clic en la pestaña **Subredes**.
- 5 Para agregar una subred, haga clic en **Agregar**.
 - a Introduzca un nombre y, si lo desea, una descripción.
 - b Introduzca el tamaño de la subred.
- 6 Para eliminar una o varias subredes, selecciónelas.
 - a Haga clic en **Eliminar**.

Equilibrio de carga avanzado

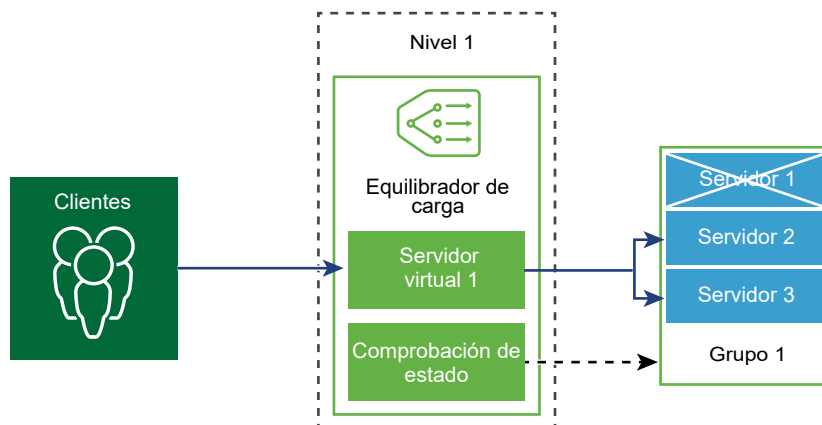
19

Esta información abarca la configuración de equilibrio de carga de NSX-T Data Center que se encuentra en la pestaña **Opciones avanzadas de redes y seguridad**.

Para obtener información sobre el equilibrador de carga avanzado de NSX (redes AVI), consulte <https://www.vmware.com/products/nsx-advanced-load-balancer.html>.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

El equilibrador de carga lógico NSX-T Data Center ofrece servicios de alta disponibilidad para aplicaciones y distribuye la carga de tráfico de red entre varios servidores.



El equilibrador de carga distribuye las solicitudes de servicio entrantes de manera uniforme entre varios servidores de forma tal que la distribución de carga sea transparente para los usuarios. El equilibrio de carga ayuda a lograr una utilización de recursos óptima, maximizar la capacidad de proceso, minimizar el tiempo de respuesta y evitar la sobrecarga.

Puede asignar una dirección IP virtual a un conjunto de servidores de grupo para equilibrio de carga. El equilibrador de carga acepta las solicitudes TCP, UDP, HTTP o HTTPS en la dirección IP virtual y decide qué grupo de servidores se va a utilizar.

Según las necesidades de su entorno, puede ampliar el rendimiento del equilibrador de carga mediante el aumento de los servidores virtuales y los miembros del grupo existentes para controlar el tráfico de red intenso.

Nota El equilibrador de carga lógico solo se admite en el enrutador lógico de nivel 1. Un equilibrador de carga solo puede asociarse a un enrutador lógico de nivel 1.

Este capítulo incluye los siguientes temas:

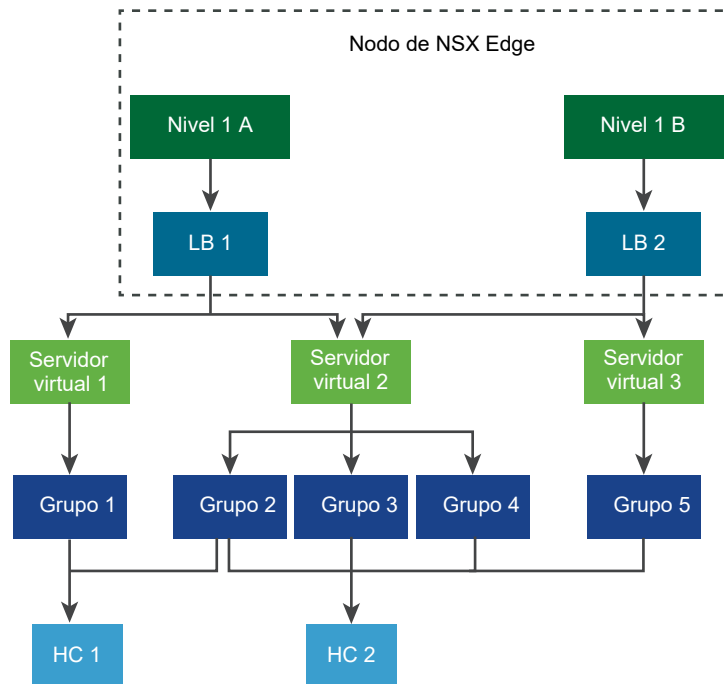
- [Conceptos clave sobre el equilibrador de carga](#)
- [Configurar componentes del equilibrador de carga](#)

Conceptos clave sobre el equilibrador de carga

El equilibrador de carga incluye servidores virtuales, grupos de servidores y monitores de comprobación de estado.

Un equilibrador de carga se conecta a un enrutador lógico de nivel 1. El equilibrador de carga aloja uno o varios servidores virtuales. Un servidor virtual es un resumen de un servicio de aplicación, representado por una combinación única de IP, puerto y protocolo. El servidor virtual está asociado a uno o varios grupos de servidores. Un grupo de servidores consta de varios servidores. Los grupos de servidores incluyen miembros de grupo de servidores individuales.

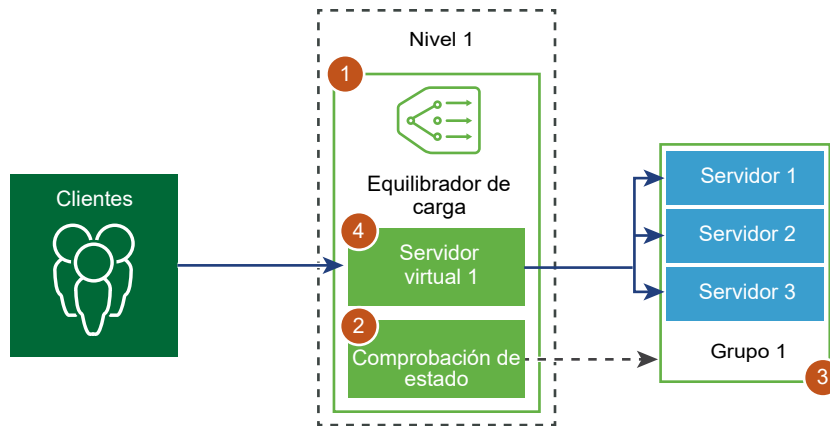
Para determinar si cada servidor ejecuta correctamente la aplicación, puede agregar monitores de comprobación de estado que comprueben el estado de mantenimiento de un servidor.



Configurar componentes del equilibrador de carga

Para utilizar equilibradores de carga lógicos, primero debe configurar un equilibrador de carga y asociarlo a un enrutador lógico de nivel 1.

A continuación, podrá configurar la supervisión de comprobación de estado para los servidores. Después debe configurar grupos de servidores para el equilibrador de carga. Por último, debe crear un servidor virtual de capa 4 o capa 7 para el equilibrador de carga.

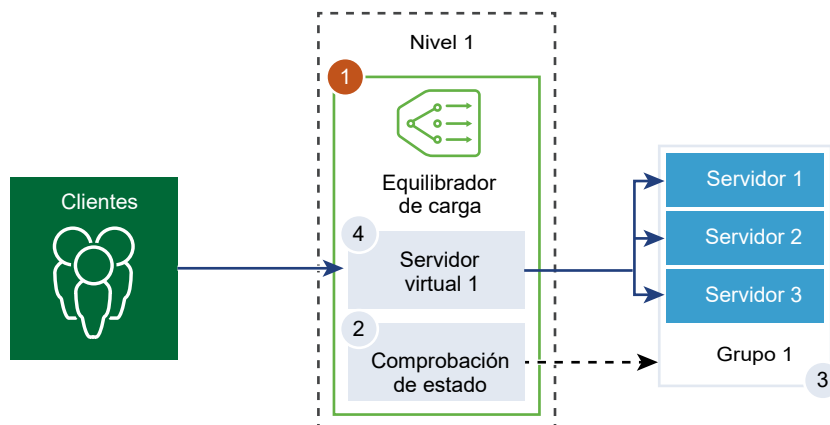


Crear un equilibrador de carga

El equilibrador de carga se crea y se asocia al enrutador lógico de nivel 1.

Puede configurar el nivel de mensajes de error que desea que el equilibrador de carga agregue al registro de errores.

Nota Evite establecer el nivel de registro como **DEPURACIÓN** en los equilibradores de carga con tráfico pesado debido al número de mensajes impresos en el registro que afectan al rendimiento.



Requisitos previos

Compruebe que el enrutador lógico de nivel 1 esté configurado. Consulte [Crear un enrutador lógico de nivel 1](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Agregar**.
- 3 Introduzca un nombre y una descripción para el equilibrador de carga.
- 4 Seleccione el tamaño del servidor virtual del equilibrador de carga y la cantidad de miembros de grupo en función de los recursos disponibles.
- 5 En el menú desplegable, defina el nivel de gravedad del registro de errores.
El equilibrador de carga recopila información sobre problemas de distintos niveles de gravedad detectados en el registro de errores.
- 6 Haga clic en **Aceptar**.
- 7 Asocie el equilibrador de carga recién creado a un servidor virtual.
 - a Seleccione el equilibrador de carga y haga clic en **Acciones > Asociar a un servidor virtual**.
 - b Seleccione un servidor virtual del menú desplegable.
 - c Haga clic en **Aceptar**.
- 8 Asocie el equilibrador de carga recién creado a un enrutador lógico de nivel 1.
 - a Seleccione el equilibrador de carga y haga clic en **Acciones > Asociar a un enrutador lógico**.
 - b Seleccione un enrutador lógico de nivel 1 existente del menú desplegable.
El enrutador de nivel 1 debe estar en el modo activo-en espera.
 - c Haga clic en **Aceptar**.
- 9 (opcional) Elimine el equilibrador de carga.
Si ya no desea utilizar el equilibrador de carga, primero debe separarlo del servidor virtual y del enrutador lógico de nivel 1.

Configurar un monitor de estado activo

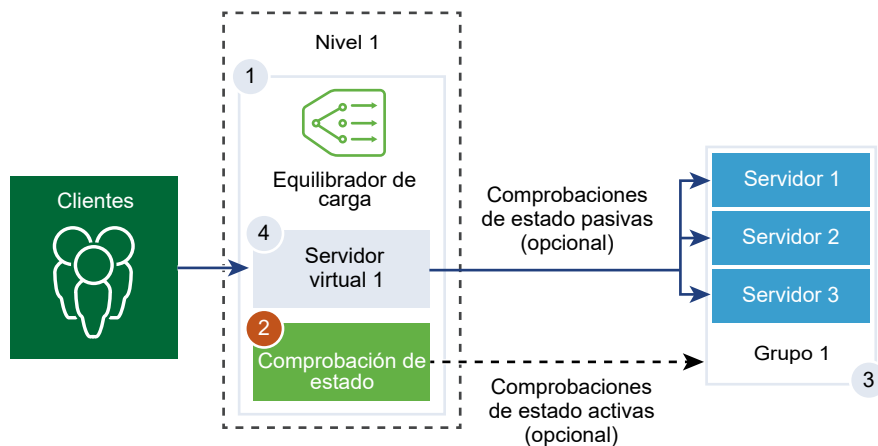
El monitor de estado activo se utiliza para comprobar si un servidor está disponible. El monitor de estado activo utiliza varios tipos de pruebas, como el envío de un ping básico a los servidores o solicitudes HTTP avanzadas para supervisar el estado de la aplicación.

Los servidores que no responden en un periodo de tiempo específico o bien responden con errores, se excluyen del posterior manejo de conexiones hasta que una comprobación de estado periódica efectuada más adelante confirma que funcionan correctamente.

Las comprobaciones de estado activas se realizan en miembros de un grupo de servidores después de asociar el miembro del grupo a un servidor virtual y de asociar dicho servidor virtual a una puerta de enlace de nivel 1 (lo que antes se denominaba enrutador lógico de nivel 1).

Si la puerta de enlace de nivel 1 está conectada a una puerta de enlace de nivel 0, se crea un puerto de vínculo de enrutador y su dirección IP (normalmente en el formato 100.64.x.x) se utiliza para realizar la comprobación de estado del servicio del equilibrador de carga. Si la puerta de enlace de nivel 1 es independiente (si tiene solo un puerto de servicio centralizado y no está conectada a una puerta de enlace de nivel 0), se utilizará la dirección IP del puerto de servicio centralizado para realizar la comprobación de estado del servicio del equilibrador de carga. Consulte [Crear un enrutador lógico de nivel 1 independiente](#) para obtener información sobre las puertas de enlace independientes de nivel 1.

Nota Se puede configurar un monitor de estado activo por grupo de servidores.



Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Monitores > Monitores de estado activo > Agregar**.
- 3 Introduzca un nombre y una descripción para el monitor de estado activo.
- 4 En el menú desplegable, seleccione un protocolo de comprobación de estado para el servidor.
También puede utilizar los protocolos predefinidos en NSX Manager; `http-monitor`, `https-monitor`, `Icmp-monitor`, `Tcp-monitor` y `Udp-monitor`.
- 5 Defina el valor del puerto de supervisión.

6 Configure los valores para supervisar un grupo de servicios.

También puede aceptar los valores predeterminados del monitor de estado activo.

Opción	Descripción
Intervalo de supervisión	Establezca los segundos que tarda el monitor en enviar otra solicitud de conexión al servidor.
Recuento de errores	Establezca un valor de errores consecutivos a partir del cual el servidor se considere temporalmente no disponible.
Recuento de subida	Establezca un número que indique el periodo de tiempo que se debe esperar para volver a intentar una nueva conexión con el servidor y comprobar si este está disponible.
Período de tiempo de espera	Establezca el número de veces que se probará el servidor antes de considerarlo como INACTIVO.

Por ejemplo, si el intervalo de supervisión se establece como 5 segundos y el tiempo de espera como 15 segundos, el equilibrador de carga envía solicitudes al servidor cada 5 segundos. En cada sondeo, si la respuesta esperada se recibe del servidor en un plazo de 15 segundos, el resultado de la comprobación de estado será CORRECTO. En caso contrario, el resultado será CRÍTICO. Si los resultados de las tres comprobaciones de estado recientes indican ACTIVO, el servidor se considera ACTIVO.

7 Si selecciona HTTP como el protocolo de comprobación de estado, complete la siguiente información.

Opción	Descripción
Método HTTP	Seleccione el método para detectar el estado del servidor en el menú desplegable: GET, OPTIONS, POST, HEAD y PUT.
URL de solicitud HTTP	Introduzca el URI de la solicitud para el método.
Versión de solicitud HTTP	En el menú desplegable, seleccione la versión de solicitud compatible. También puede aceptar la versión predeterminada: HTTP_VERSION_1_1.
Cuerpo de solicitud HTTP	Introduzca el cuerpo de la solicitud. Válido para los métodos POST y PUT.
Código de respuesta HTTP	Introduzca la cadena de la cual el monitor espera encontrar una coincidencia en la línea de estado del cuerpo de la respuesta HTTP. El código de respuesta es una lista separada por comas. Por ejemplo, 200, 301, 302, 401.
Cuerpo de respuesta HTTP	Si la cadena del cuerpo de respuesta HTTP y el cuerpo de la respuesta de la comprobación de estado HTTP coinciden, se considerará que el servidor funciona correctamente.

- 8 Si selecciona HTTPS como el protocolo de comprobación de estado, complete la siguiente información.

- a Seleccione la lista de protocolos SSL.

Las versiones TLS1.1 y TLS1.2 son compatibles y están habilitadas de forma predeterminada. Se admite la versión TLS1.0, pero está deshabilitada de forma predeterminada.

- b Haga clic en la flecha y mueva los protocolos a la sección seleccionada.
- c Asigne un cifrado SSL predeterminado o cree un cifrado SSL personalizado.
- d Complete los siguientes detalles para HTTP como protocolo de comprobación de estado.

Opción	Descripción
Método HTTP	Seleccione el método para detectar el estado del servidor en el menú desplegable: GET, OPTIONS, POST, HEAD y PUT.
URL de solicitud HTTP	Introduzca el URI de la solicitud para el método.
Versión de solicitud HTTP	En el menú desplegable, seleccione la versión de solicitud compatible. También puede aceptar la versión predeterminada: HTTP_VERSION_1_1.
Cuerpo de solicitud HTTP	Introduzca el cuerpo de la solicitud. Válido para los métodos POST y PUT.
Código de respuesta HTTP	Introduzca la cadena de la cual el monitor espera encontrar una coincidencia en la línea de estado del cuerpo de la respuesta HTTP. El código de respuesta es una lista separada por comas. Por ejemplo, 200, 301, 302, 401.
Cuerpo de respuesta HTTP	Si la cadena del cuerpo de respuesta HTTP y el cuerpo de la respuesta de la comprobación de estado HTTP coinciden, se considerará que el servidor funciona correctamente.

- 9 Si selecciona ICMP como el protocolo de comprobación de estado, asigne el tamaño de los datos en bytes del paquete de comprobación de estado ICMP.
- 10 Si selecciona TCP como el protocolo de comprobación de estado, puede dejar los parámetros vacíos.

Si no se muestran los enviados y los esperados, se establece una conexión TCP de protocolo de enlace triple para validar el estado del servidor. No se enviarán datos. Si se muestran los datos esperados, estos deben ser cadenas y pueden encontrarse en cualquier lugar de la respuesta. No se admiten expresiones regulares.

- 11 Si selecciona UDP como el protocolo de comprobación de estado, complete la siguiente información obligatoria.

Opción obligatoria	Descripción
Datos de UDP enviados	Introduzca la cadena que se enviará al servidor después de establecer una conexión.
Datos de UDP esperados	Introduzca la cadena que se espera recibir del servidor. El servidor solo se considerará ACTIVO si la cadena recibida coincide con esta definición.

- 12 Haga clic en **Finalizar**.

Pasos siguientes

Asocie el monitor de estado activo a un grupo de servidores. Consulte [Agregar un grupo de servidores para el equilibrio de carga](#).

Configurar los monitores de estado pasivos

Los equilibradores de carga realizan comprobaciones de estado pasivas para supervisar errores durante las conexiones de cliente y marcar los servidores que generan errores constantes y muestran el estado INACTIVO.

La comprobación de estado pasiva supervisa el tráfico de cliente que pasa a través del equilibrador de carga para ver si tiene errores. Por ejemplo, si un miembro del grupo envía un restablecimiento (Reset, RST) de TCP en respuesta a una conexión de cliente, el equilibrador de carga detecta dicho error. Si se producen varios errores consecutivos, el equilibrador de carga considera que ese miembro del grupo de servidores no está disponible temporalmente y deja de enviarle solicitudes de conexión durante un tiempo. Después de cierto tiempo, el equilibrador de carga envía una solicitud de conexión para comprobar si el miembro del grupo se recuperó. Si esa conexión es correcta, el miembro del grupo se considera en buen estado. De lo contrario, el equilibrador de carga espera un momento y vuelve a intentarlo.

La comprobación de estado pasiva considera los siguientes escenarios como errores en el tráfico de cliente.

- En el caso de los grupos de servidores asociados con servidores virtuales de capa 7, si se produce un error en la conexión con el miembro del grupo. Por ejemplo, si se produce un error cuando el miembro del grupo envía un TCP RST cuando el equilibrador de carga intenta conectarse o realizar un protocolo de enlace SSL entre el equilibrador de carga y el miembro del grupo.
- En el caso de los grupos de servidores asociados con servidores virtuales de TCP de capa 4, si el miembro del grupo envía un TCP RST en respuesta al TCP SYN de cliente o no responde.
- En el caso de los grupos de servidores asociados con servidores virtuales de UDP de capa 4, si se recibe un mensaje de error ICMP que indica que no se puede acceder a un puerto o a un destino en respuesta a un paquete UDP de cliente.

En los grupos de servidores asociados a servidores virtuales de capa 7, el número de errores en la conexión se incrementa cuando se producen errores de conexión de TCP; por ejemplo, se producen errores de TCP RST para el envío de datos o errores de protocolo de enlace SSL.

En los grupos de servidores asociados con servidores virtuales de capa 4, si no se recibe ninguna respuesta a un TCP SYN enviado al miembro del grupo de servidores o si se recibe un TCP RST en respuesta a un TCP SYN, el miembro del grupo de servidores se considera como INACTIVO. Se incrementa el número de errores.

En el caso de los servidores virtuales de UDP de capa 4, si se recibe un error ICMP (por ejemplo, puerto o destino inaccesible) en respuesta al tráfico de cliente, se considera el miembro como INACTIVO.

Nota Puede configurar un monitor de estado pasivo por grupo de servidores.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Monitores > Monitores de estado pasivo > Agregar**.
- 3 Introduzca un nombre y una descripción para el monitor de estado pasivo.
- 4 Configure los valores para supervisar un grupo de servicios.

También puede aceptar los valores predeterminados del monitor de estado activo.

Opción	Descripción
Recuento de errores	Establezca un valor de errores consecutivos a partir del cual el servidor se considere temporalmente no disponible.
Período de tiempo de espera	Establezca el número de veces que se probará el servidor antes de considerarlo como INACTIVO.

Por ejemplo, cuando los errores consecutivos alcanzan el valor configurado 5, ese miembro se considera como no disponible temporalmente durante 5 segundos. Tras este período, el miembro se volverá a probar con una nueva conexión para ver si está disponible. Si esa conexión es correcta, se considera que el miembro está disponible y el número de errores se establece en cero. Sin embargo, si se produce un error de conexión, el miembro no se utiliza durante otro intervalo de tiempo de espera de 5 segundos.

- 5 Haga clic en **Aceptar**.

Pasos siguientes

Asocie el monitor de estado pasivo con un grupo de servidores. Consulte [Agregar un grupo de servidores para el equilibrio de carga](#).

Agregar un grupo de servidores para el equilibrio de carga

Un grupo de servidores se compone de uno o varios servidores configurados que ejecutan la misma aplicación. Un solo grupo puede asociarse a servidores virtuales de capa 4 y capa 7.

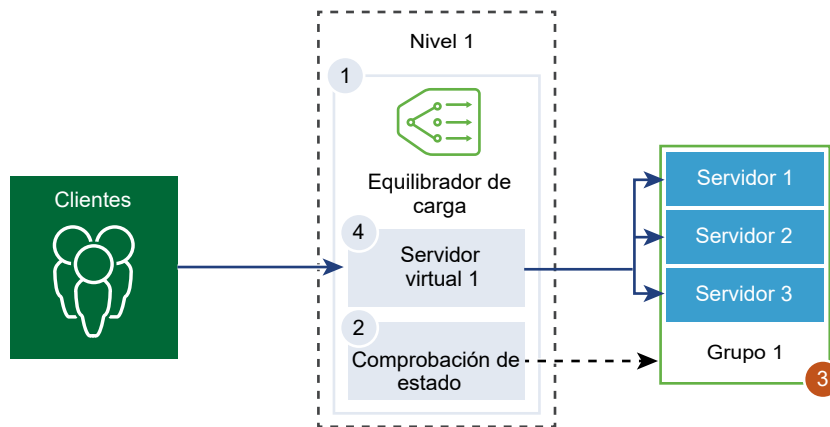
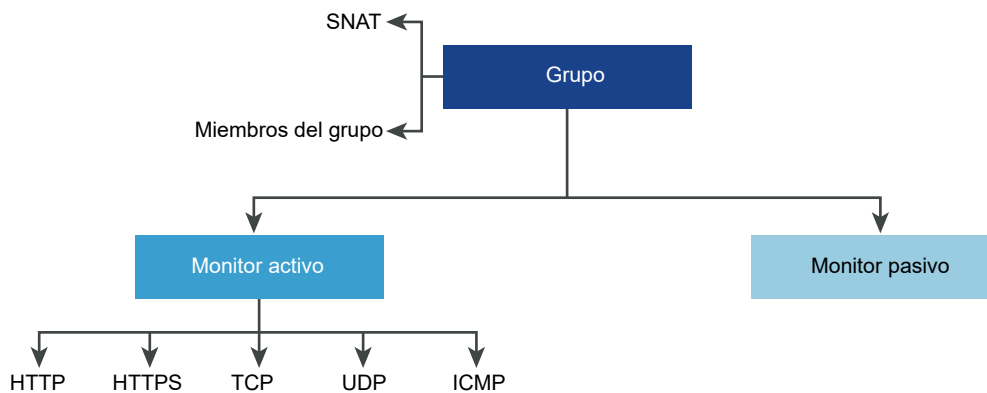


Figura 19-1. Configuración de los parámetros de grupo de servidores



Requisitos previos

- Si usa miembros de grupo dinámico, debe configurar un grupo NSGroup. Consulte [Crear un grupo NSGroup](#).
- Según la supervisión que utilice, compruebe que los monitores de estado activos o pasivos estén configurados. Consulte [Configurar un monitor de estado activo](#) o [Configurar los monitores de estado pasivos](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Grupos de servidores > Agregar**.

3 Escriba un nombre y una descripción para el grupo de equilibradores de carga.

Opcionalmente, describa las conexiones que administra el grupo de servidores.

4 Seleccione el método de equilibrio de algoritmos del grupo de servidores.

El algoritmo de equilibrio de carga controla la manera en la que se distribuyen las conexiones entrantes entre los miembros. El algoritmo puede utilizarse en un grupo de servidores o directamente en un servidor.

Todos los algoritmos de equilibrio de carga omiten los servidores que cumplen con alguna de las siguientes condiciones:

- El estado de administrador está establecido como DESHABILITADO.
- El estado de administrador está establecido como DESHABILITADO_ESTABLE y no hay ninguna entrada de persistencia coincidente.
- El estado de la comprobación de estado activa o pasiva es INACTIVO.
- Se alcanzó el máximo de conexiones simultáneas del grupo de servidores.

Opción	Descripción
ROUND_ROBIN	Las solicitudes de clientes entrantes pasan por una lista de servidores disponibles capaces de gestionar la solicitud. Ignora la ponderación de los miembros del grupo de servidores, aunque se haya configurado.
WEIGHTED_ROUND_ROBIN	A cada servidor se le asigna un valor de ponderación que indica el rendimiento de ese servidor en relación con los demás servidores del grupo. El valor determina cuántas solicitudes de clientes se envían a un servidor en comparación con otros servidores del grupo. Este algoritmo de equilibrio de carga se centra en distribuir de forma equitativa la carga entre los recursos del servidor disponibles.
LEAST_CONNECTION	Se distribuyen las solicitudes de los clientes entre varios servidores según la cantidad de conexiones existentes en el servidor. Las conexiones nuevas se envían al servidor con menos conexiones. Ignora la ponderación de los miembros del grupo de servidores, aunque se haya configurado.
WEIGHTED_LEAST_CONNECTION	A cada servidor se le asigna un valor de ponderación que indica el rendimiento de ese servidor en relación con los demás servidores del grupo. El valor determina cuántas solicitudes de clientes se envían a un servidor en comparación con otros servidores del grupo. Este algoritmo de equilibrio de carga se centra en utilizar el valor de ponderación para distribuir la carga equitativamente entre los recursos disponibles del servidor. De forma predeterminada, el valor de ponderación es 1 si no está configurado y si el inicio lento está habilitado.
IP-HASH	Selecciona un servidor según un hash de la dirección IP de origen y el peso total de los servidores en ejecución.

- 5 Active el botón de multiplexación de TCP para habilitar este elemento de menú.

Con la multiplexación de TCP, es posible utilizar la misma conexión de TCP entre un equilibrador de carga y el servidor para enviar varias solicitudes de clientes de diferentes conexiones de TCP de clientes.

- 6 Establezca el número máximo de conexiones de multiplexación de TCP por grupo que se mantienen activas para enviar posteriores solicitudes de clientes.
- 7 Seleccione el modo de NAT de origen (Source NAT, SNAT).

En función de la topología, SNAT podría ser necesario para que el equilibrador de carga reciba el tráfico del servidor destinado al cliente. SNAT se puede habilitar por grupo de servidores.

Modo	Descripción
Modo transparente	El equilibrador de carga utiliza la suplantación de puerto y dirección IP del cliente al establecer conexiones con los servidores. No se necesita SNAT.
Modo de asignación automática	El equilibrador de carga utiliza el puerto efímero y la dirección IP de interfaz para continuar la comunicación con un cliente que inicialmente estaba conectado a uno de los puertos de escucha establecidos del servidor. Se necesita SNAT. Habilite la sobrecarga de puertos para permitir que la misma IP y el mismo puerto de SNAT se utilicen para varias conexiones si la tupla (IP de origen, puerto de origen, IP de destino, puerto de destino y protocolo IP) es exclusiva después de realizar el proceso de SNAT. También puede establecer el factor de sobrecarga de puertos para admitir el número máximo de veces que se puede utilizar un puerto de forma simultánea para varias conexiones.
Modo de lista de direcciones IP	Especifique un único rango de direcciones IP (por ejemplo, 1.1.1.1-1.1.1.10) que se utilizará para SNAT al conectarse a cualquiera de los servidores del grupo. De forma predeterminada, se utiliza el rango de puertos de 4000 a 64000 para todas las direcciones IP de SNAT configuradas. Los rangos de puertos de 1000 a 4000 están reservados para fines como las comprobaciones de estado y las conexiones iniciadas desde aplicaciones de Linux. Si existen varias direcciones IP, se seleccionarán mediante Round Robin. Habilite la sobrecarga de puertos para permitir que la misma IP y el mismo puerto de SNAT se utilicen para varias conexiones si la tupla (IP de origen, puerto de origen, IP de destino, puerto de destino y protocolo IP) es exclusiva después de realizar el proceso de SNAT. También puede establecer el factor de sobrecarga de puertos para admitir el número máximo de veces que se puede utilizar un puerto de forma simultánea para varias conexiones.

- 8 Seleccione los miembros del grupo de servidores.

Un grupo de servidores consta de uno o varios miembros del grupo. Cada miembro del grupo tiene una dirección IP y un puerto.

Cada miembro del grupo de servidores se puede configurar con una ponderación para usarla en el algoritmo de equilibrio de carga. La ponderación indica la cantidad de carga aproximada que puede gestionar un determinado miembro del grupo en relación con otros miembros del mismo grupo.

La designación de un miembro del grupo como miembro de respaldo funciona con el monitor de estado para proporcionar un estado activo/en espera. Si los miembros activos no cumplen la comprobación de estado, se producirá una conmutación por error de tráfico para los miembros de copia de seguridad.

Opción	Descripción
Estático	Haga clic en Agregar para incluir un miembro de grupo estático. También puede clonar un miembro del grupo estático existente.
Dinámico	Seleccione el grupo NSGroup en el menú desplegable. Los criterios de pertenencia del grupo de servidores se definen en el grupo. De forma opcional, puede definir la lista del máximo de direcciones IP del grupo.

- 9 Introduzca la cantidad mínima de miembros activos que siempre debe mantener el grupo de servidores.
- 10 Seleccione un monitor de estado activo y uno pasivo para el grupo de servidores en el menú desplegable.

Establecer un monitor de estado activo y pasivo para el grupo de servidores es opcional. Cuando se selecciona un monitor de estado activo y la puerta de enlace de nivel 1 está conectada a una puerta de enlace de nivel 0, se crea un puerto de vínculo de enrutador. La dirección IP del puerto de vínculo del enrutador (generalmente con el formato 100.64.x.x) se utiliza para realizar la comprobación de estado del servicio del equilibrador de carga. Si la puerta de enlace de nivel 1 es independiente (si tiene solo un puerto de servicio centralizado y no está conectada a una puerta de enlace de nivel 0), se utilizará la dirección IP del puerto de servicio centralizado para realizar la comprobación de estado del servicio del equilibrador de carga. Consulte [Crear un enrutador lógico de nivel 1 independiente](#) para obtener información sobre las puertas de enlace independientes de nivel 1.

Agregue una regla de firewall para permitir que la dirección IP realice la comprobación de estado del servicio del equilibrador de carga.

- 11 Haga clic en **Finalizar**.

Configuración de los componentes de servidor virtual

Con el servidor virtual, hay varios componentes que se pueden configurar, como perfiles de aplicaciones, perfiles persistentes y reglas de equilibrador de carga.

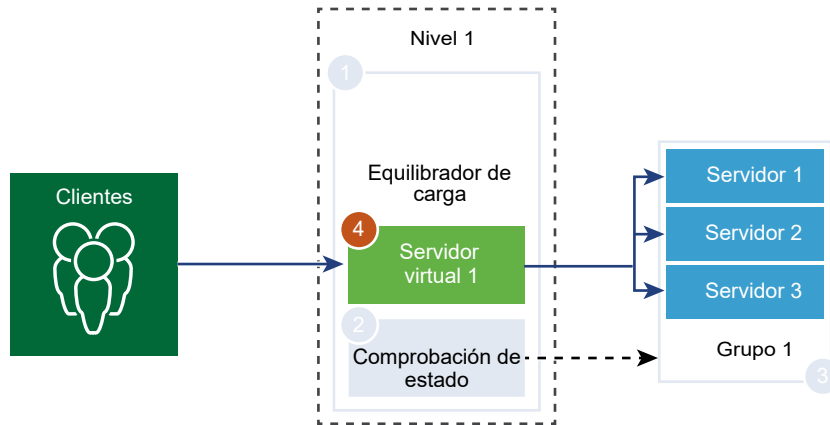
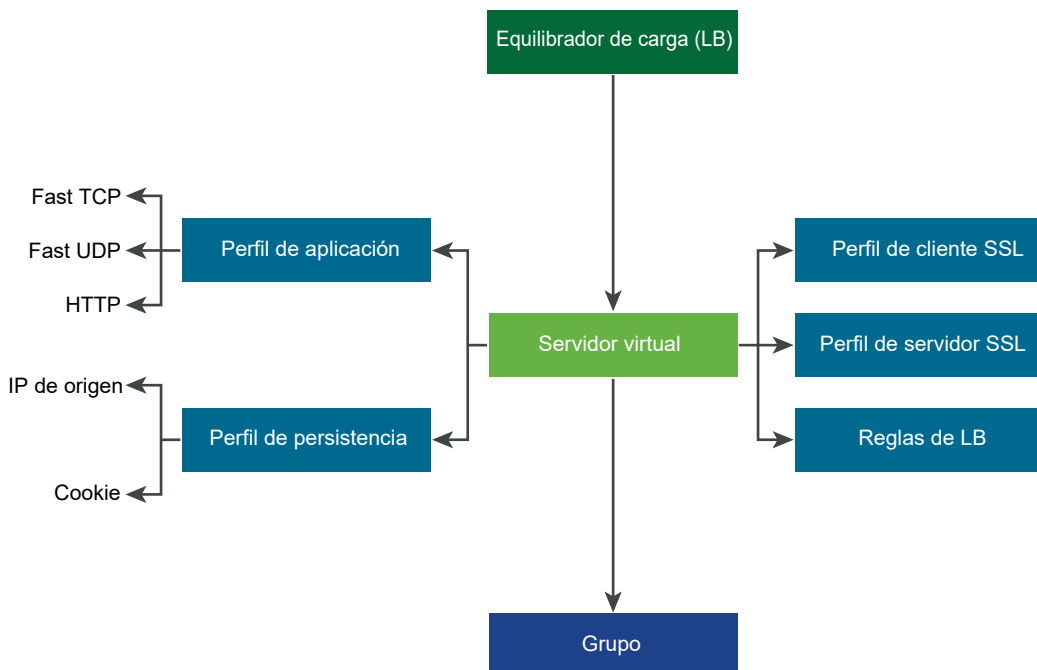


Figura 19-2. Componentes de servidor virtual



Configurar perfiles de aplicaciones

Los perfiles de aplicaciones se asocian con los servidores virtuales para mejorar el tráfico de red de equilibrio de carga y simplificar las tareas de administración de tráfico.

Los perfiles de aplicaciones definen el comportamiento de un tipo determinado de tráfico de red. El servidor virtual asociado procesa el tráfico de red según los valores especificados en el perfil de aplicación. Los tipos de perfiles de aplicaciones compatibles son FAST TCP, FAST UDP y HTTP.

El perfil de aplicación TCP se utiliza de forma predeterminada cuando no hay ningún perfil de aplicación asociado a un servidor virtual. Los perfiles de aplicaciones TCP y UDP se usan cuando una aplicación está en ejecución en un protocolo TCP o UDP y no requiere un equilibrio de carga de nivel de aplicación, como equilibrio de carga de dirección URL o HTTP. Estos perfiles también se utilizan cuando solo desea el equilibrio de carga de capa 4, que tiene un rendimiento más rápido y es compatible con la creación de reflejo de conexión.

El perfil de aplicación HTTP se utiliza para las aplicaciones HTTP y HTTPS cuando el equilibrador de carga debe realizar acciones en función de la capa 7, como equilibrar la carga de todas las solicitudes de imágenes con un miembro específico del grupo de servidores o finalizar HTTPS para descargar SSL de los miembros del grupo. A diferencia del perfil de aplicación TCP, el perfil de aplicación HTTP finaliza la conexión TCP de cliente antes de seleccionar el miembro del grupo de servidores.

Figura 19-3. Perfiles de aplicaciones TCP y UDP de capa 4

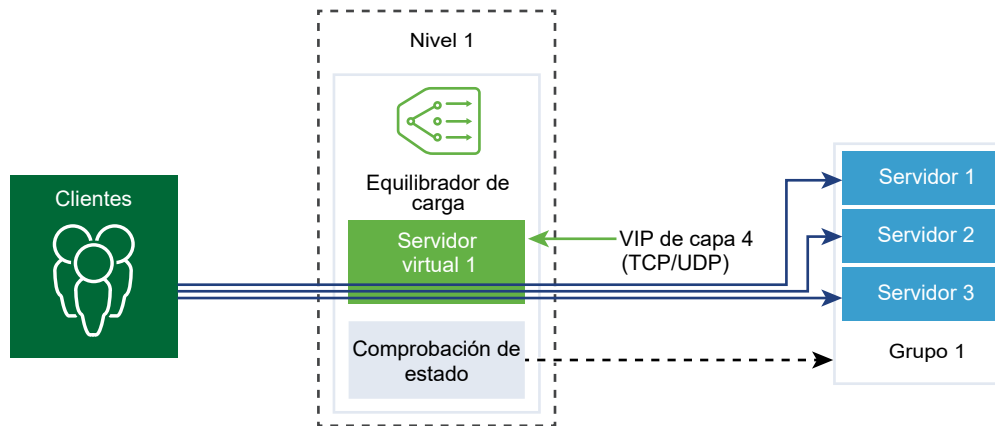
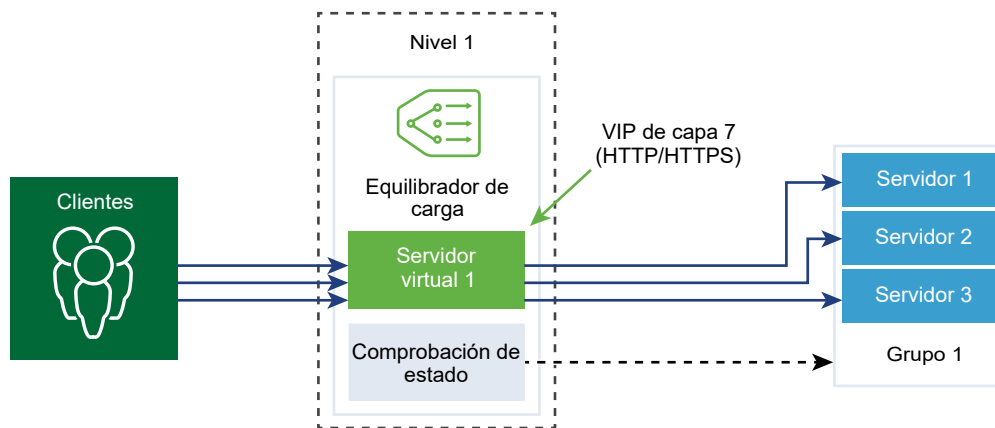


Figura 19-4. Perfil de aplicación HTTPS de capa 7



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Perfiles > Perfiles de aplicaciones**.
- 3 Cree un perfil de aplicación FAST TCP.
 - a Seleccione **Agregar > Perfil FAST TCP** en el menú desplegable.
 - b Introduzca un nombre y una descripción para el perfil de aplicación FAST TCP.

- c Complete los detalles del perfil de aplicación.

También puede aceptar la configuración predeterminada del perfil FAST TCP.

Opción	Descripción
Tiempo de espera de inactividad de conexión	<p>Introduzca, en segundos, el tiempo que el servidor puede estar inactivo después de que se establece una conexión TCP.</p> <p>El tiempo de inactividad debe ser el tiempo real de inactividad de la aplicación, con algunos segundos más para que el equilibrador de carga no cierre sus conexiones antes que la aplicación.</p>
Tiempo de espera de cierre de la conexión	<p>Introduzca, en segundos, el tiempo que la conexión TCP FIN o RST se debe mantener para una aplicación antes de cerrar la conexión.</p> <p>Se podría necesitar un tiempo de espera corto para el cierre, de modo que se puedan admitir velocidades de conexión rápidas.</p>
Creación de reflejo de flujo de HA	<p>Active el botón para que todos los flujos al servidor virtual asociado reflejen el nodo de espera de HA.</p>

- d Haga clic en **Aceptar**.

4 Cree un perfil de aplicación FAST UDP.

También puede aceptar la configuración predeterminada del perfil UDP.

- a Seleccione **Agregar > Perfil FAST UDP** en el menú desplegable.
- b Introduzca un nombre y una descripción para el perfil de aplicación FAST UDP.
- c Complete los detalles del perfil de aplicación.

Opción	Descripción
Tiempo de espera de inactividad	<p>Introduzca, en segundos, el tiempo que el servidor puede estar inactivo después de que se establece una conexión UDP.</p> <p>UDP es un protocolo sin conexión. Para equilibrar la carga, se considera que todos los paquetes UDP con la misma firma de flujo, como la dirección IP de origen y la de destino o los puertos y el protocolo IP recibidos dentro del mismo período de tiempo de espera de inactividad, pertenecen a la misma conexión y se envían al mismo servidor.</p> <p>Si no se reciben paquetes durante el período de tiempo de espera de inactividad, se cierra la conexión que se encuentra en una asociación entre la firma de flujo y el servidor seleccionado.</p>
Creación de reflejo de flujo de HA	<p>Active el botón para que todos los flujos al servidor virtual asociado reflejen el nodo de espera de HA.</p>

- d Haga clic en **Aceptar**.

5 Cree un perfil de aplicación HTTP.

También puede aceptar la configuración predeterminada del perfil HTTP.

El perfil de aplicación HTTP se utiliza para las aplicaciones HTTP y HTTPS.

- a Seleccione **Agregar > Perfil FAST HTTP** en el menú desplegable.
- b Introduzca un nombre y una descripción para el perfil de aplicación HTTP.

c Complete los detalles del perfil de aplicación.

Opción	Descripción
Redireccionamiento	<ul style="list-style-type: none"> ■ Ninguno: si un sitio web está temporalmente fuera de servicio, el usuario recibe un mensaje de error que indica que no se encontró la página. ■ Redireccionamiento de HTTP: si un sitio web está temporalmente fuera de servicio o se movió, las solicitudes entrantes de ese servidor virtual se pueden redirigir de forma temporal a una URL que se especifique aquí. Solo se admite el redireccionamiento estático. <p>Por ejemplo, si el redireccionamiento de HTTP se establece en <code>http://sitedown.abc.com/sorry.html</code>, independientemente de la solicitud real (por ejemplo, <code>http://original_app.site.com/home.html</code> o <code>http://original_app.site.com/somepage.html</code>), las solicitudes entrantes se redirigen a la URL especificada cuando el sitio web original está fuera de servicio.</p> <ul style="list-style-type: none"> ■ Redireccionamiento de HTTP a HTTPS: es posible que determinadas aplicaciones seguras deseen forzar la comunicación a través de SSL, pero, en lugar de rechazar las conexiones que no son de SSL, pueden redirigir la solicitud del cliente para que use SSL. Con el redireccionamiento de HTTP a HTTPS, puede conservar las rutas de host y URI y redirigir la solicitud del cliente para que use SSL. <p>Para el redireccionamiento de HTTP a HTTPS, el servidor virtual HTTPS debe tener el puerto 443 y se debe configurar la misma dirección IP de servidor virtual en el mismo equilibrador de carga.</p> <p>Por ejemplo, una solicitud de cliente para <code>http://app.com/path/page.html</code> se redirige a <code>https://app.com/path/page.html</code>. Si el nombre de host o el URI deben modificarse durante el redireccionamiento (por ejemplo, redirigir a <code>https://secure.app.com/path/page.html</code>), se deben utilizar reglas de equilibrio de carga.</p>
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ Insertar: si el encabezado HTTP XFF no está presente en la solicitud entrante, el equilibrador de carga inserta un encabezado XFF nuevo con la dirección IP del cliente. Si el encabezado HTTP XFF está presente en la solicitud entrante, el equilibrador de carga anexa el encabezado XFF a la dirección IP del cliente. ■ Reemplazar: si el encabezado HTTP XFF está presente en la solicitud entrante, el equilibrador de carga lo reemplaza. <p>Los servidores web registran cada solicitud que controlan con la dirección IP del cliente solicitante. Estos registros se utilizan con fines de depuración y análisis. Si la topología de implementación requiere SNAT en el equilibrador de carga, el servidor utiliza la dirección IP de SNAT del cliente, lo cual va en contra del propósito del registro.</p> <p>Como solución alternativa, puede configurar el equilibrador de carga para insertar el encabezado HTTP XFF con la dirección IP del cliente original. Los servidores pueden configurarse para registrar la dirección IP en el encabezado XFF en lugar de la dirección IP de origen de la conexión.</p>
Tiempo de espera de inactividad de conexión	<p>Introduzca, en segundos, el tiempo que una aplicación HTTP puede permanecer inactiva, en lugar de la opción de socket TCP que debe estar configurada en el perfil de aplicación TCP.</p>

Opción	Descripción
Tamaño del encabezado de solicitud	Especifique, en bytes, el tamaño máximo de búfer que se utiliza para almacenar los encabezados de solicitud HTTP.
Autenticación NTLM	<p>Active el botón para que el equilibrador de carga desactive la multiplexación de TCP y habilite HTTP persistente.</p> <p>NTLM es un protocolo de autenticación que puede utilizarse a través de HTTP. Para el equilibrio de carga con autenticación NTLM, se debe deshabilitar la multiplexación de TCP para los grupos de servidores que alojan aplicaciones basadas en NTLM. De lo contrario, una conexión del lado servidor establecida con las credenciales de un cliente puede utilizarse potencialmente para atender las solicitudes de otro cliente.</p> <p>Si NTLM se habilita en el perfil y se asocia a un servidor virtual y la multiplexación de TCP está habilitada en el grupo de servidores, NTLM tiene prioridad. No se realizará la multiplexación de TCP para ese servidor virtual. Sin embargo, si el mismo grupo se asocia a otro servidor virtual que no tiene NTLM, la multiplexación de TCP está disponible para las conexiones a ese servidor virtual.</p> <p>Si el cliente utiliza HTTP/1.0, el equilibrador de carga se actualiza al protocolo HTTP/1.1 y se establece HTTP persistente. Todas las solicitudes HTTP recibidas en la misma conexión TCP del lado cliente se envían al mismo servidor a través de una sola conexión TCP para asegurarse de que no se requiera una nueva autorización.</p>

- d Haga clic en **Aceptar**.

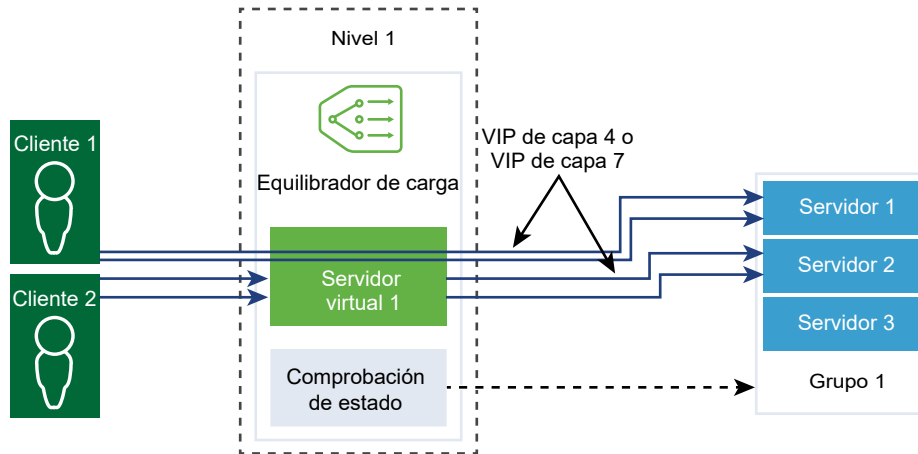
Configurar perfiles persistentes

Para garantizar la estabilidad de las aplicaciones con estado, los equilibradores de carga implementan persistencia que dirige todas las conexiones relacionadas al mismo servidor. Se admiten distintos tipos de persistencia para abordar diferentes tipos de necesidades de aplicaciones.

Algunas aplicaciones mantienen el estado del servidor, como los carritos de compra. Dicho estado podría ser por cliente y estar identificado con la dirección IP del cliente, o bien por sesión HTTP. Las aplicaciones pueden acceder a este estado o modificarlo durante el procesamiento de las conexiones relacionadas posteriores desde el mismo cliente o la misma sesión HTTP.

El perfil de persistencia de IP de origen realiza un seguimiento de las sesiones en función de la dirección IP de origen. Cuando un cliente solicita una conexión a un servidor virtual que permite la persistencia de la dirección de origen, el equilibrador de carga comprueba si ese cliente se conectó anteriormente y, si lo hizo, devuelve el cliente al mismo servidor. De lo contrario, puede seleccionar un miembro del grupo de servidores en función del algoritmo de equilibrio de carga del grupo. El perfil de persistencia de IP de origen es utilizado por los servidores virtuales de capa 4 y capa 7.

El perfil de persistencia de cookie inserta una única cookie para identificar la sesión la primera vez que un cliente accede al sitio. El cliente reenvía la cookie HTTP en solicitudes posteriores y el equilibrador de carga utiliza esa información para proporcionar la persistencia de cookie. El perfil de persistencia de cookie solo puede ser utilizado por los servidores virtuales de capa 7. Tenga en cuenta que **no** se admiten espacios en blanco en el nombre de las cookies.



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Perfiles > Perfiles de persistencia**.
- 3 Cree un perfil de persistencia de IP de origen.
 - a Seleccione **Agregar > Persistencia de IP de origen** en el menú desplegable.
 - b Introduzca un nombre y una descripción para el perfil de persistencia de IP de origen.

- c Complete los detalles del perfil de persistencia.

También puede aceptar la configuración predeterminada del perfil de IP de origen.

Opción	Descripción
Compartir persistencia	<p>Active el botón para compartir la persistencia de modo que todos los servidores virtuales con los que está asociado este perfil puedan compartir la tabla de persistencia.</p> <p>Si no está habilitada la opción para compartir la persistencia en el perfil de persistencia de IP de origen asociado a un servidor virtual, cada servidor virtual al que el perfil está asociado mantiene una tabla de persistencia privada.</p>
Tiempo de espera de entrada de persistencia	<p>Introduzca el tiempo de caducidad de la persistencia en segundos.</p> <p>La tabla de persistencia del equilibrador de carga mantiene las entradas para registrar que las solicitudes de los clientes se dirigen al mismo servidor.</p> <ul style="list-style-type: none"> ■ Si no se reciben nuevas solicitudes de conexión del mismo cliente dentro del tiempo de espera, la entrada de persistencia caducará y se eliminará. ■ Si se recibe una nueva solicitud de conexión del mismo cliente dentro del período de tiempo de espera, se restablece el temporizador y se envía la solicitud de cliente a un miembro estable del grupo. <p>Una vez transcurrido el tiempo de espera, se envían nuevas solicitudes de conexión a un servidor asignado por el algoritmo de equilibrio de carga.</p> <p>En el escenario de persistencia de IP de origen de TCP de equilibrio de carga de capa 7, el tiempo de espera de la entrada de persistencia se agota si no se producen nuevas conexiones TCP durante un tiempo, aunque las conexiones existentes aún estén activas.</p>
Creación de reflejo de persistencia de HA	<p>Active el botón para sincronizar entradas de persistencia con el elemento de HA del mismo nivel.</p>
Purgar entradas al llenarse	<p>Purgue las entradas cuando se llene la tabla de persistencia.</p> <p>Un valor de tiempo de espera grande puede hacer que la tabla de persistencia se llene rápidamente si el tráfico es intenso. Cuando se llena la tabla de persistencia, se elimina la entrada más antigua para aceptar la entrada más reciente.</p>

- d Haga clic en **Aceptar**.

4 Cree un perfil de persistencia de cookie.

- Selecione **Agregar > Persistencia de cookie** en el menú desplegable.
- Introduzca un nombre y una descripción para el perfil de persistencia de cookie.

- c Active el botón **Compartir persistencia** para compartir la persistencia entre varios servidores virtuales que están asociados a los mismos miembros del grupo.

El perfil de persistencia de cookie inserta una cookie con el formato `<name>.<profile-id>.<pool-id>`.

Si la persistencia compartida no está habilitada en el perfil de persistencia de cookie asociado con un servidor virtual, el miembro del grupo utiliza y completa la persistencia de cookie privada para cada servidor virtual. El equilibrador de carga inserta una cookie con el formato, `<name>.<virtual_server_id>.<pool_id>`.

- d Haga clic en **Siguiente**.
- e Complete los detalles del perfil de persistencia.

Opción	Descripción
Modo de cookie	<p>Seleccione un modo en el menú desplegable.</p> <ul style="list-style-type: none"> ■ INSERTAR: agrega una cookie exclusiva para identificar la sesión. ■ PREFIJO: se anexa a la información de cookie HTTP existente. ■ REESCRITURA: reescribe la información de cookie HTTP existente.
Nombre de cookie	<p>Introduzca el nombre de la cookie. Tenga en cuenta que no se admiten espacios en blanco en el nombre de las cookies.</p>
Dominio de cookie	<p>Introduzca el nombre de dominio.</p> <p>El dominio de la cookie HTTP puede configurarse únicamente en el modo INSERTAR.</p>
Ruta de cookie	<p>Introduzca la ruta de URL de la cookie.</p> <p>La ruta HTTP de la cookie se puede establecer únicamente en el modo INSERTAR.</p>
Cifrado de cookie	<p>Cifre la información de dirección IP de servidor y la información de puerto de la cookie.</p> <p>Active el botón para deshabilitar el cifrado. Cuando se deshabilita el cifrado, la información de dirección IP de servidor y de puerto de la cookie aparece en texto sin formato.</p>
Reserva de cookie	<p>Seleccione un nuevo servidor para controlar una solicitud de cliente si la cookie apunta a un servidor que se encuentra en estado DESHABILITADO o INACTIVO.</p> <p>Active el botón para que se rechace la solicitud del cliente si la cookie apunta a un servidor que se encuentra en estado DESHABILITADO o INACTIVO.</p>

- f Complete los detalles de caducidad de la cookie.

Opción	Descripción
Tipo de tiempo de cookie	<p>Seleccione el tipo de tiempo de cookie en el menú desplegable.</p> <p>La cookie de sesión no se almacena y se perderá al cerrar el navegador.</p> <p>El navegador almacena la cookie de persistencia y no se pierde al cerrar el navegador.</p>
Tiempo de inactividad máximo	Introduzca, en segundos, el tiempo que una cookie puede estar inactiva antes de caducar.
Antigüedad máxima de cookie	Solo se aplica a la cookie de sesión . Introduzca, en segundos, la antigüedad máxima que puede estar activa una cookie.

- g Haga clic en **Finalizar**.

Configurar perfil SSL

Los perfiles SSL configuran las propiedades de SSL independientes de la aplicación, como listas de cifrado, y vuelven a utilizar dichas listas a través de varias aplicaciones. Las propiedades SSL son diferentes cuando el equilibrador de carga actúa como un cliente y como un servidor; como resultado se admiten perfiles SSL separados para cliente y para servidor.

Nota El perfil de SSL no se admite en la versión NSX-T Data Center Limited Export.

El perfil SSL del lado cliente hace referencia al equilibrador de carga actuando como un servidor SSL y finalizando la conexión SSL de cliente. El perfil SSL del lado servidor hace referencia al equilibrador de carga actuando como un cliente y estableciendo una conexión con el servidor.

Puede especificar una lista de claves de cifrado en los perfiles SSL del lado cliente y del lado servidor.

El almacenamiento en caché de la sesión SSL permite que el cliente SSL y el servidor reutilicen los parámetros de seguridad negociados previamente, lo que evita la costosa operación de clave pública durante el protocolo de enlace SSL. El almacenamiento en caché de la sesión SSL está deshabilitado de forma predeterminada en el lado cliente y el lado servidor.

Los vales de sesión SSL son un mecanismo alternativo que permiten al cliente y al servidor SSL reutilizar los parámetros de sesión negociados previamente. En los vales de sesión SSL, el cliente y el servidor negocian si son compatibles con los vales de sesión SSL durante el intercambio de protocolos de enlace. Si ambos son compatibles, el servidor puede enviar al cliente un vale de SSL, que incluye los parámetros de sesión SSL cifrados. El cliente puede utilizar ese vale en las conexiones posteriores para volver a utilizar la sesión. Los vales de sesión SSL se habilitan en el lado cliente y se deshabilitan en el lado servidor.

Figura 19-5. Descarga de SSL

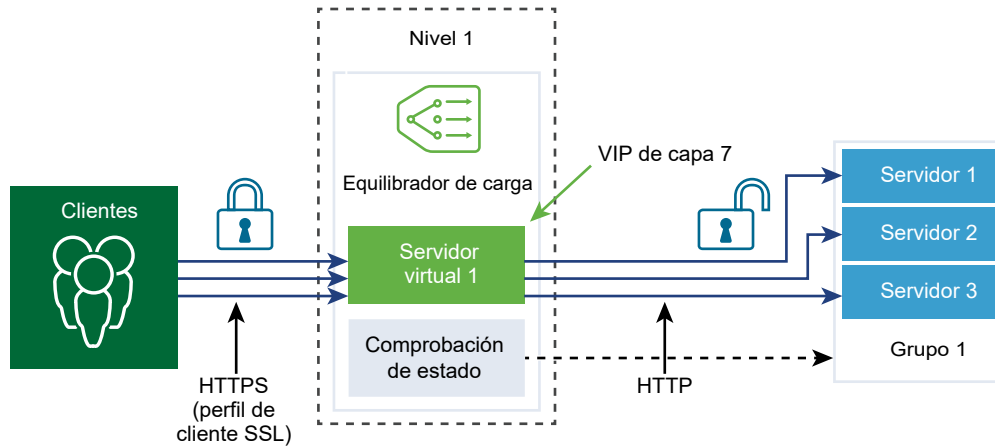
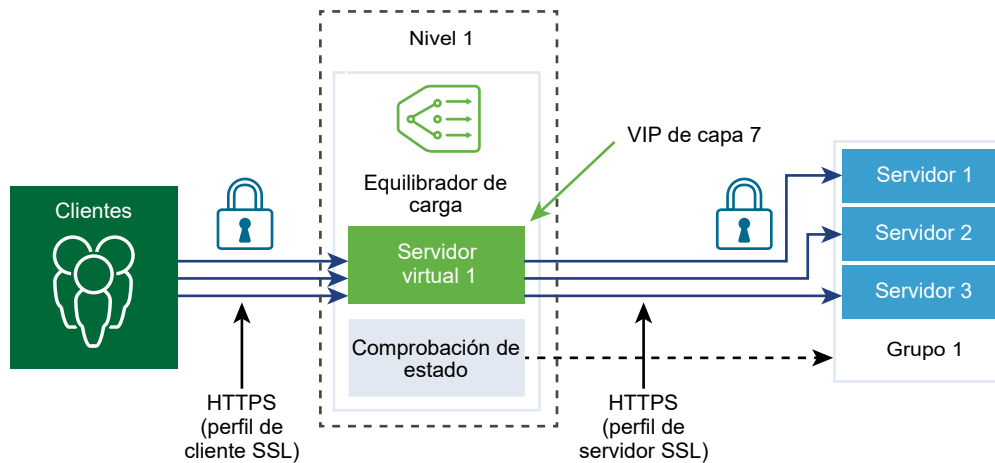


Figura 19-6. SSL de un extremo a otro



Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Perfiles > Perfiles SSL**.
- 3 Cree un perfil SSL de cliente.
 - a Seleccione **Agregar > SSL del lado cliente** en el menú desplegable.
 - b Introduzca un nombre y una descripción para el perfil SSL de cliente.
 - c Asigne las claves de cifrado SSL que se incluirán en el perfil SSL de cliente.
También puede crear claves de cifrado SSL personalizadas.
 - d Haga clic en la flecha para mover las claves de cifrado a la sección Seleccionados.
 - e Haga clic en la pestaña **Protocolos y sesiones**.

- f Seleccione los protocolos SSL que se incluirán en el perfil SSL de cliente.

Las versiones del protocolo SSL TLS1.1 y TLS1.2 están habilitadas de forma predeterminada. TLS1.0 también es compatible, pero está deshabilitada de forma predeterminada.

- g Haga clic en la flecha para mover el protocolo a la sección Seleccionados.
- h Complete la información del protocolo SSL.

También puede aceptar la configuración predeterminada del perfil SSL.

Opción	Descripción
Almacenamiento en caché de la sesión	El almacenamiento en caché de la sesión SSL permite que el cliente SSL y el servidor reutilicen los parámetros de seguridad negociados previamente, lo que evita la costosa operación de clave pública durante un protocolo de enlace SSL.
Tiempo de espera de la entrada de memoria caché de sesión	Introduzca, en segundos, el tiempo de espera de la memoria caché para especificar durante cuánto tiempo se deben mantener y se pueden reutilizar los parámetros de sesión SSL.
Preferir clave de cifrado de servidor	<p>Active el botón para que el servidor pueda seleccionar la primera clave de cifrado compatible de la lista que puede admitir.</p> <p>Durante un protocolo de enlace SSL, el cliente envía al servidor una lista ordenada de las claves de cifrado compatibles.</p>

- i Haga clic en **Aceptar**.

4 Cree un perfil de servidor SSL.

- a Seleccione **Agregar > SSL del lado servidor** en el menú desplegable.
 - b Introduzca un nombre y una descripción para el perfil SSL de servidor.
 - c Seleccione las claves de cifrado SSL que se incluirán en el perfil SSL de servidor.
- También puede crear claves de cifrado SSL personalizadas.

- d Haga clic en la flecha para mover las claves de cifrado a la sección Seleccionados.
- e Haga clic en la pestaña **Protocolos y sesiones**.
- f Seleccione los protocolos SSL que se incluirán en el perfil SSL de servidor.

Las versiones del protocolo SSL TLS1.1 y TLS1.2 están habilitadas de forma predeterminada. TLS1.0 también es compatible, pero está deshabilitada de forma predeterminada.

- g Haga clic en la flecha para mover el protocolo a la sección Seleccionados.

- h Acepte la configuración de almacenamiento en caché de sesión predeterminada.

El almacenamiento en caché de la sesión SSL permite que el cliente SSL y el servidor reutilicen los parámetros de seguridad negociados previamente, lo que evita la costosa operación de clave pública durante un protocolo de enlace SSL.

- i Haga clic en **Aceptar**.

Configurar servidores virtuales de capa 4

Los servidores virtuales reciben todas las conexiones de cliente y las distribuyen entre los servidores. Un servidor virtual tiene una dirección IP, un puerto y un protocolo. Para los servidores virtuales de capa 4, se pueden especificar listas de rangos de puertos en lugar de un solo puerto TCP o UDP para admitir protocolos complejos con puertos dinámicos.

Un servidor virtual de capa 4 debe estar asociado a un grupo de servidores principal, también denominado grupo predeterminado.

Si se deshabilita el estado de un servidor virtual, se rechazarán los nuevos intentos de conexión al servidor virtual mediante el envío de un TCP RST para la conexión TCP o un mensaje de error ICMP para UDP. Se rechazarán las nuevas conexiones incluso si hay entradas de persistencia coincidentes para ellas. Se seguirán procesando las conexiones activas. Si un servidor virtual se elimina o desasocia de un equilibrador de carga, las conexiones activas con ese servidor virtual generan un error.

Requisitos previos

- Compruebe que los perfiles de aplicaciones estén disponibles. Consulte [Configurar perfiles de aplicaciones](#).
- Compruebe que los perfiles persistentes estén disponibles. Consulte [Configurar perfiles persistentes](#).
- Compruebe que los perfiles de SSL para el cliente y el servidor estén disponibles. Consulte [Configurar perfil SSL](#).
- Compruebe que los grupos de servidores estén disponibles. Consulte [Agregar un grupo de servidores para el equilibrio de carga](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Servidores virtuales > Agregar**.
- 3 Introduzca un nombre y una descripción para el servidor virtual de capa 4.

- 4 Seleccione un protocolo de capa 4 en el menú desplegable.

Los servidores virtuales de capa 4 admiten el protocolo FAST TCP o FAST UDP, pero no ambos. Para admitir el protocolo FAST TCP o FAST UDP en la misma dirección IP y el mismo puerto, por ejemplo DNS, se debe crear un servidor virtual para cada protocolo.

En base al tipo de protocolo, se rellenará automáticamente el perfil de aplicación existente.

- 5 Active el botón Registro de acceso para habilitar el registro del servidor virtual de capa 4.

- 6 Haga clic en **Siguiente**.

- 7 Introduzca el número de puerto y la dirección IP del servidor virtual.

Puede especificar el número de puerto o un rango de puertos del servidor virtual.

- 8 Complete los detalles de las propiedades avanzadas.

Opción	Descripción
Máximo de conexiones simultáneas	Establezca la cantidad máxima de conexiones simultáneas permitidas con un servidor virtual de modo que el servidor virtual no consuma recursos de otras aplicaciones alojadas en el mismo equilibrador de carga.
Velocidad máxima de conexión nueva	Establezca el máximo para la nueva conexión con un miembro del grupo de servidores de modo que un servidor virtual no consuma recursos.
Puerto de miembro de grupo predeterminado	<p>Introduzca un puerto de miembro de grupo predeterminado si el puerto de miembro de grupo de un servidor virtual no está definido.</p> <p>Por ejemplo, si se define un servidor virtual con el rango de puertos 2000-2999 y el rango de puertos del miembro de grupo predeterminado se establece en 8000-8999, se envía una conexión de cliente entrante con el puerto de servidor virtual 2500 a un miembro del grupo con un puerto de destino establecido en 8500.</p>

- 9 Seleccione un grupo de servidores existente en el menú desplegable.

El grupo de servidores consta de uno o varios servidores, también denominados miembros de grupo, que están configurados de manera similar y ejecutan la misma aplicación.

- 10 Seleccione un grupo de servidores de respaldo existente en el menú desplegable.

El grupo de servidores de respaldo atiende la solicitud cuando un equilibrador de carga no puede seleccionar un servidor de back-end para atender la solicitud del grupo predeterminado.

- 11 Haga clic en **Siguiente**.

- 12 Seleccione el perfil de persistencia existente en el menú desplegable.

El perfil de persistencia se puede habilitar en un servidor virtual para permitir que las conexiones de cliente relacionadas se envíen al mismo servidor.

- 13 Haga clic en **Finalizar**.

Configurar servidores virtuales de capa 7

Los servidores virtuales reciben todas las conexiones de cliente y las distribuyen entre los servidores. Un servidor virtual tiene una dirección IP, un puerto y un protocolo TCP.

Las reglas de equilibrador de carga son compatibles solo con los servidores virtuales de capa 7 con un perfil de aplicación HTTP. Distintos servicios de equilibrador de carga pueden utilizar reglas de equilibrador de carga.

Cada regla de equilibrador de carga consta de una o varias condiciones de coincidencia y una o varias acciones. Si no se especifican las condiciones de coincidencia, la regla de equilibrador de carga siempre coincide y se utiliza para definir las reglas predeterminadas. Si se especifica más de una condición de coincidencia, la estrategia de coincidencia determina si deben coincidir todas o algunas de las condiciones para que la regla de equilibrador de carga se considere como coincidencia.

Cada regla de equilibrador de carga se implementa en una fase específica del procesamiento de equilibrio de carga: reescritura de solicitud HTTP, reenvío de solicitud HTTP y reescritura de respuesta HTTP. No todas las condiciones de coincidencia y las acciones se aplican a cada fase.

Si se deshabilita el estado de un servidor virtual, se rechazarán los nuevos intentos de conexión al servidor virtual mediante el envío de un TCP RST para la conexión TCP o un mensaje de error ICMP para UDP. Se rechazarán las nuevas conexiones incluso si hay entradas de persistencia coincidentes para ellas. Se seguirán procesando las conexiones activas. Si un servidor virtual se elimina o desasocia de un equilibrador de carga, las conexiones activas con ese servidor virtual generan un error.

Requisitos previos

- Compruebe que los perfiles de aplicaciones estén disponibles. Consulte [Configurar perfiles de aplicaciones](#).
- Compruebe que los perfiles persistentes estén disponibles. Consulte [Configurar perfiles persistentes](#).
- Compruebe que los perfiles de SSL para el cliente y el servidor estén disponibles. Consulte [Configurar perfil SSL](#).
- Compruebe que los grupos de servidores estén disponibles. Consulte [Agregar un grupo de servidores para el equilibrio de carga](#).
- Compruebe que el certificado de CA y de cliente estén disponibles. Consulte [Crear un archivo de solicitud de firma del certificado](#).
- Compruebe que exista una lista de revocación de certificación (Certification Revocation List, CRL). Consulte [Importar una lista de revocación de certificados](#).
- [Configurar grupo y reglas de servidor virtual de capa 7](#)

Con servidores virtuales de capa 7, opcionalmente, puede configurar reglas de equilibrador de carga y personalizar el comportamiento de equilibrio de carga mediante reglas de coincidencia o de acción.

■ Configurar perfiles de equilibrio de carga de servidor virtual de capa 7

Con los servidores virtuales de capa 7, puede configurar de forma opcional persistencia de equilibrador de carga, SSL del lado cliente y perfiles SSL del lado servidor.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Equilibrador de carga > Servidores virtuales > Agregar**.
- 3 Introduzca un nombre y una descripción para el servidor virtual de capa 7.
- 4 Seleccione el elemento de menú de capa 7.
Los servidores virtuales de capa 7 admiten los protocolos HTTP y HTTPS.
El perfil de aplicación HTTP existente se rellenará automáticamente.
- 5 (opcional) Haga clic en **Siguiente** para configurar perfiles de grupo de servidores y de equilibrio de carga.
- 6 Haga clic en **Finalizar**.

Configurar grupo y reglas de servidor virtual de capa 7

Con servidores virtuales de capa 7, opcionalmente, puede configurar reglas de equilibrador de carga y personalizar el comportamiento de equilibrio de carga mediante reglas de coincidencia o de acción.

Las reglas del equilibrador de carga admiten REGEX para los tipos de coincidencia. Los patrones REGEX de estilo PCRE se admiten con algunas limitaciones en los casos de uso avanzado. Cuando se utiliza REGEX en condiciones de coincidencia, se admiten grupos de captura con nombre.

Estas son las restricciones de REGEX:

- No se admiten uniones ni intersecciones de caracteres. Por ejemplo, no utilice `[a-z[0-9]]` ni `[a-z&&[aeiou]]`; en su lugar, use `[a-z0-9]` y `[aeiou]`, respectivamente.
- Solo se admiten 9 referencias inversas, y se pueden usar de `\1` a `\9` para hacer referencia a ellas.
- Utilice el formato `\Odd` para hacer coincidir caracteres octales, no el formato `\ddd`.
- No se admiten marcas integradas en el nivel superior; este tipo de marca solo se admite en los grupos. Por ejemplo, no utilice `"Case (?i:sensitive)"`; en su lugar, use `"Case ((?i:sensitive))"`.
- No se admiten las operaciones de preprocesamiento `\l`, `\u`, `\L` ni `\U`. Donde `\l` indica que el siguiente carácter será una minúscula; `\u` indica que el siguiente carácter será una mayúscula; `\L` indica que el texto estará en minúscula hasta `\E`; y, por último, `\U` indica que el texto estará en mayúscula hasta `\E`.
- `(?(condition)X)`, `(?{code})`, `(?{Code})` y `(?#comment)` no se admiten.

- No se admite la clase de carácter Unicode predefinida \X.
- No se admiten construcciones de caracteres con nombre para los caracteres Unicode. Por ejemplo, no utilice \N{name}; en su lugar, use \u2018.

Cuando se utiliza REGEX en condiciones de coincidencia, se admiten grupos de captura con nombre. Por ejemplo, el patrón de coincidencia REGEX `/news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+)/?(<article>.*))` se puede utilizar para hacer coincidir un URI como `/news/2018-06-15/news1234.html`.

A continuación, las variables se establecen como se indica a continuación: `$year = "2018"` `$month = "06"` `$day = "15"` `$article = "news1234.html"`. Después de definir las variables, estas se pueden utilizar en las acciones de regla del equilibrador de carga. Por ejemplo, el URI se puede reescribir con las variables de coincidencia como `/news.py?year=$year&month=$month&day=$day&article=$article`. Seguidamente, el URI se reescribirá como `/news.py?year=2018&month=06&day=15&article=news1234.html`.

Las acciones de reescritura pueden utilizar una combinación de grupos de captura con nombre y variables integradas. Por ejemplo, el URI se puede reescribir como `/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr`. A continuación, el URI de ejemplo se reescribirá como `/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1`.

Nota Para los grupos de captura con nombre, el nombre no puede comenzar con el carácter `"_"`.

Además de los grupos de captura con nombre, se pueden usar las siguientes variables integradas en las acciones de reescritura. Todos los nombres de las variables integradas comienzan con `_`.

- `$_args`: los argumentos de la solicitud.
- `$_arg_<nombre>`: el `<nombre>` del argumento de la línea de solicitud.
- `$_cookie_<nombre>`: el valor de la cookie `<nombre>`.
- `$_upstream_cookie_<nombre>`: la cookie con el nombre especificado que envía el servidor upstream del campo de encabezado de respuesta "Set-Cookie".
- `$_upstream_http_<nombre>`: un campo de encabezado de respuesta arbitrario, y `<nombre>` es el nombre del campo convertido en minúscula con guiones reemplazados por guiones bajos.
- `$_host` (en orden de precedencia): el nombre de host de la línea de la solicitud, el nombre de host del campo "Host" del encabezado de la solicitud, o el nombre del servidor que coincida con una solicitud.
- `$_http_<nombre>`: un campo de encabezado de la solicitud arbitrario, y `<nombre>` es el nombre del campo en minúscula con guiones reemplazados por guiones bajos.
- `$_https`: "on" si la conexión funciona en modo SSL; de lo contrario, "".
- `$_is_args`: "?" si una línea de la solicitud tiene argumentos; de lo contrario, "".
- `$_query_string`: igual que `$_args`.

- `$_remote_addr`: la dirección del cliente.
- `$_remote_port`: el puerto del cliente.
- `$_request_uri`: el URI completo de la solicitud original (con argumentos).
- `$_scheme`: el esquema de la solicitud, "http" o "https".
- `$_server_addr`: la dirección del servidor que aceptó una solicitud.
- `$_server_name`: el nombre del servidor que aceptó una solicitud.
- `$_server_port`: el puerto del servidor que aceptó una solicitud.
- `$_server_protocol`: el protocolo de solicitud; suele ser "HTTP/1.0" o "HTTP/1.1".
- `$_ssl_client_cert`: devuelve el certificado de cliente en formato PEM para una conexión SSL establecida con cada línea, exceptuando la primera antecedida por el carácter de tabulación.
- `$_ssl_server_name`: devuelve el nombre del servidor solicitado mediante la SNI.
- `$_uri`: la ruta del URI de la solicitud.
- `$_ssl_ciphers`: devuelve los cifrados SSL de cliente
- `$_ssl_client_i_dn`: devuelve la cadena "DN de emisor" del certificado de cliente para una conexión SSL establecida de acuerdo con RFC 2253
- `$_ssl_client_s_dn`: devuelve la cadena "DN de asunto" del certificado de cliente para una conexión SSL establecida de acuerdo con RFC 2253
- `$_ssl_protocol`: devuelve el protocolo de una conexión SSL establecida
- `$_ssl_session_reused`: devuelve "r" si se reutilizó una sesión SSL, o "." en el resto de casos

Requisitos previos

Compruebe que haya disponible un servidor virtual de capa 7. Consulte [Configurar servidores virtuales de capa 7](#).

Procedimiento

- 1 Abra el servidor virtual de capa 7.
- 2 Vaya a la página Identificadores de servidor virtual.
- 3 Introduzca el número de puerto y la dirección IP del servidor virtual.

Puede especificar el número de puerto o un rango de puertos del servidor virtual.

4 Complete los detalles de las propiedades avanzadas.

Opción	Descripción
Máximo de conexiones simultáneas	Establezca la cantidad máxima de conexiones simultáneas permitidas con un servidor virtual de modo que el servidor virtual no consuma recursos de otras aplicaciones alojadas en el mismo equilibrador de carga.
Velocidad máxima de conexión nueva	Establezca el máximo para la nueva conexión con un miembro del grupo de servidores de modo que un servidor virtual no consuma recursos.
Puerto de miembro de grupo predeterminado	<p>Introduzca un puerto de miembro de grupo predeterminado si el puerto de miembro de grupo de un servidor virtual no está definido.</p> <p>Por ejemplo, si se define un servidor virtual con el rango de puertos 2000-2999 y el rango de puertos del miembro de grupo predeterminado se establece en 8000-8999, se envía una conexión de cliente entrante con el puerto de servidor virtual 2500 a un miembro del grupo con un puerto de destino establecido en 8500.</p>

5 (opcional) Seleccione un grupo de servidores predeterminado existente en el menú desplegable.

El grupo de servidores consta de uno o varios servidores, denominados miembros de grupo, que están configurados de manera similar y ejecutan la misma aplicación.

6 Haga clic en **Agregar** para configurar las reglas de equilibrador de carga para la fase de reescritura de solicitud HTTP.

Los tipos de coincidencia compatibles son REGEX, STARTS_WITH, ENDS_WITH, entre otras, y la opción inversa.

Condición de coincidencia compatible	Descripción
Método de solicitud HTTP	Coincide con un método de solicitud HTTP. http_request.method: valor que debe coincidir.
URI de solicitud HTTP	Coincide con un URI de solicitud HTTP sin argumentos de consulta. http_request.uri: valor que debe coincidir.
Argumentos de URI de solicitud HTTP	Coincide con un argumento de consulta URI de solicitud HTTP. http_request.uri_arguments: valor que debe coincidir.
Versión de solicitud HTTP	Coincide con una versión de solicitud HTTP. http_request.version: valor que debe coincidir.
Encabezado de solicitud HTTP	Coincide con cualquier encabezado de solicitud HTTP. http_request.header_name: nombre de encabezado que debe coincidir. http_request.header_value: valor que debe coincidir.
Carga de solicitud HTTP	Coincide con el contenido del cuerpo de la solicitud HTTP. http_request.body_value: valor que debe coincidir.

Condición de coincidencia compatible	Descripción
Campos de encabezado TCP	<p>Coincide con un puerto TCP de origen o destino.</p> <p>tcp_header.source_port: puerto de origen que debe coincidir.</p> <p>tcp_header.destination_port: puerto de destino que debe coincidir.</p>
Campos de encabezado IP	<p>Coincide con una dirección IP de origen o destino.</p> <p>ip_header.source_address: dirección de origen que debe coincidir.</p> <p>ip_header.destination_address: dirección de destino que debe coincidir.</p>
Acción	Descripción
Reescritura de URI de solicitud HTTP	<p>Modifica un URI.</p> <p>http_request.uri: URI (sin argumentos de consulta) que se debe escribir.</p> <p>http_request.uri_args: argumentos de consulta URI que se deben escribir.</p>
Reescritura de encabezado de solicitud HTTP	<p>Modifica el valor de un encabezado HTTP.</p> <p>http_request.header_name: nombre de encabezado.</p> <p>http_request.header_value: valor que se debe escribir.</p>

- Haga clic en **Agregar** para configurar las reglas de equilibrador de carga para el reenvío de solicitud HTTP.

Todos los valores de coincidencia aceptan expresiones regulares.

Condición de coincidencia compatible	Descripción
Método de solicitud HTTP	<p>Coincide con un método de solicitud HTTP.</p> <p>http_request.method: valor que debe coincidir.</p>
URI de solicitud HTTP	<p>Coincide con un URI de solicitud HTTP.</p> <p>http_request.uri: valor que debe coincidir.</p>
Argumentos de URI de solicitud HTTP	<p>Coincide con un argumento de consulta URI de solicitud HTTP.</p> <p>http_request.uri_args: valor que debe coincidir.</p>
Versión de solicitud HTTP	<p>Coincide con una versión de solicitud HTTP.</p> <p>http_request.version: valor que debe coincidir.</p>
Encabezado de solicitud HTTP	<p>Coincide con cualquier encabezado de solicitud HTTP.</p> <p>http_request.header_name: nombre de encabezado que debe coincidir.</p> <p>http_request.header_value: valor que debe coincidir.</p>
Carga de solicitud HTTP	<p>Coincide con el contenido del cuerpo de la solicitud HTTP.</p> <p>http_request.body_value: valor que debe coincidir.</p>

Condición de coincidencia compatible	Descripción
Campos de encabezado TCP	Coincide con un puerto TCP de origen o destino. tcp_header.source_port: puerto de origen que debe coincidir. tcp_header.destination_port: puerto de destino que debe coincidir.
Campos de encabezado IP	Coincide con una dirección IP de origen. ip_header.source_address: dirección de origen que debe coincidir.
Acción	Descripción
Rechazar	Rechaza una solicitud, por ejemplo, estableciendo el estado en 5xx. http_forward.reply_status: código de estado HTTP utilizado para el rechazo. http_forward.reply_message: mensaje de rechazo de HTTP.
Redirigir	Redirige una solicitud. El código de estado debe establecerse en 3xx. http_forward.redirect_status: código de estado HTTP de redirección. http_forward.redirect_url: URL de redirección de HTTP.
Seleccionar grupo	Fuerza la solicitud a un grupo de servidores específicos. El algoritmo configurado del miembro del grupo especificado (predictor) se utiliza para seleccionar un servidor del grupo de servidores. http_forward.select_pool: UUID de grupo de servidores.

- 8 Haga clic en **Agregar** para configurar las reglas de equilibrador de carga para la reescritura de respuesta HTTP.

Todos los valores de coincidencia aceptan expresiones regulares.

Condición de coincidencia compatible	Descripción
Encabezado de respuesta HTTP	Coincide con cualquier encabezado de respuesta HTTP. http_response.header_name: nombre del encabezado que debe coincidir. http_response.header_value: valor que debe coincidir.
Acción	Descripción
Reescritura de encabezado de respuesta HTTP	Modifica el valor del encabezado de una respuesta HTTP. http_response.header_name: nombre de encabezado. http_response.header_value: valor que se debe escribir.

- 9 (opcional) Haga clic en **Siguiente** para configurar perfiles de equilibrio de carga.

- 10 Haga clic en **Finalizar**.

Configurar perfiles de equilibrio de carga de servidor virtual de capa 7

Con los servidores virtuales de capa 7, puede configurar de forma opcional persistencia de equilibrador de carga, SSL del lado cliente y perfiles SSL del lado servidor.

Nota El perfil de SSL no se admite en la versión NSX-T Data Center Limited Export.

Si se configura un enlace de perfil SSL del lado cliente en un servidor virtual, pero no un enlace de perfil SSL del lado servidor, el servidor virtual funciona en un modo de finalización de SSL, que tiene una conexión cifrada con el cliente y una conexión de texto sin formato con el servidor. Si se configuran enlaces de perfil SSL del lado cliente y el lado servidor, el servidor virtual funciona en modo de servidor proxy SSL, que tiene una conexión cifrada con el cliente y el servidor.

Actualmente no se permite asociar un enlace de perfil SSL del lado servidor sin asociar un enlace de perfil SSL del lado cliente. Si un enlace de perfil SSL del lado cliente y del lado servidor no está asociado a un servidor virtual y la aplicación está basada en SSL, el servidor virtual funciona en un modo que no es compatible con SSL. En este caso, el servidor virtual debe configurarse para la capa 4. Por ejemplo, el servidor virtual puede asociarse a un perfil FAST TCP.

Requisitos previos

Compruebe que haya disponible un servidor virtual de capa 7. Consulte [Configurar servidores virtuales de capa 7](#).

Procedimiento

- 1 Abra el servidor virtual de capa 7.
- 2 Desplácese hasta la página Perfiles de equilibrio de carga.
- 3 Active el botón Persistencia para habilitar el perfil.

El perfil de persistencia permite que las conexiones del cliente relacionadas se envíen al mismo servidor.

- 4 Seleccione el perfil de persistencia de IP de origen o de persistencia de cookies.
- 5 Seleccione el perfil de persistencia existente en el menú desplegable.
- 6 Haga clic en **Siguiente**.

- 7 Active el botón SSL del lado cliente para habilitar el perfil.

El enlace de perfil SSL del lado cliente permite que haya varios certificados, de modo que los nombres de host se asocien con el mismo servidor virtual.

El perfil SSL del lado cliente asociado se rellenará automáticamente.

- 8 Seleccione un certificado predeterminado en el menú desplegable.

Este certificado se usa si el servidor no aloja varios nombres de host en la misma dirección IP o si el cliente no admite la extensión de Indicación de nombre de servidor (Server Name Indication, SNI).

- 9 Seleccione el certificado de SNI disponible y haga clic en la flecha para mover el certificado a la sección Seleccionados.
- 10 (opcional) Active la autenticación obligatoria de cliente para habilitar ese elemento de menú.
- 11 Seleccione el certificado de CA disponible y haga clic en la flecha para mover el certificado a la sección Seleccionados.

- 12 Establezca la profundidad de la cadena de certificados para comprobar la profundidad de la cadena de certificados de servidor.

- 13 Seleccione la CRL disponible y haga clic en la flecha para mover el certificado a la sección Seleccionados.

Se puede configurar una CRL para no permitir certificados de servidor comprometidos.

- 14 Haga clic en **Siguiente**.

- 15 Active el botón SSL del lado servidor para habilitar el perfil.

El perfil SSL del lado servidor asociado se rellenará automáticamente.

- 16 Seleccione un certificado de cliente en el menú desplegable.

El certificado de cliente se usa si el servidor no aloja varios nombres de host en la misma dirección IP o si el cliente no admite la extensión de Indicación de nombre de servidor (Server Name Indication, SNI).

- 17 Seleccione el certificado de SNI disponible y haga clic en la flecha para mover el certificado a la sección Seleccionados.

- 18 (opcional) Active la autenticación de servidor para habilitar ese elemento de menú.

El enlace de perfil SSL del lado servidor especifica si se debe validar o no el certificado de servidor presentado al equilibrador de carga durante el protocolo de enlace SSL. Cuando se habilita la validación, el certificado de servidor debe estar firmado por una de las CA de confianza cuyos certificados autofirmados se especifican en el mismo enlace de perfil SSL del lado servidor.


- 19 Seleccione el certificado de CA disponible y haga clic en la flecha para mover el certificado a la sección Seleccionados.

- 20 Establezca la profundidad de la cadena de certificados para comprobar la profundidad de la cadena de certificados de servidor.

- 21 Seleccione la CRL disponible y haga clic en la flecha para mover el certificado a la sección Seleccionados.

Se puede configurar una CRL para no permitir certificados de servidor comprometidos. OCSP y la asociación de OCSP no se admiten en el lado servidor.

- 22 Haga clic en **Finalizar**.

Nota Si utiliza la interfaz de usuario **Opciones avanzadas de redes y seguridad** para modificar los objetos creados en la interfaz de directivas, es posible que algunos ajustes no se puedan configurar. Estos ajustes de solo lectura muestran este icono: . Consulte [Capítulo 1 Descripción general de NSX Manager](#) para obtener más información.

Este capítulo incluye los siguientes temas:

- [Agregar o eliminar una regla de firewall de un enrutador lógico](#)
- [Configurar el firewall de un puerto de puente del conmutador lógico](#)
- [Secciones y reglas de firewall](#)
- [Acerca de las reglas de firewall](#)

Agregar o eliminar una regla de firewall de un enrutador lógico

Puede agregar reglas de firewall a un enrutador lógico de nivel 0 o de nivel 1 para controlar la comunicación del enrutador.

El firewall de Edge se implementa en puertos de enrutador de vínculo superior. Esto quiere decir que las reglas de firewall solo se aplican si el tráfico llega a los puertos de enrutador de vínculo superior de Edge. Para aplicar reglas de Firewall a un destino de IP específico, debe configurar grupos con la red /32. Si proporciona una subred que no sea /32, las reglas de firewall se aplicarán a toda la subred.

Requisitos previos

Familiarícese con los parámetros de una regla de firewall. Consulte [Agregar una regla de firewall](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Redes > Enrutadores**.
- 3 Haga clic en la pestaña **Enrutadores** si aún no está seleccionada.

- 4 Haga clic en el nombre de un enrutador lógico.
- 5 Seleccione **Servicios > Firewall de Edge**.
- 6 Haga clic en una regla o una sección.
- 7 Para agregar una regla, haga clic en **Agregar regla** en la barra de menús y seleccione **Agregar regla anterior** o **Agregar regla siguiente**; también puede hacer clic en el icono de menú que aparece en la primera columna de una regla, seleccionar **Agregar regla anterior** o **Agregar regla siguiente** y especificar los parámetros de la regla.

El campo Se aplica a no aparece porque esta regla solo se aplica al enrutador lógico.

- 8 Para eliminar una regla, selecciónela, haga clic en **Eliminar** en la barra de menús, o bien haga clic en el icono de menú que aparece en la primera columna y seleccione **Eliminar**.

Resultados

Nota Si agrega una regla de firewall a un enrutador lógico de nivel 0 y el clúster de NSX Edge que soporta al enrutador se está ejecutando en modo activo-activo, el firewall solo puede ejecutarse en modo sin estado. Si configura la regla de firewall con servicios con estado, como HTTP, SSL, TCP, etc, la regla de firewall no funcionará según lo esperado. Para evitar este problema, configure el clúster de NSX Edge de manera que se ejecute en el modo activo-en espera.

Configurar el firewall de un puerto de puente del conmutador lógico

Puede configurar secciones y reglas de firewall para el puerto de puente de un conmutador lógico respaldado por un puente de Capa 2. El puente debe crearse con nodos de NSX Edge.

Requisitos previos

Compruebe que el conmutador esté conectado a un perfil de puente. Consulte [Crear un conmutador lógico respaldado por puentes de Capa 2](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall de puente**.
- 3 Seleccione un conmutador lógico.
El conmutador debe asociarse a un perfil de puente.
- 4 Siga los mismos pasos de las secciones anteriores para configurar el firewall de Capa 2 o 3.

Secciones y reglas de firewall

Las secciones de firewall se utilizan para agrupar un conjunto de reglas de firewall.

Una sección de firewall está constituida por una o varias reglas de firewall individuales. Cada regla de firewall individual contiene instrucciones que determinan si un paquete se debe permitir o bloquear, qué protocolos y puertos puede utilizar, etc. Las secciones se utilizan para varios arrendamientos, como reglas específicas de departamentos de ventas e ingeniería de secciones independientes.

Una sección se puede definir como reglas sin estado o con estado impositivo. Las reglas sin estado se consideran ACL sin estado tradicionales. Las ACL reflexivas no son compatibles con las secciones sin estado. No le recomendamos que utilice una combinación de reglas con estado y sin estado en un puerto de conmutador lógico único, ya que se podría producir un comportamiento no definido.

Las reglas se pueden subir o bajar en una sección. En el caso del tráfico que intenta atravesar el firewall, la información del paquete está sujeta a las reglas en el orden que se muestra en la sección, empezando por el principio y siguiendo por la regla predeterminada en la parte inferior. La primera regla que coincide con el paquete tiene su acción configurada aplicada. Además, los procesos especificados en las opciones configuradas de la regla se realizan y todas las reglas posteriores se ignoran (incluso si una regla posterior es una coincidencia mejor). Por lo tanto, debe colocar las reglas específicas por encima de las reglas más generales para garantizar que no se ignoren dichas reglas. La regla predeterminada situada en la parte inferior de la tabla de reglas es una regla "catchall", por lo que la regla predeterminada aplicará los paquetes que no coincidan con ninguna otra regla.

Nota Un conmutador lógico tiene una propiedad denominada modo de N-VDS. Esta propiedad proviene de la zona de transporte a la que pertenece el conmutador. Si el modo de N-VDS es `ENS` (también conocido como `Enhanced Datapath`), no se puede crear una sección o una regla de firewall con el conmutador o sus puertos en los campos `Source`, `Destination` o `Applied To`.

Habilitar y deshabilitar el firewall distribuido

Puede habilitar o deshabilitar la función del firewall distribuido.

Si está deshabilitada, no se aplicarán reglas de firewall a nivel del plano de datos. Al volver a habilitar esta función, se volverán a aplicar las reglas.

Procedimiento

- 1 Desplácese a **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **Configuración**.
- 3 Haga clic en Firewall distribuido **Editar**.
- 4 En el cuadro de diálogo, cambie el estado del firewall a verde (habilitado) o gris (deshabilitado).

- 5 Haga clic en **Guardar**.

Agregar una sección de reglas de firewall

Una sección de regla de firewall se edita y guarda de manera independiente; se utiliza para aplicar diferentes configuraciones de firewall en los arrendatarios.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Haga clic en una regla o una sección.
- 4 Haga clic en el icono de la sección en la barra de menús y seleccione **Agregar sección de arriba** o **Agregar sección de abajo**.

Nota Si el tráfico intenta acceder a través del firewall, la información del paquete está sujeta a las reglas en el orden que aparece en la Tabla de reglas, comenzando por el principio hasta las reglas predeterminadas situadas al final. En algunos casos, el orden de prioridad de dos o más reglas puede ser importante a la hora de determinar la disposición del paquete.

- 5 Escriba el nombre de la sección.
- 6 Para configurar el firewall sin estado, seleccione **Habilitar firewall sin estado**. Esta opción solo se aplica a la Capa 3.

Los firewalls sin estado inspeccionan el tráfico de red y restringen o bloquean paquetes en base a las direcciones de origen y destino u otros valores de estado. Para los flujos TCP y UDP, después del primer paquete, se crea y se mantiene una memoria caché para la tupla de tráfico en cualquier de ambas direcciones si el resultado del firewall es ALLOW. Esto significa que el tráfico ya no necesita comprobar las reglas del firewall, lo que provoca una latencia más baja. Por tanto, los firewalls sin estado son generalmente más rápidos y logran un mejor rendimiento durante cargas de tráfico más altas.

Los firewalls con estado pueden inspeccionar los flujos de tráfico de un extremo a otro. Siempre se consultará al firewall para cada paquete con el objeto de validar el estado y los números de secuencia. Los firewalls con estado son mejores a la hora de identificar comunicaciones no autorizadas y falsificadas.

No es posible alternar entre con o sin estado una vez definido.

- 7 Seleccione uno o varios objetos para aplicarlos a la sección.

Los tipos de objetos son puertos lógicos, conmutadores lógicos y NSGroups. Si selecciona un grupo NSGroup, este debe contener uno o varios conmutadores lógicos o puertos lógicos. El grupo NSGroup se ignorará si solo contiene conjuntos de direcciones IP o de direcciones MAC.

Nota La opción **Se aplica a** en una sección anulará los ajustes de **Se aplica a** en las reglas de esa sección.

- 8 Haga clic en **Aceptar**.

Pasos siguientes

Agregue reglas de firewall a la sección.

Eliminar una sección de reglas de firewall

Una sección de reglas de firewall se puede eliminar cuando ya no se utiliza.

Al quitar una sección de reglas de firewall, todas las reglas de la sección se eliminan. No puede eliminar una sección y volver a agregarla en otro lugar de la tabla de firewall. Para hacerlo, debe eliminar la sección y publicar la configuración. A continuación, agregue la sección eliminada en la tabla de firewall y vuelva a publicar la configuración.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Haga clic en el icono de menú que aparece en la primera columna de la sección y seleccione **Eliminar sección**.

También puede seleccionar la sección y hacer clic en el icono de eliminación de la barra de menús.

Habilitar y deshabilitar reglas de sección

Puede habilitar o deshabilitar todas las reglas de una sección de reglas de firewall.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Haga clic en el icono de menú de la primera columna de la sección y seleccione **Habilitar todas las reglas** o **Deshabilitar todas las reglas**.
- 4 Haga clic en **Publicar**.

Habilitar y deshabilitar reglas de registro

Si habilita registros de reglas de sección, se registrará información sobre los paquetes de todas las reglas de una sección. En función del número de reglas de una sección, una sección de firewall común generará grandes cantidades de información de registro y puede afectar al rendimiento.

Los registros se almacenan en el archivo `/var/log/dfwpktlogs.log` de los hosts KVM y ESXi.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Haga clic en el icono de menú de la primera columna de la sección y seleccione **Habilitar registros** o **Deshabilitar registros**.
- 4 Haga clic en **Publicar**.

Configurar una lista de exclusión en el firewall

Un puerto lógico, un conmutador lógico o NSGroup pueden excluirse de una regla del firewall.

Después de haber creado una sección con reglas de firewall, puede que quiera excluir un puerto de dispositivo de NSX-T Data Center de las reglas del firewall.

Nota NSX-T Data Center agrega automáticamente las máquinas virtuales del nodo de NSX Manager y NSX Edge a la lista de exclusión del firewall.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido > Lista de exclusión > Agregar**.
- 2 Seleccione un tipo y un objeto.
Los tipos disponibles son **Puerto lógico**, **Conmutador lógico** y **Grupo NSGroup**.
- 3 Haga clic en **Aceptar**.
- 4 Para eliminar un objeto de la lista de exclusión, selecciónelo y haga clic en **Eliminar** en la barra de menús.

Acerca de las reglas de firewall

NSX-T Data Center utiliza reglas de firewall para especificar el control de tráfico dentro y fuera de la red.

Firewall presenta varios conjuntos de reglas de configuración: reglas de Capa 3 (pestaña General) y reglas de Capa 2 (pestaña Ethernet). Las reglas de firewall de Capa 2 se procesan antes que las reglas de Capa 3. Puede configurar una lista de exclusión que contenga los conmutadores lógicos, los puertos lógicos o los grupos que se excluirán de la aplicación del firewall.

Las reglas de firewall se aplican de la siguiente manera:

- Las reglas se procesan siguiendo un orden de arriba a abajo.
- Cada paquete se compara con la regla principal de la tabla antes de bajar a las reglas subsiguientes de esa tabla.
- Se aplica la primera regla de la tabla que coincide con los parámetros de tráfico.

No se pueden aplicar las reglas subsiguientes, ya que la búsqueda en ese paquete finaliza. Debido a este comportamiento, se recomienda siempre colocar las directivas más pormenorizadas al principio de la tabla. Esto garantizará que se apliquen antes que otras reglas más específicas.

La regla predeterminada, situada al final de la tabla, es una regla catch-all que aplicará los paquetes que no coincidan con ninguna otra regla. Tras la operación de preparación del host, la acción de la regla predeterminada se establece como Permitir. Esto asegura que la comunicación de máquina virtual a máquina virtual no se interrumpa durante las fases de almacenamiento o migración. Se recomienda cambiar la acción de la regla predeterminada a Bloquear y aplicar el control de acceso mediante un modelo de control positivo (por ejemplo, que solo el tráfico especificado en la regla de firewall se permita en la red).

Nota TCP estricto se puede habilitar en cada sección para desactivar la recogida de sesiones medias y exigir el requisito de un protocolo de enlace de tres vías. Cuando se habilita el modo TCP estricto en una sección de firewall distribuido en particular y se utiliza una regla de bloqueo ANY-ANY predeterminada, se descartan los paquetes que no completan los requisitos de conexión de protocolo de tres vías y que coinciden con una regla basada en TCP en esta sección. El modo TCP estricto solo se aplica a las reglas de TCP con estado y se habilita en el nivel de la sección de firewall distribuido. TCP estricto no se aplica a los paquetes que coinciden con el permiso ANY-ANY predeterminado, sin especificar ningún servicio TCP.

Tabla 20-1. Propiedades de una regla de firewall

Propiedad	Descripción
Nombre	Nombre de la regla de firewall.
ID	Identificador único generado por el sistema para cada regla.
Origen	El origen de la regla puede ser tanto una dirección IP o MAC como un objeto diferente. El origen coincidirá con cualquiera si no está definido. Tanto IPv4 como IPv6 son compatibles con el rango de origen o destino.
Destino	La dirección/máscara de red IP o MAC de destino de la conexión afectada por la regla. El destino coincidirá con cualquiera si no está definido. Tanto IPv4 como IPv6 son compatibles con el rango de origen o destino.
Servicio	El servicio puede ser una combinación de protocolos de puertos predeterminados para la Capa 3. Para la Capa 2 puede ser EtherType. Para las Capas 2 y 3, es posible definir de forma manual un nuevo servicio o grupo de servicio. El servicio coincidirá con cualquiera si no se especificó.
Se aplica a	Define el ámbito de aplicación de la regla. Si no está definido el ámbito incluirá todos los puertos lógicos. Si agregó "Se aplica a" a una sección, se sobrescribirá la regla.
Registrar	Se puede activar o desactivar el registro. Los registros se almacenan en el archivo <code>/var/log/dfwpktlogs.log</code> en los hosts ESX y KVM.

Tabla 20-1. Propiedades de una regla de firewall (continuación)

Propiedad	Descripción
Acción	La acción que aplica la regla puede ser Permitir , Quitar o Rechazar . La opción predeterminada es Permitir .
Protocolo IP	Las opciones son IPv4 , IPv6 e IPv4_IPv6 . El valor predeterminado es IPv4_IPv6 . Para acceder a esta propiedad, haga clic en el icono Configuración avanzada .
Dirección	Las opciones son Entrada , Salida y Entrada/salida . El valor predeterminado es Entrada/salida . Este campo hace referencia a la dirección del tráfico desde el punto de vista del objeto de destino. Entrada significa que solo se comprueba el tráfico que entra al objeto, Salida significa que solo se comprueba el tráfico que sale del objeto y Entrada/salida significa que se comprueba el tráfico en ambas direcciones. Para acceder a esta propiedad, haga clic en el icono Configuración avanzada .
Etiquetas de regla	Las etiquetas que se han agregado a la regla. Para acceder a esta propiedad, haga clic en el icono Configuración avanzada .
Estadísticas de flujo	Campo de lectura que muestra el byte, el recuento de paquetes y las sesiones. Para acceder a esta propiedad, haga clic en el icono de gráfico.

Nota Si Spoofguard no está habilitado, no se puede garantizar que los enlaces de direcciones detectados automáticamente sean de confianza, ya que una máquina virtual maliciosa puede reclamar la dirección de otra máquina virtual. Si SpoofGuard está habilitado, verifica cada enlace detectado, de forma que solo se presenten los enlaces aprobados.

Agregar una regla de firewall

Un firewall es un sistema de seguridad de red que supervisa y controla el tráfico de red entrante y saliente en función de las reglas de firewall predeterminadas.

Las reglas de firewall se agregan al ámbito de NSX Manager. Mediante el campo Se aplica a, se puede delimitar el ámbito en el que se desea aplicar la regla. Es posible agregar varios objetos en los niveles de origen y destino para cada regla, lo que permite reducir la cantidad total de reglas de firewall que se deben agregar.

Nota De forma predeterminada, una regla coincide con los elementos predeterminados de las reglas de origen, destino y servicio, coincidiendo con todas las interfaces y direcciones de tráfico. Si desea restringir el efecto de la regla en interfaces o direcciones de tráfico determinadas, debe especificar la restricción en la regla.

Requisitos previos

Para utilizar un grupo de direcciones, primero asocie de forma manual la dirección IP y MAC de cada máquina virtual con su conmutador lógico.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.

- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Haga clic en una regla o una sección.
- 4 Haga clic en el icono de menú en la primera columna de una regla y seleccione **Agregar regla anterior** o **Agregar regla siguiente**.

Aparece una nueva fila para definir la regla de firewall.

Nota Si el tráfico intenta acceder a través del firewall, la información del paquete está sujeta a las reglas en el orden que aparece en la Tabla de reglas, comenzando por el principio hasta las reglas predeterminadas situadas al final. En algunos casos, el orden de prioridad de dos o más reglas puede ser importante a la hora de determinar la disposición del paquete.

- 5 En la columna **Nombre**, escriba el nombre de la regla.
- 6 En la columna **Origen**, haga clic en el icono de edición y seleccione el origen de la regla. El origen coincidirá con cualquiera si no está definido.

Opción	Descripción
Direcciones IP	Introduzca varias direcciones IP o MAC en una lista separada por comas. La lista puede contener hasta 255 caracteres. Son compatibles los formatos IPv4 y IPv6.
Objetos de contenedor	Los objetos disponibles son Conjunto de direcciones IP, Puerto lógico, Conmutador lógico y Grupo NS. Seleccione los objetos y haga clic en Aceptar .

- 7 En la columna **Destino**, haga clic en el icono de edición y seleccione el destino. El destino coincidirá con cualquiera si no está definido.

Opción	Descripción
Direcciones IP	Puede introducir varias direcciones IP o MAC en una lista separada por comas. La lista puede contener hasta 255 caracteres. Son compatibles los formatos IPv4 y IPv6.
Objetos de contenedor	Los objetos disponibles son Conjunto de direcciones IP, Puerto lógico, Conmutador lógico y Grupo NS. Seleccione los objetos y haga clic en Aceptar .

- 8 En la columna **Servicio**, haga clic en el icono de edición y seleccione los servicios. El servicio coincidirá con cualquiera si no está definido.
- 9 Para seleccionar un servicio predefinido, seleccione uno o más de los servicios disponibles.

- 10 Para definir un nuevo servicio, haga clic en la pestaña **Protocolo de puertos sin formato** y haga clic en **Agregar**.

Opción	Descripción
Tipo de servicio	<ul style="list-style-type: none"> ■ ALG ■ ICMP ■ IGMP ■ IP ■ Conjunto de puertos de Capa 4
Protocolo	Seleccione uno de los protocolos disponibles.
Puertos de origen	Introduzca el puerto de origen.
Puertos de destino	Seleccione el puerto de destino.

- 11 En la columna **Se aplica a**, haga clic en el icono de edición y seleccione los objetos.

- 12 En la columna **Registro**, configure la opción de registro.

Los registros se almacenan en el archivo `/var/log/dfwpktlogs.log` en ESXi y los hosts KVM. Si el registro se habilita, el rendimiento puede verse afectado.

- 13 En la columna **Acción**, seleccione una acción.

Opción	Descripción
Permitir	Permite el acceso directo de todo el tráfico de Capa 3 y Capa 2 con el origen, destino y protocolo especificados a través del contexto de firewall presente. Los paquetes que coincidan con la regla, y que se acepten, atravesarán el sistema como si el firewall no estuviera presente.
Quitar	Descarta paquetes con el origen, destino y protocolo especificados. Descartar un paquete es una acción silenciosa que no envía ninguna notificación a los sistemas de origen y de destino. Al descartar el paquete, se intentará recuperar la conexión hasta que se alcance el umbral de reintentos.
Rechazar	Rechaza paquetes con el origen, destino y protocolo especificados. Rechazar un paquete es una manera más estable para denegarlo, ya que envía un mensaje de destino no alcanzable al remitente. Si el protocolo es TCP, se envía un mensaje TCP RST. Se envían mensajes ICMP con código prohibido de forma administrativa para conexiones UDP, ICMP y otras conexiones IP. Una ventaja de utilizar la opción Rechazar es que la aplicación que envía el mensaje recibe una notificación después de que se produzca un único intento de establecer conexión sin éxito.

- 14 Haga clic en el icono **Configuración avanzada** para especificar el protocolo de IP, la dirección, las etiquetas de regla y los comentarios.

- 15 Haga clic en **Publicar**.

Eliminar una regla de firewall

Un firewall es un sistema de seguridad de red que supervisa y controla el tráfico de red entrante y saliente en función de las reglas de firewall predeterminadas. Las reglas personalizadas definidas se pueden agregar y eliminar.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Haga clic en el icono de menú que aparece en la primera columna de la regla y seleccione **Eliminar regla**.
- 4 Haga clic en **Publicar**.

Editar la regla de Distributed Firewall predeterminada

Puede editar la configuración de firewall predeterminada que se aplica al tráfico que no coincide con ninguna de las reglas de firewall definidas por el usuario.

Las reglas de firewall predeterminadas se aplican al tráfico que no coincide con ninguna de las reglas de firewall definidas por el usuario. La regla de capa 3 predeterminada se encuentra en la pestaña **General** y la regla de capa 2 está en la pestaña **Ethernet**.

Las reglas de firewall predeterminadas permiten el acceso de todo el tráfico de capa 3 y capa 2 a los clústeres preparados en la infraestructura. La regla predeterminada se encuentra siempre al final de la tabla de reglas y no se puede eliminar. Sin embargo, puede cambiar el elemento **Acción** de la regla de **Permitir** a **Quitar** o **Rechazar** (no se recomienda) e indicar si el tráfico de esa regla se debe registrar.

La regla de firewall de capa 3 predeterminada se aplica a todo el tráfico, incluido DHCP. Si cambia el valor de **Acción** a **Quitar** o **Rechazar**, se bloqueará el tráfico DHCP. Tendrá que crear una regla para permitir el tráfico DHCP.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 En la columna **Nombre**, escriba un nuevo nombre.
- 4 En la columna **Acción**, seleccione una de las opciones.
 - Permitir: permite que todo el tráfico de Capa 3 y Capa 2 con el origen, el destino y el protocolo especificados atraviese el contexto de firewall actual. Los paquetes que coincidan con la regla y se acepten atraviesan el sistema como si el firewall no estuviese presente.

- **Descartar:** descarta los paquetes con el origen, el destino y el protocolo especificados. Descartar un paquete es una acción silenciosa que no envía ninguna notificación a los sistemas de origen y de destino. Al descartar el paquete, se intentará recuperar la conexión hasta que se alcance el umbral de reintentos.
- **Rechazar:** rechaza los paquetes con el origen, el destino y el protocolo especificados. Rechazar un paquete es una manera más estable para denegarlo, ya que envía un mensaje de destino no alcanzable al remitente. Si el protocolo es TCP, se envía un mensaje TCP RST. Se envían mensajes ICMP con código prohibido de forma administrativa para conexiones UDP, ICMP y otras conexiones IP. Una ventaja de utilizar la opción Rechazar es que la aplicación que envía el mensaje recibe una notificación después de que se produzca un único intento de establecer conexión sin éxito.

Nota No le recomendamos que seleccione **Rechazar** como la acción para la regla predeterminada.

- 5 En la opción **Registro**, habilite o deshabilite el registro.
Si el registro se habilita, el rendimiento puede verse afectado.
- 6 Haga clic en **Publicar**.

Cambiar el orden de una regla de firewall

Las reglas se procesan siguiendo un orden de arriba a abajo. Se puede cambiar el orden de las reglas en la lista.

En el caso de tráfico que intente acceder a través del firewall, la información del paquete está sujeta a reglas en el orden que aparece en la Tabla de reglas, comenzando por el principio hasta las reglas predeterminadas situadas al final. En algunos casos, el orden de prioridad de dos o más reglas puede ser importante a la hora de determinar el flujo de tráfico.

Es posible mover una regla personalizada hacia arriba o abajo en la tabla. La regla predeterminada siempre se coloca en la parte inferior de la tabla y no se puede mover.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 Seleccione la regla y haga clic en el icono **Mover hacia arriba** o **Mover hacia abajo** en la barra de menús.
- 4 Haga clic en **Publicar**.

Filtrar reglas de firewall

Cuando acceda por primera vez a la sección del firewall, aparecen todas las reglas. Puede aplicar un filtro para controlar qué se muestra, para así ver solamente un subgrupo de reglas. Esto puede facilitar la administración de las reglas.

Procedimiento

- 1 Seleccione **Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido**.
- 2 Haga clic en la pestaña **General** para las reglas de Capa 3 o en la pestaña **Ethernet** para las reglas de Capa 2.
- 3 En el campo de texto de búsqueda que se encuentra en el lado derecho de la barra de menús, seleccione un objeto o introduzca los primeros caracteres de un nombre para delimitar la lista de objetos que puede seleccionar.

Después de seleccionar un objeto, se aplica el filtro y se actualiza la lista de reglas, mostrando únicamente las reglas que contienen el objeto en cualquiera de las siguientes columnas:

- Orígenes
 - Destinos
 - Se aplica a
 - Servicios
- 4 Para eliminar el filtro, borre el nombre del objeto del campo de texto.

Es posible que necesite cambiar la configuración de los dispositivos instalados (por ejemplo, añadir licencias y certificados, así como cambiar contraseñas). También hay tareas de mantenimiento rutinarias que debe llevar a cabo, como realizar copias de seguridad. Además, hay herramientas que le ayudarán a encontrar información sobre los dispositivos que forman parte de la infraestructura de NSX-T Data Center y las redes lógicas que crea NSX-T Data Center, como el registro del sistema remoto, Traceflow y las conexiones de puertos.

Este capítulo incluye los siguientes temas:

- Ver los paneles de control de supervisión
- Ver el uso y la capacidad de las categorías de objetos
- Comprobar el estado de realización de un cambio de configuración
- Buscar objetos
- Filtrar por atributos de objeto
- Agregar un administrador de equipos
- Agregar una instancia de Active Directory
- Agregar un servidor LDAP
- Sincronizar Active Directory
- Administrar las cuentas de usuarios y el control de acceso basado en funciones
- Restaurar y hacer copias de seguridad de NSX Manager
- Quitar una extensión NSX-T Data Center de vCenter Server
- Administrar el clúster de NSX Manager
- Reemplazar un nodo de transporte de NSX Edge en un clúster de NSX Edge
- Recuperar NSX-T cuando se pierde vCenter Server y no se puede recuperar
- Implementación multisitio de NSX-T Data Center
- Configurar dispositivos
- Agregar una clave de licencia y generar un informe de uso de licencias
- Configurar certificados

- Configuración basada en cumplimiento
- Recopilar paquetes de soporte
- Mensajes de registro y códigos de error
- Programa de mejora de la experiencia de cliente
- Agregar etiquetas a un objeto
- Buscar la huella digital SSH de un servidor remoto
- Ver datos de aplicaciones que se ejecutan en máquinas virtuales
- Configurar un equilibrador de carga externo

Ver los paneles de control de supervisión

La interfaz de NSX Manager ofrece numerosos paneles de control de supervisión que muestran detalles sobre el estado del sistema, la seguridad y las redes, y los informes de cumplimiento. Se puede acceder a esta información a través de la interfaz de NSX Manager, pero también se puede consultar en conjunto en la página **Inicio > Paneles de control de supervisión**.

Puede acceder a los paneles de control de desde la página Inicio de la interfaz de NSX Manager. En los paneles de control, puede hacer clic y acceder a las páginas de origen de las que se obtienen los datos del panel.

Procedimiento

- 1 Inicie sesión como administrador en la interfaz de NSX Manager.
- 2 Haga clic en **Inicio** si aún no está en la página de inicio.
- 3 Haga clic en Paneles de control de supervisión y seleccione la categoría en el menú desplegable.

La página muestra los paneles de control de las categorías seleccionadas. Los gráficos del panel de control están codificados por colores, y la clave de código de color se muestra directamente sobre los paneles.

- 4 Para acceder a un nivel más detallado, haga clic en el título del panel de control o en uno de sus elementos, si está activado.

En las siguientes tablas se describen los paneles de control predeterminados y el origen de la información que muestran.

Tabla 21-1. Paneles del sistema

Panel de control	Orígenes	Descripción
Sistema	Sistema > Dispositivos > Información general	Muestra el estado y el consumo de recursos (CPU, memoria, disco) del clúster de NSX Manager.
Tejido	Sistema > Tejido > Nodos Sistema > Tejido > Zonas de transporte Sistema > Tejido > Administradores de equipos	Muestra el estado del tejido de NSX-T, incluidos los nodos de transporte de Edge y host, las zonas de transporte y los administradores de equipos.
Copias de seguridad	Sistema > Copia de seguridad y restauración	Muestra el estado de las copias de seguridad de NSX-T, si están configuradas. Se recomienda configurar copias de seguridad programadas que se almacenen de forma remota en un sitio SFTP.
Protección de endpoints	Sistema > Implementaciones de servicio	Muestra el estado de la implementación de protección de endpoints.

Tabla 21-2. Paneles de control de redes y seguridad

Panel de control	Orígenes	Descripción
Seguridad	Inventario > Grupos Seguridad > Firewall distribuido	Muestra el estado de los grupos y las directivas de seguridad. Un grupo es un conjunto de cargas de trabajo, segmentos, puertos de segmentos y direcciones IP en el que se pueden aplicar directivas de seguridad, como reglas de firewall de este a oeste.
Puertas de enlace	Redes > Puertas de enlace de nivel 0 Redes > Puertas de enlace de nivel 1	Muestra el estado de las puertas de enlace de nivel 0 y 1.
Segmentos	Redes > Segmentos	Muestra el estado de segmentos de red.
Equilibradores de carga	Redes > Equilibrio de carga	Muestra el estado de las máquinas virtuales del equilibrador de carga.
VPN	Redes > VPN	Muestra el estado de las redes privadas virtuales.

Tabla 21-3. Paneles de Opciones avanzadas de redes y seguridad

Panel de control	Orígenes	Descripción
Equilibradores de carga	Opciones avanzadas de redes y seguridad > Equilibradores de carga	Muestra el estado de los servicios del equilibrador de carga, los servidores virtuales del equilibrador de carga y los grupos de servidores del equilibrador de carga. Un equilibrador de carga puede alojar uno o varios servidores virtuales. Un servidor virtual está vinculado a un grupo de servidores que incluye aplicaciones que alojan miembros.
Firewall	Opciones avanzadas de redes y seguridad > Seguridad > Firewall distribuido Opciones avanzadas de redes y seguridad > Seguridad > Firewall de puente Opciones avanzadas de redes y seguridad > Redes > Enrutadores	Indica si el firewall está habilitado y muestra el número de directivas, reglas y miembros de la lista de exclusiones. Nota Cada elemento detallado que se muestra en este panel se origina de una subpestaña específica de la página de origen citada.
VPN	No aplicable.	Muestra el estado de las redes privadas virtuales y el número de sesiones de IPSec y VPN de nivel 2 abiertas.
Conmutación	Opciones avanzadas de redes y seguridad > Conmutación	Muestra el estado de los conmutadores lógicos y los puertos lógicos, incluidos los puertos de máquina virtual y de contenedor.

Tabla 21-4. Panel de control del informe de cumplimiento

Columna	Descripción
Código de no cumplimiento	Muestra el código de no cumplimiento específico.
Descripción	Causa específica del estado de no cumplimiento.
Nombre de recurso	El recurso NSX-T (nodo, conmutador y perfil) que incumple.
Tipo de recurso	Tipo de recurso de causa.
Recursos afectados	Número de recursos afectados. Haga clic en el valor numérico para ver una lista.

Consulte [Códigos de informe de estado de cumplimiento](#) para obtener más información sobre cada uno de los códigos de los informes de cumplimiento.

Ver el uso y la capacidad de las categorías de objetos

Puede ver el uso y la capacidad de varias categorías de objetos en el entorno de NSX-T Data Center. También puede establecer alertas que le permitan ver fácilmente cuándo se alcanzan ciertos umbrales de uso.

Para ver el uso y la capacidad de diferentes categorías de objetos, haga clic en una de las siguientes pestañas:

- **Redes > Información general de la red > Capacidad**
- **Seguridad > Información general de seguridad > Capacidad**
- **Inventario > Información general del inventario > Capacidad**
- **Sistema > Información general del sistema > Capacidad**

También puede desplazarse hasta **Planificar y solucionar problemas > Capacidad consolidada** para ver todas las categorías de objetos en una misma página.

En las páginas de capacidad, por cada categoría de objeto se muestra la siguiente información:

- Capacidad máxima: este valor se basa en la capacidad de un dispositivo de gran tamaño.
- Inventario actual (realizado): el número de objetos creados o configurados correctamente. Este número refleja los objetos de NSX Manager que se muestran en la pestaña **Opciones avanzadas de redes y seguridad**. Estos objetos pueden incluir algunos de los que cree en las pestañas **Redes**, **Seguridad**, **Inventario** o **Sistema**. Aparece una barra codificada por colores para indicar el porcentaje de uso. Si el uso está por debajo del nivel de alerta de advertencia, la barra será de color verde. Si el uso está por encima del nivel de alerta de advertencia, pero por debajo del nivel de alerta crítico, la barra será de color naranja. Si el uso supera el nivel de alerta crítico, la barra será de color rojo.
- Alerta de advertencia: indica el nivel de uso en el que la barra mencionada anteriormente se muestra de color naranja. Puede cambiar este valor.
- Alerta crítica: indica el nivel de uso en el que la barra mencionada anteriormente se muestra de color rojo. Puede cambiar este valor.

Si cambia el valor de la alerta de advertencia o la alerta crítica, puede hacer clic en **Revertir** para volver al último valor guardado. También puede hacer clic en **Restablecer valores** para restaurar los valores predeterminados de todas las categorías de objetos.

La página de capacidad de redes muestra las siguientes categorías de objetos:

- Enrutadores lógicos de nivel 0
- Enrutadores lógicos de nivel 1
- Listas de prefijos
- Reglas NAT de todo el sistema
- Instancias de servidor DHCP
- Rangos/grupos de DHCP en todo el sistema
- Enrutadores lógicos de nivel 1 con regla NAT habilitada
- Conmutadores lógicos
- Puertos de conmutadores lógicos de todo el sistema

La página de capacidad de seguridad muestra las siguientes categorías de objetos:

- Hosts con protección de endpoints en todo el sistema habilitada
- Máquinas virtuales con protección de endpoints en todo el sistema habilitada
- Grupos de Active Directory
- Dominios de Active Directory
- Reglas de firewall distribuido
- Reglas de firewall de todo el sistema
- Secciones de firewall de todo el sistema
- Secciones de firewall distribuido

La página de capacidad de inventario muestra las siguientes categorías de objetos:

- Grupos de redes y seguridad
- Conjuntos de direcciones IP
- Grupos basados en conjuntos de direcciones IP
- Clústeres de vCenter
- Hosts de hipervisor

La página de capacidad de sistema muestra las siguientes categorías de objetos:

- Interfaces virtuales de todo el sistema
- Clústeres de Edge
- Nodos de Edge de todo el sistema

Comprobar el estado de realización de un cambio de configuración

Cuando se realiza un cambio de configuración, NSX Manager por lo general envía una solicitud a otro componente para implementar el cambio. En algunas entidades de Capa 3, si realiza el cambio de configuración mediante la API, puede rastrear el estado de la solicitud para ver si el cambio se implementó correctamente.

El cambio de configuración que se inicia se denomina “estado deseado”. El resultado de implementar el cambio se denomina “estado realizado”. Si NSX Manager implementa el cambio correctamente, el estado realizado será el mismo que el estado deseado. Si se produce un error, el estado realizado no coincidirá con el estado deseado.

En algunas entidades de Capa 3, cuando se llama a una API para realizar un cambio de configuración, la respuesta incluye el parámetro `request_id`. Puede utilizar los parámetros `request_id` y `entity_id` para realizar una llamada API a fin de averiguar el estado de la solicitud.

Esta función es compatible con las siguientes entidades y API:

```

EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>

AdvertisementConfig
  PUT /logical-routers/<logical-router-id>/routing/advertisement

AdvertiseRouteList
  PUT /logical-routers/<logical-router-id>/routing/advertisement/rules

NatRule
  POST /logical-routers/<logical-router-id>/nat/rules
  PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>
  DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>

DhcpRelayService
  POST /dhcp/relays
  PUT /dhcp/relays/<relay-id>
  DELETE /dhcp/relays/<relay-id>

```

```

DhcpRelayProfile
  POST /dhcp/relay-profiles
  PUT /dhcp/relay-profiles/<relay-profile-id>
  DELETE /dhcp/relay-profiles/<relay-profile-id>

StaticHopBfdPeer
  POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
  PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>

IPPrefixList
  POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
  PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>

RouteMap
  POST /logical-routers/<logical-router-id>/routing/route-maps
  PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
  DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>

RedistributionConfig
  PUT /logical-routers/<logical-router-id>/routing/redistribution
RedistributionRuleList
  PUT /logical-routers/<logical-router-id>/routing/redistribution/rules

BfdConfig
  PUT /logical-routers/<logical-router-id>/routing/bfd-config

MplsConfig
  PUT /logical-routers/<logical-router-id>/routing/mppls

RoutingGlobalConfig
  PUT /logical-routers/<logical-router-id>/routing

IPSecVPNIKEProfile
  POST /vpn/ipsec/ike-profiles
  PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
  DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>

IPSecVPNDPDProfile
  POST /vpn/ipsec/dpd-profiles
  PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
  DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>

IPSecVPNTunnelProfile
  POST /vpn/ipsec/tunnel-profiles
  PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
  DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>

IPSecVPNLocalEndpoint
  POST /vpn/ipsec/local-endpoints
  PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
  DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>

```

```

IPSecVPNPeerEndpoint
  POST /vpn/ipsec/peer-endpoints
  PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
  DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>

IPSecVPNService
  POST /vpn/ipsec/services
  PUT /vpn/ipsec/services/<service-id>
  DELETE /vpn/ipsec/services/<service-id>

IPSecVPNSession
  POST /vpn/ipsec/sessions
  PUT /vpn/ipsec/sessions/<session-id>
  DELETE /vpn/ipsec/sessions/<session-id>

DhcpServer
  POST /dhcp/servers
  PUT /dhcp/servers/<server-id>
  DELETE /dhcp/servers/<server-id>

DhcpStaticBinding
  POST /dhcp/servers/static-bindings
  PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
  DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>

DhcpIpPool
  POST /dhcp/servers/ip-pools
  PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
  DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>

DnsForwarder
  POST /dns/forwarders
  PUT /dns/forwarders/<forwarder-id>
  DELETE /dns/forwarders/<forwarder-id>

```

Puede llamar a las siguientes API para obtener los estados realizados:

```

EdgeCluster
Request - GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>
Response - An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the
edge cluster is deleted then the state will be unknown and it will return the common entity
not found error.

LogicalRouter / All L3 Entites - All L3 entities can use this API to get realization state
Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of
logical router but if the logical router itself is deleted then the state will be unknown and
it will return the common entity not found error.

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API
to get the realization state
Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-
id>
Response - An instance of LogicalServiceRouterClusterState which will inherit

```

```

ConfigurationState.

LogicalRouterPort / DhcprelayService / DhcprelayProfile
Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint /
IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession
Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>
Response - An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If
the session is deleted then the state will be unknown and it will return the common entity
not found error. When IPSecVPNService is disabled, IKE itself is down and it does not
respond. It will return unknown state in such a case.

DhcpServer
Request - GET /dhcp/servers/<server-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpStaticBinding
Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?
request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpIpPool
Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DnsForwarder
Request - GET /dns/forwarders/<forwarder-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

```

Para obtener más información acerca de las API, consulte la *Referencia de API de NSX-T Data Center*.

Buscar objetos

Puede buscar objetos usando varios criterios en el inventario de NSX-T Data Center.

Los resultados de la búsqueda se ordenan por relevancia y puede filtrar esos resultados según la consulta de búsqueda.

Nota Si tiene caracteres especiales en la consulta de búsqueda que también actúen como operadores, debe agregar una barra diagonal inversa inicial. Los caracteres que funcionan como los operadores son: +, -, =, &&, ||, <, >, !, (,), {, }, [,], ^, ", ~, ?, :, / y \.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.

- 2 En la página principal, introduzca un patrón de búsqueda para un objeto o un tipo de objeto.


A medida que introduce el patrón de búsqueda, la función de búsqueda ofrece asistencia mostrando las palabras clave aplicables.

Buscar	Consulta de búsqueda
Objetos que contengan Lógico como nombre o propiedad	Logical
Nombre exacto del conmutador lógico	nombre_para_mostrar:LSP-301
Nombres con caracteres especiales, como !	Logical\!

Todos los resultados de búsqueda relacionados se enumeran y se agrupan por tipo de recurso en diferentes pestañas.

Puede hacer clic en las pestañas de resultados de búsqueda específicos para un tipo de recurso.

- 3 (opcional) En la barra de búsqueda, haga clic en el icono Guardar para guardar los criterios de búsqueda que se restringieron.

- 4 En la barra de búsqueda, haga clic en el icono  para abrir la columna de búsqueda avanzada, donde podrá restringir la búsqueda.

- 5 Especifique uno o varios criterios para restringir la búsqueda.

- Nombre
- Tipo de recurso
- Descripción
- ID
- Creado por
- Modificado por
- Etiquetas
- Fecha de creación
- Fecha de modificación

También puede ver los resultados de búsquedas recientes y los criterios de búsqueda guardados.

- 6 (opcional) Haga clic en **Borrar todo** para restablecer los criterios de búsqueda avanzada.

Filtrar por atributos de objeto


Cuando vea objetos en NSX Manager, puede filtrarlos por uno o varios de sus atributos. Por ejemplo, cuando esté viendo los detalles de las puertas de enlace de nivel 0, podrá filtrarlos por **Estado** y ver solo las puertas de enlace que estén **inactivas**.

Están disponibles los siguientes tipos de filtros:

- Filtros predefinidos: una lista de los filtros utilizados más frecuentemente que se pueden aplicar a los objetos.
- Filtro basado en texto: filtro basado en el valor de atributo que introduzca. Este filtro solo se aplica a los atributos **Nombre**, **Etiqueta**, **Ruta de acceso** y **Descripción** de los objetos.
- Pares atributo-valor: un menú desplegable de atributos que se puede utilizar para especificar pares atributo-valor con los que filtrar.

Puede utilizar varios atributos de un objeto o varios valores de un solo atributo para filtrar objetos. El operador AND se aplica cuando se seleccionan varios atributos, mientras que el operador OR se utiliza cuando se especifican varios valores de un solo atributo.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese hasta la pestaña que incluye los objetos que desea ver.
- 3 Especifique los atributos que desea utilizar para filtrar los objetos.
 - Haga clic en  y seleccione los filtros de la lista de filtros predefinidos.
 - Introduzca un valor para los atributos **Nombre**, **Etiqueta**, **Ruta de acceso** o **Descripción**.
 - Seleccione un atributo en el menú desplegable y especifique su valor. Por ejemplo:
Estado: Inactivo

Se mostrarán los objetos que cumplen los criterios de filtro.

- 4 (opcional) Haga clic en **Borrar** para restablecer los filtros.

Agregar un administrador de equipos

Un administrador de equipos, por ejemplo vCenter Server, es una aplicación que administra recursos, como hosts y máquinas virtuales.

NSX-T Data Center sondea los administradores de equipos para recopilar información del clúster de vCenter Server.

Al agregar un administrador de equipo de vCenter Server, debe proporcionar las credenciales de un usuario de vCenter Server. Puede proporcionar las credenciales del administrador de vCenter Server o crear específicamente una función y un usuario para NSX-T Data Center y proporcionar las credenciales de este usuario. Esta función debe tener los siguientes privilegios de vCenter Server:

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

Para obtener más información sobre las funciones y los privilegios de vCenter Server, consulte el documento *Seguridad de vSphere*.

Requisitos previos

- Compruebe que usa la versión compatible de vSphere. Consulte [Versión de vSphere admitida](#).
- Comunicación de IPv6 e IPv4 con vCenter Server.

- Compruebe que usa el número recomendado de administradores de equipos. Consulte <https://configmax.vmware.com/home>.

Nota NSX-T Data Center no es compatible con el mismo vCenter Server para registrarse con más de un NSX Manager.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Tejido > Administradores de equipos > Agregar**.
- 3 Complete la información de los administradores de equipos.

Opción	Descripción
Nombre y descripción	<p>Escriba el nombre para identificar vCenter Server.</p> <p>De forma opcional, puede incluir cualquier información especial, como el número de clústeres en vCenter Server.</p>
Dirección IP o nombre de dominio	Especifique la dirección IP de vCenter Server.
Tipo	Mantenga la opción predeterminada.
Nombre de usuario y contraseña	Escriba las credenciales para iniciar sesión en vCenter Server.
Huella digital	Escriba el valor del algoritmo de huella digital SHA-256 de vCenter Server.

Si deja el valor de huella digital en blanco, se le solicitará que acepte la huella digital que proporciona el servidor.

Tras aceptar la huella digital, NSX-T Data Center tarda unos segundos en detectar y registrar los recursos de vCenter Server.

- 4 Si el icono de progreso cambia de **En curso** a **No registrado**, realice los siguientes pasos para resolver el error.
 - a Seleccione el mensaje de error y haga clic en **Resolver**. Un posible mensaje de error será el siguiente:

Extension already registered at CM <vCenter Server name> with id <extension ID>

- b Introduzca las credenciales de vCenter Server y haga clic en **Resolver**.
Si ya existe un registro, se reemplazará.

Resultados

El administrador de equipos tarda un poco en registrarse en vCenter Server, y lo mismo sucede para que el estado de conexión aparezca como **Activo**.

Puede hacer clic en el nombre del administrador de equipos para ver su información, para editarlo, o bien para administrar las etiquetas que se aplican a este.

Una vez que vCenter Server se registre correctamente, no apague ni elimine la máquina virtual de NSX Manager sin eliminar primero el administrador de recursos de equipos. De lo contrario, cuando implemente una instancia de NSX Manager nueva, no podrá volver a registrar el mismo vCenter Server. Aparecerá un mensaje de error para indicarle que vCenter Server ya está registrado con otra instancia de NSX Manager.

Agregar una instancia de Active Directory

Active Directory se utiliza para crear reglas de firewall de identidad establecidas por el usuario.

No se admite Windows 2008 como servidor de Active Directory ni como sistema operativo del servidor RDSH.

Puede registrar uno o varios dominios de Windows en NSX Manager. NSX Manager obtiene información del grupo y del usuario, así como de la relación existente entre estos elementos, desde cada dominio con el que está registrado. NSX Manager también recupera las credenciales de Active Directory (AD).

Una vez que Active Directory se sincroniza con NSX Manager, puede crear grupos de seguridad basados en la identidad del usuario, así como crear reglas de firewall basadas en identidad.

Nota Para aplicar la regla del firewall de identidad, el servicio hora de Windows debe estar **activado** para todas las máquinas virtuales que utilicen Active Directory. De esta forma, se asegurará de que la fecha y la hora de Active Directory y de las máquinas virtuales estén sincronizadas. Los cambios en la pertenencia al grupo de AD (incluida la habilitación y eliminación de usuarios) no se aplican inmediatamente a los usuarios que hayan iniciado sesión. Para que los cambios se apliquen, los usuarios deben cerrar sesión y volver a iniciarla. Los administradores de AD deben forzar el cierre de sesión cuando se modifique la pertenencia al grupo. Este comportamiento es una limitación de Active Directory.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Sistema > Active Directory**.
- 3 Haga clic en **Agregar Active Directory**.
- 4 Introduzca el nombre de Active Directory.
- 5 Escriba el **Nombre de NetBIOS** y el **Nombre distintivo de la base**.

Para recuperar el nombre netBIOS del dominio, introduzca `nbtstat -n` en una ventana de comandos de una estación de trabajo con Windows que sea parte de un dominio o se encuentre en un controlador de dominio. En la Tabla de nombre local NetBIOS (NetBIOS Local Name Table), la entrada con el prefijo <00> y el tipo Grupo (Group) es el nombre de NetBIOS.

Se necesita un nombre distintivo base (DN base) para agregar un dominio de Active Directory. Un DN base es el punto de partida que utiliza un servidor LDAP al buscar la autenticación de usuarios en un dominio de Active Directory. Por ejemplo, si el nombre de dominio es corp.local, el DN del DN base para Active Directory sería "DC=corp,DC=local".

- 6 Establezca el **Intervalo de sincronización diferencial** si es necesario. Una sincronización diferencial actualiza los objetos AD locales que han cambiado desde el último evento de sincronización.

Los cambios realizados en Active Directory no se verán en el NSX Manager hasta que se haya realizado una sincronización completa o diferencial.

- 7 Haga clic en **Guardar**.

Agregar un servidor LDAP

La configuración y la funcionalidad del servidor de LDAP (Lightweight Directory Access Protocol) solo se utiliza con el firewall de identidad. LDAP proporciona una ubicación central para la autenticación, lo que significa que, cuando se configura una conexión con el servidor LDAP, los registros de usuario se almacenan en el servidor LDAP externo.

Requisitos previos

La cuenta de dominio debe tener permisos de lectura de AD para todos los objetos en el árbol de dominios. La cuenta del lector de registros de eventos debe tener permisos de lectura para los registros de eventos de seguridad.

Cuando hay un clúster de NSX Manager, todos los nodos necesitan poder comunicarse con el servidor LDAP.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Sistema > Active Directory**.
- 3 Seleccione la pestaña **Servidor LDAP**.
- 4 Haga clic en **Agregar servidor LDAP**.
- 5 Introduzca el **Nombre de host** del servidor LDAP.
- 6 Seleccione la sesión de Active Directory a la que está conectado el servidor LDAP en el menú desplegable **Conectado a (Active Directory)**.
- 7 (opcional) Seleccione el **Protocolo**: LDAP (no protegido) o LDAPS (protegido).
- 8 Si seleccionó LDAPS, haga clic en la huella digital SHA-256 sugerida por NSX Manager o introduzca una huella digital SHA-256.

9 Introduzca el **Número de puerto** del servidor LDAP.

Para los controladores de dominio locales, los puertos 389 y 636 predeterminados del servidor LDAP se utilizan en la sincronización de Active Directory, y no se deben modificar los valores predeterminados.

10 Introduzca el **nombre de usuario** y la **contraseña** de una cuenta de Active Directory con un mínimo de acceso de solo lectura en el dominio de Active Directory.

11 Haga clic en **Guardar**.

12 Para comprobar que puede conectarse al servidor LDAP, haga clic en **Probar conexión**.

Sincronizar Active Directory

Pueden usarse los objetos de Active Directory para crear grupos de seguridad basados en identidades de usuario y reglas de firewall basadas en identidades.

Si utiliza la API para finalizar manualmente una sincronización completa después de que haya comenzado, las estadísticas de sincronización no se actualizarán correctamente.

Nota IDFW se basa en la seguridad y la integridad del sistema operativo invitado. Existen varios métodos para que un Local Manager malintencionado suplante su identidad para omitir las reglas de firewall. Guest Introspection Agent de las máquinas virtuales invitadas proporciona la información de identidad del usuario. Los administradores de seguridad deben asegurarse de que NSX Guest Introspection Agent esté instalado y en ejecución en cada máquina virtual invitada. Los usuarios que iniciaron sesión no deben tener el privilegio para eliminar o detener el agente.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Desplácese a **Sistema > Active Directory**.
- 3 Haga clic en el icono de menú de tres botones junto a la instancia de Active Directory que desea sincronizar y seleccione una de las siguientes opciones:

Elemento del menú	Descripción
Sincronizar diferencial	Realice una sincronización diferencial, donde se actualizan los objetos locales de Active Directory que cambiaron desde la última sincronización.
Sincronizar todo	Realice una sincronización completa, donde se actualiza el estado local de todos los objetos de Active Directory.

- 4 Haga clic en **Ver estado de sincronización** para ver el estado actual de Active Directory, el estado de sincronización anterior, el estado de sincronización y la última hora de sincronización.

Administrar las cuentas de usuarios y el control de acceso basado en funciones

Los dispositivos de NSX-T Data Center tienen dos usuarios integrados: el administrador y la auditoría. Puede integrar NSX-T Data Center a VMware Identity Manager (vIDM) y configurar el control de acceso basado en funciones (role-based access control, RBAC) para los usuarios que vIDM administra.

Para los usuarios que administra vIDM, la directiva de autenticación que se aplica es la que configuró el administrador de vIDM, no la directiva de autenticación de NSX-T Data Center, la cual se aplica solo a los usuarios de administración y de auditoría.

Administrar una contraseña de usuario

Cada dispositivo NSX Manager y NSX Edge tiene tres cuentas locales: administrador, auditoría y raíz (root). Puede administrar la contraseña de estos usuarios, pero no puede agregar ni eliminar usuarios.

El usuario de auditoría no está activo de forma predeterminada. Para activarlo, inicie sesión como administrador, ejecute el comando `set user audit` e introduzca una nueva contraseña. Cuando se le solicite la contraseña actual, pulse la tecla Intro.

De forma predeterminada, las contraseñas de usuario caducan a los 90 días. Puede cambiar o deshabilitar la caducidad de las contraseñas de cada usuario.

Cuando la contraseña de un usuario local en NSX Manager caduca dentro del plazo de 30 días, la interfaz web de NSX Manager muestra una notificación de caducidad de contraseña. Si establece la caducidad de la contraseña de un usuario local en 30 días o menos, la notificación siempre estará presente.

A partir de NSX-T Data Center 2.5.1, la notificación incluye un vínculo "Cambiar contraseña". Haga clic en el vínculo para cambiar la contraseña del usuario local desde la interfaz web.

Requisitos previos

Familiarícese con los requisitos de nivel de complejidad de las contraseñas de NSX Manager y NSX Edge. Consulte las secciones "Instalación de NSX Manager" e "Instalación de NSX Edge" en la *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 Inicie sesión en la CLI del dispositivo.
- 2 Para cambiar la contraseña, ejecute el comando `set user`. Por ejemplo:

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

- 3 Para obtener la información sobre la caducidad de la contraseña, ejecute el comando `get user <username> password-expiration`. Por ejemplo:

```
nsx> get user admin password-expiration
Password expires 90 days after last change
nsx>
```

- 4 Para establecer el tiempo de caducidad de la contraseña en días, ejecute el comando `set user <username> password-expiration <number of days>`. Por ejemplo:

```
nsx> set user admin password-expiration 120
nsx>
```

- 5 Para deshabilitar la caducidad de la contraseña, ejecute el comando `clear user <username> password-expiration`. Por ejemplo:

```
nsx> clear user admin password-expiration
nsx>
```

Restablecer las contraseñas de un dispositivo

El siguiente procedimiento se aplica a los dispositivos de NSX Manager, NSX Edge y Cloud Service Manager.

Nota Si tiene un clúster de NSX Manager, al restablecer la contraseña del usuario de `root`, `admin` o `audit` en una instancia de NSX Manager, se restablecerá la contraseña de las demás instancias de NSX Manager del clúster automáticamente. Tenga en cuenta que la sincronización de la contraseña puede tardar más de varios minutos.

Si ha cambiado el nombre del usuario `admin` o `audit`, utilice el nuevo nombre en los siguientes procedimientos.

Cuando se reinicia un dispositivo, el menú de arranque de GRUB no aparece de forma predeterminada. El siguiente procedimiento requiere que haya configurado GRUB para que muestre el menú de arranque de GRUB. Para obtener más información sobre cómo configurar GRUB y cambiar la contraseña `root` de GRUB, consulte "Configurar NSX-T Data Center para que aparezca el menú GRUB durante el arranque" en la *Guía de instalación de NSX-T Data Center*.

Si está ejecutando NSX-T Data Center 2.5.2 o una versión posterior y conoce la contraseña de `root`, pero olvidó la contraseña de `admin` o `audit`, puede restablecerla mediante el siguiente procedimiento:

- 1 Inicie sesión en el dispositivo como `root`.
- 2 Para NSX Edge, ejecute el comando `/etc/init.d/nsx-edge-api-server stop`. De lo contrario, ejecute el comando `/etc/init.d/nsx-mp-api-server stop`.
- 3 Para restablecer la contraseña de `admin`, ejecute el comando `passwd admin`.
- 4 Para restablecer la contraseña de `audit`, ejecute el comando `passwd audit`.

- 5 Ejecute el comando `touch /var/vmware/nsx/reset_cluster_credentials`.
- 6 Para NSX Edge, ejecute el comando `/etc/init.d/nsx-edge-api-server start`. De lo contrario, ejecute el comando `/etc/init.d/nsx-mp-api-server start`.

Si olvidó la contraseña de usuario de `root`, puede restablecerla siguiendo este procedimiento. Si está ejecutando NSX-T Data Center 2.5.0 o 2.5.1 y desea restablecer la contraseña de `admin` y `audit`, utilice también el siguiente procedimiento. Si está ejecutando NSX-T Data Center 2.5.2 o una versión posterior, puede utilizar el procedimiento anterior para restablecer la contraseña de `admin` o `audit` después de restablecer la contraseña de `root`.

Procedimiento

- 1 Conéctese a la consola del dispositivo.
- 2 Reinicie el sistema.
- 3 Cuando aparezca el menú de arranque GRUB, pulse rápidamente la tecla **MAYÚS** izquierda o **ESC**. Si espera demasiado y la secuencia de arranque no se pausa, debe volver a reiniciar el sistema.
- 4 Presione **e** para editar el menú.

Introduzca el nombre de usuario (`root`) y la contraseña de GRUB para `root` (distinta que para `root` de usuario del dispositivo).
- 5 Mantenga el cursor en la selección de Ubuntu.
- 6 Presione **e** para editar la opción seleccionada.
- 7 Busque la línea que comienza con `linux`.
- 8 Si está ejecutando NSX-T Data Center 2.5.0 o 2.5.1, realice los siguientes pasos:
 - a Elimine todas las opciones después de `root=UUID=<ID number>` y agregue `rw single init=/bin/bash` después del UUID.
 - b Presione **Ctrl-X** para arrancar.
 - c Cuando los mensajes de registro se detengan, presione Entrar.
Verá el mensaje `root@ (none) :/#`.
 - d Si desea restablecer la contraseña de `root`, ejecute el comando `passwd`.

Si desea restablecer la contraseña de `admin` o `audit`, ejecute el comando `passwd <admin or audit user ID>`.

Puede ejecutar el comando `passwd` varias veces.
 - e Introduzca una nueva contraseña y vuelva a introducirla para confirmarla.
 - f Si desea restablecer la contraseña de una instancia de NSX Manager, ejecute el comando `touch /var/vmware/nsx/reset_cluster_credentials`.

- g Ejecute el comando `sync`.
 - h Ejecute el comando `reboot -f`.
- 9 Si está ejecutando NSX-T Data Center 2.5.2 o versiones posteriores, realice los siguientes pasos:
- a Agregue `systemd.wants=PasswordRecovery.service` al final de la línea.
 - b Presione **Ctrl-X** para arrancar.
 - c Introduzca una nueva contraseña para `root` y vuelva a introducirla para confirmarla.

Una vez que se complete el proceso de arranque, puede comprobar el cambio de contraseña iniciando sesión como `root` con la nueva contraseña.

Configuración de la directiva de autenticación

Puede ver o cambiar la configuración de la directiva de autenticación utilizando la CLI.

Puede consultar o establecer la longitud mínima de la contraseña con los siguientes comandos:

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

Se aplican los siguientes comandos para iniciar sesión en la interfaz de usuario de NSX Manager o realizar una llamada de API:

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

Se aplican los siguientes comandos para iniciar sesión en la CLI de un nodo de NSX Manager o de NSX Edge:

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

Para obtener más información sobre los comandos de la CLI, consulte la *referencia de la interfaz de la línea de comandos de NSX-T*.

De forma predeterminada, después de cinco intentos consecutivos fallidos de iniciar sesión en la interfaz de usuario de NSX Manager, la cuenta del administrador se bloquea durante 15 minutos. Puede usar el siguiente comando para deshabilitar el bloqueo de la cuenta:

```
set auth-policy api lockout-period 0
```

De forma similar, puede usar el siguiente comando de la CLI para deshabilitar el bloqueo de la cuenta:

```
set auth-policy cli lockout-period 0
```

Obtener la huella digital del certificado desde un host de vIDM

Antes de configurar la integración de vIDM con NSX-T, debe obtener la huella digital del certificado desde el host de vIDM.

Debe usar la versión 1.x o una posterior de OpenSSL para la huella digital. En el host de vIDM, el comando `openssl` ejecuta una versión anterior de OpenSSL, por lo que debe utilizar el comando `openssl1` en el host de vIDM. Este comando solo está disponible en el host de vIDM.

En un servidor que no sea el host de vIDM, puede utilizar el comando `openssl` que ejecuta la versión 1.x o una posterior de OpenSSL.

Procedimiento

- 1 Inicie sesión en la consola del host de vIDM o utilice SSH en el host de vIDM como el usuario **sshuser**, o bien inicie sesión en cualquier servidor que pueda hacer ping al host de vIDM.
- 2 Ejecute uno de los siguientes comandos para obtener la huella digital del host de vIDM.
 - Si inició sesión en el host de vIDM, ejecute el comando `openssl1` para obtener la huella digital:

```
openssl1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl  
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

Si se produce un error al ejecutar el comando, es posible que deba ejecutar `openssl1` con el comando `sudo`, es decir, `sudo openssl1`

- Si ha iniciado sesión en un servidor que pueda hacer ping al host vIDM, ejecute el comando `openssl` para obtener la huella digital:

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl  
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

Configurar la integración de VMware Identity Manager

NSX-T Data Center se puede integrar con VMware Identity Manager (vIDM), que proporciona servicios de administración de identidades. La implementación de vIDM puede ser un host vIDM independiente o un clúster de vIDM.

El host vIDM o todos los componentes del clúster de vIDM deben tener un certificado firmado por una entidad de certificación (CA). De lo contrario, es posible que no se pueda iniciar sesión en vIDM desde NSX Manager en algunos exploradores, como Microsoft Edge o Internet Explorer 11. Para obtener información sobre cómo instalar un certificado firmado por una entidad de certificación en vIDM, consulte la documentación de VMware Identity Manager en <https://docs.vmware.com/es/VMware-Identity-Manager/index.html>.

Al registrar NSX Manager con vIDM, se especifica un URI de redireccionamiento que apunta a NSX Manager. Puede proporcionar el nombre de dominio completo (Fully Qualified Domain Name, FQDN) o la dirección IP. Es importante que recuerde si utiliza el FQDN o la dirección IP. Cuando intente iniciar sesión en NSX Manager a través de vIDM, debe especificar el nombre de host en la dirección URL del mismo modo: es decir, si se utiliza el FQDN al registrar la instancia de Manager con vIDM, debe utilizar el FQDN en la URL, y si utiliza la dirección IP al registrar la instancia de Manager con vIDM, debe utilizar la dirección IP en la dirección URL. De lo contrario, se producirá un error en el inicio de sesión.

Si se necesita acceso a la API de NSX-T, una de las siguientes configuraciones debe ser verdadera:

- vIDM tiene un certificado conocido firmado por una CA.
- vIDM tiene el certificado de CA del conector de confianza en el lado del servicio vIDM.
- vIDM utiliza el modo de conector de salida.

Nota Las instancias de NSX Manager y vIDM deben estar en la misma zona horaria. Se recomienda usar UTC.

Debe configurar los servidores DNS para que tengan registros PTR si no utiliza una IP virtual o un equilibrador de carga externo (esto significa que la instancia de Manager está configurada con la IP física o el FQDN del nodo).

Si configura vIDM para que se integre con un equilibrador de carga externo, debe habilitar la persistencia de sesión en el equilibrador de carga para evitar problemas como páginas que no se cargan o un usuario que cierra la sesión de forma inesperada.

Si la implementación de vIDM es un clúster de vIDM, el equilibrador de carga de vIDM debe estar configurado para la terminación y reencriptación de SSL.

Si vIDM está habilitado, puede seguir iniciando sesión en NSX Manager con una cuenta de usuario local a través de la URL `https://<nsx-manager-ip-address>/login.jsp?local=true`.

Si utiliza UserPrincipalName (UPN) para iniciar sesión en vIDM, es posible que no pueda autenticarse en NSX-T. Para evitar este problema, utilice otro tipo de credenciales, por ejemplo, SAMAccountName.

Si utiliza NSX Cloud, puede iniciar sesión en CSM de forma independiente mediante la URL `https://<csm-ip-address>/login.jsp?local=true`.

Requisitos previos

- Compruebe que dispone de la huella digital del certificado del host de vIDM o del equilibrador de carga de vIDM, en función del tipo de implementación de vIDM (un host de vIDM independiente o un clúster de vIDM). El comando para obtener la huella digital es el mismo en ambos casos. Consulte [Obtener la huella digital del certificado desde un host de vIDM](#).
- Compruebe que NSX Manager está registrado como un cliente OAuth en vIDM. Durante el proceso de registro, anote el ID y el secreto del cliente. Para obtener más información, consulte la documentación de VMware Identity Manager en <https://docs.vmware.com/es/VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html>. Al crear el cliente, solo es necesario realizar las siguientes acciones:
 - En **Tipo de acceso**, establezca el valor **Token de cliente de servicio**.
 - Especifique un identificador de cliente.
 - Expanda el campo **Avanzado** y haga clic en **Generar secreto compartido**.
 - Haga clic en **Agregar**.

Nota de NSX Cloud Si utiliza NSX Cloud, verifique también que CSM esté registrado como un cliente OAuth en vIDM.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Usuarios**.
- 3 Haga clic en la pestaña **Configuración**.
- 4 Haga clic en **Editar**.
- 5 Para habilitar la integración del equilibrador de carga externo, haga clic en el botón de alternancia **Integración del equilibrador de carga externo**.

Nota Si tiene la IP virtual (VIP) configurada (compruebe **Sistema > Dispositivos > IP virtual**), no podrá utilizar la **Integración de equilibrador de carga externo**, aunque la habilite. Esto se debe a que puede tener la IP virtual o el equilibrador de carga externo mientras configura vIDM, pero no ambos. Deshabilite la IP virtual si desea utilizar el equilibrador de carga externo. Puede consultar más información en la sección [Configurar una dirección IP virtual para un clúster](#) de la *Guía de instalación de NSX-T Data Center*.

- 6 Para habilitar la integración de VMware Identity Manager, haga clic en el botón de alternancia **Integración con VMware Identity Manager**.

7 Proporcione la siguiente información.

Parámetro	Descripción
Dispositivo de VMware Identity Manager	El nombre de dominio completo (FQDN) del host de vIDM o del equilibrador de carga de vIDM, en función del tipo de implementación de vIDM (un host de vIDM independiente o un clúster de vIDM).
Identificador de cliente OAuth	El identificador que se crea al registrar NSX Manager en vIDM.
Secreto de cliente OAuth	El secreto que se crea al registrar NSX Manager en vIDM.
Huella digital de SSL	La huella digital del certificado del host de vIDM.
Dispositivo de NSX	La dirección IP o el nombre de dominio completo (FQDN) de NSX Manager. Si utiliza un clúster de NSX Manager, use el FQDN del equilibrador de carga, o bien la dirección IP o el FQDN de la dirección VIP del clúster. Si especifica un FQDN, debe acceder a NSX Manager desde un explorador utilizando el FQDN del administrador en la URL. Si especifica una dirección IP, debe utilizar la dirección IP en la URL. Opcionalmente, el administrador de vIDM puede configurar el cliente de NSX Manager para que pueda conectarse usando el FQDN o la dirección IP.

8 Haga clic en **Guardar**.

9 Si utiliza NSX Cloud, repita los pasos del 1 al 8 en el dispositivo de CSM. Para ello, inicie sesión en CSM en lugar de en NSX Manager.

Validar la funcionalidad de VMware Identity Manager

Después de configurar VMware Identity Manager, valide la funcionalidad. A menos que VMware Identity Manager se haya configurado y validado correctamente, algunos usuarios pueden recibir mensajes no autorizados (código de error 98) al intentar iniciar sesión.

A menos que VMware Identity Manager se haya configurado y validado correctamente, algunos usuarios pueden recibir mensajes no autorizados (código de error 98) al intentar iniciar sesión.

Procedimiento

1 Cree una codificación base64 del nombre de usuario y la contraseña.

Ejecute el siguiente comando para obtener la codificación y eliminar el carácter final '\n'. Por ejemplo:

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

2 Compruebe que cada usuario puede llamar a la API para cada nodo.

Use un comando curl de autorización remota: `curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy`. Por ejemplo:

```
curl -k -H 'Authorization: Remote c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

Esto devuelve la configuración de directiva de autorización, por ejemplo:

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

Si el comando no devuelve un error, significa que VMware Identity Manager funciona correctamente. No se requiere ningún paso adicional. Si el comando curl devuelve un error, es posible que el usuario esté bloqueado.

Nota Las directivas de bloqueo de cuentas se establecen y se aplican por nodo. Si un nodo del clúster bloqueó a un usuario, es posible que no haya otros nodos.

3 Para restablecer un bloqueo de usuario en un nodo:

- a Recupere la directiva de autorización mediante el usuario admin local NSX Manager:

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b Guarde la salida en un archivo JSON en el directorio de trabajo actual.
- c Modifique el archivo para cambiar la configuración del período de bloqueo.

Por ejemplo, muchos de los ajustes predeterminados aplican períodos de bloqueo y restablecimiento de 900 segundos. Cambie estos valores para habilitar el restablecimiento inmediato, por ejemplo:

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d Aplique el cambio al nodo afectado.

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e (opcional) Devuelva los archivos de configuración de directiva de autorización a su configuración anterior.

Esto debería resolver el problema de bloqueo. Si todavía puede realizar llamadas API de autenticación remota, pero aún no puede iniciar sesión a través del navegador, es posible que el navegador tenga una caché o una cookie no válidas almacenadas. Borre la memoria caché y las cookies, y vuelva a intentarlo.

Sincronización de hora entre NSX Manager, vIDM y componentes relacionados

Para que la autenticación funcione correctamente, la hora de NSX Manager, vIDM y otros proveedores de servicios (p. ej., Active Directory) debe estar sincronizada. En esta sección se describe cómo sincronizar la hora de estos componentes.

VMware Infrastructure

Siga las instrucciones en los siguientes artículos de la base de conocimientos para sincronizar los hosts ESXi.

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

Infraestructura de terceros

Siga la documentación del proveedor sobre cómo sincronizar las máquinas virtuales y los hosts.

Configurar NTP en el servidor vIDM (no recomendado)

Si no puede sincronizar la hora en los hosts, puede deshabilitar la sincronización con el host y configurar NTP en el servidor vIDM. No se recomienda este método, ya que requiere la apertura del puerto UDP 123 en el servidor vIDM.

- Compruebe el reloj en el servidor vIDM y asegúrese de que la hora sea correcta.

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- Edite `/etc/ntp.conf` y agregue las siguientes entradas si no existen.

```
server time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- Abra el puerto UDP 123.

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

Ejecute el siguiente comando para comprobar que el puerto está abierto.

```
# iptables -L -n
```

- Inicie el servicio NTP.

```
/etc/init.d/ntp start
```

- Configure NTP de manera que se ejecute automáticamente después de un reinicio.

```
# chkconfig --add ntp
# chkconfig ntp on
```

- Compruebe que se puede acceder al servidor NTP.

```
# ntpq -p
```

La columna `reach` no debe mostrar 0. La columna `st` debe mostrar un número distinto de 16.

Control de acceso basado en funciones

Con el control de acceso basado en funciones (role-based access control, RBAC) puede establecer que solo accedan al sistema los usuarios autorizados. Las funciones se asignan a los usuarios y cada función tiene permisos específicos.

Existen cuatro tipos de permisos:

- Acceso completo
- Ejecución
- Lectura
- Ninguno

Acceso completo proporciona al usuario todos los permisos. El permiso de ejecución incluye el permiso de lectura.

NSX-T Data Center tiene las siguientes funciones integradas. No puede agregar funciones nuevas.

- Administrador empresarial
- Auditor
- Ingeniero de redes
- Operaciones de redes
- Ingeniero de seguridad
- Operaciones de seguridad

- Administrador del equilibrador de carga
- Auditor del equilibrador de carga
- Administrador de VPN
- Administrador de Guest Introspection
- Administrador de introspección de red

Tras asignar una función a un usuario de Active Directory (AD), si se cambia el nombre de usuario en el servidor de AD, debe volver a asignar la función con el nombre de usuario nuevo.

Funciones y permisos

[Tabla 21-5. Funciones y permisos](#) y [Tabla 21-6. Funciones y permisos para opciones avanzadas de redes y seguridad](#) muestra los permisos que cada función tiene para diferentes operaciones. Se utilizan las siguientes abreviaturas:

- AE: administrador empresarial
- A: auditor
- IR: ingeniero de redes
- OR: operaciones de redes
- IS: ingeniero de seguridad
- OS: operaciones de seguridad
- Adm. EC: administrador del equilibrador de carga
- Aud. EC: auditor del equilibrador de carga
- Adm. VPN: administrador de VPN
- Adm. GI: administrador de Guest Introspection
- Adm. IR: administrador de introspección de red
- AC: acceso completo
- E: ejecutar
- L: lectura

Tabla 21-5. Funciones y permisos

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Redes > Puertas de enlace de nivel 0	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Interfaz de red	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Enrutamientos estáticos de red	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Servicios de configuración regional	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Configuración de ARP estática	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Segmentos	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Segmentos > Perfiles de segmentos	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Redes > Grupos de direcciones IP	AC	L	AC	AC	L	L	AC	L	L	L	Ninguna	Ninguna	Ninguno
Redes > Directivas de reenvío	AC	L	AC	L	AC	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Redes > DNS	AC	L	AC	AC	L	L	AC	L	L	L	Ninguna	Ninguna	Ninguno
Redes > Equilibrio de carga	AC	L	Ninguna	Ninguno	L	Ninguno	AC	L	AC	L	Ninguna	Ninguna	Ninguno
Redes > NAT	AC	L	AC	L	AC	L	AC	L	L	L	Ninguna	Ninguna	Ninguno
Redes > VPN	AC	L	AC	L	AC	L	AC	L	Ninguna	Ninguno	AC	Ninguna	Ninguno
Redes > Perfiles IPv6													
Seguridad > Firewall distribuido	AC	L	L	L	AC	L	AC	L	L	L	L	L	L
Seguridad > Firewall de puerta de enlace	AC	L	L	L	AC	L	AC	L	Ninguna	Ninguno	Ninguna	Ninguno	AC
Seguridad > Introspección de red	AC	L	L	L	L	L	AC	L	Ninguna	Ninguno	Ninguna	Ninguno	AC
Seguridad > Reglas de protección de endpoints	AC	L	L	L	L	L	AC	L	Ninguna	Ninguno	Ninguno	AC	Ninguno
Inventario > Perfiles de contexto	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Inventario > Máquinas virtuales	L	L	L	L	L	L	L	L	L	L	L	L	L
Planificar y solucionar problemas > Reflejo del puerto	AC	L	AC	L	L	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Planificar y solucionar problemas > Enlaces de reflejo del puerto	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Planificar y solucionar problemas > Enlaces del perfil de supervisión	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Planificar y solucionar problemas > Perfiles de IPFIX para los firewalls	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Planificar y solucionar problemas > Perfiles de IPFIX para el conmutador	AC	L	AC	L	L	L	AC	L	L	L	L	L	L
Sistema > Tejido > Nodos > Hosts	AC	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Nodos > Nodos	AC	L	AC	L	AC	L	L	L	L	L	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Nodos > Edge	AC	L	AC	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Nodos > Clústeres de Edge	AC	L	AC	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Nodos > Puentes	AC	L	AC	L	L	L	Ninguna	Ninguno	L	L	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Nodos > Nodos de transporte	AC	L	L	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguno

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Sistema > Tejido > Nodos > Túneles	L	L	L	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Perfiles > Perfiles de vínculo superior	AC	L	L	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Perfiles > Perfiles de clústeres de Edge	AC	L	AC	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Perfiles > Configuración	AC	L	Ninguna	Ninguna	Ninguna	Ninguno	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Zonas de transporte > Zonas de transporte	AC	L	L	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguno

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Sistema > Tejido > Zonas de transporte > Perfiles de zonas de transporte	AC	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Tejido > Administradores de equipos	AC	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguno	L	L
Sistema > Certificados	AC	L	Ninguna	Ninguno	AC	L	Ninguna	Ninguno	AC	L	AC	Ninguna	Ninguno
Sistema > Implementaciones de servicio > Instancias de servicio	AC	L	L	L	AC	L	AC	L	Ninguna	Ninguna	Ninguno	AC	AC
Sistema > Utilidades > Paquete de soporte técnico	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Sistema > Utilidades > Copia de seguridad	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Utilidades > Restaurar	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Utilidades > Actualizar	AC	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Usuarios > Asignaciones de funciones	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Active Directory	AC	L	AC	L	AC	AC	L	L	L	L	L	L	L
Sistema > Usuarios > Configuración	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Sistema > Licencias	AC	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno

Tabla 21-5. Funciones y permisos (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Sistema > Administración del sistema	AC	L	L	L	L	L	L	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Configuración del panel personalizada	AC	L	L	L	L	L	AC	L	L	L	L	L	L
Sistema > Administración del ciclo de vida > Migrar	AC	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno

Tabla 21-6. Funciones y permisos para opciones avanzadas de redes y seguridad

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Herramientas > Conexión de puerto	E	L	E	E	E	E	E	L	E	E	Ninguna	Ninguna	Ninguno
Herramientas > Traceflow	E	L	E	E	E	E	E	L	E	E	Ninguna	Ninguna	Ninguno
Herramientas > Creación de reflejo de puerto	AC	L	AC	L	L	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Herramientas > IPFIX	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L

Tabla 21-6. Funciones y permisos para opciones avanzadas de redes y seguridad (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Firewall > Firewall distribuido > General	AC	L	L	L	AC	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguno	L
Firewall > Firewall distribuido > Configuración	AC	L	L	L	AC	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
Firewall > Firewall de Edge	AC	L	L	L	AC	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguno	AC
Enrutamiento > Enrutadores	AC	L	AC	AC	L	L	AC	L	L	L	L	Ninguno	L
Enrutamiento > NAT	AC	L	AC	L	AC	L	AC	L	L	L	Ninguna	Ninguna	Ninguno
DHCP > Perfiles de servidor	AC	L	AC	L	Ninguna	Ninguno	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
DHCP > Servidores	AC	L	AC	L	Ninguna	Ninguno	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
DHCP > Perfiles de retransmisión	AC	L	AC	L	Ninguna	Ninguno	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
DHCP > Servicios de retransmisión	AC	L	AC	L	Ninguna	Ninguno	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno

Tabla 21-6. Funciones y permisos para opciones avanzadas de redes y seguridad (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
DHCP > Servidores proxy de metadatos	AC	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno
IPAM	AC	L	AC	AC	L	L	Ninguna	Ninguno	L	L	Ninguna	Ninguna	Ninguno
Conmutación > Conmutadores	AC	L	AC	AC	L	L	AC	L	L	L	L	Ninguno	L
Conmutación > Puertos	AC	L	AC	AC	L	L	AC	L	L	L	L	Ninguno	L
Conmutación > Perfiles de conmutación	AC	L	AC	AC	L	L	AC	L	L	L	Ninguna	Ninguna	Ninguno
Redes > Equilibradores de carga	AC	L	Ninguna	Ninguno	L	Ninguno	AC	L	AC	L	Ninguna	Ninguna	Ninguno
Equilibrio de carga > Perfiles > Perfiles de SSL	AC	L	Ninguna	Ninguno	AC	L	AC	L	AC	L	Ninguna	Ninguna	Ninguno
Inventario > Grupos	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventario > Conjuntos de direcciones IP	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L

Tabla 21-6. Funciones y permisos para opciones avanzadas de redes y seguridad (continuación)

Operación	AE	A	IR	OR	IS	OS	Adm. CS	Aud. CS	Adm. EC	Aud. EC	Adm. VPN	Adm. GI	Adm. IR
Inventario > Grupos de direcciones IP	AC	L	AC	L	Ninguna	Ninguna	Ninguna	Ninguno	L	L	L	L	L
Inventario > Conjuntos de direcciones MAC	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventario > Servicios	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventario > Máquinas virtuales	L	L	L	L	L	L	L	L	L	L	L	L	L
Inventario > Máquinas virtuales > Configurar etiquetas	AC	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguno

Agregar una asignación de funciones o la identidad principal

Puede asignar funciones a usuarios o grupos de usuarios si VMware Identity Manager está integrado en NSX-T Data Center. También puede asignar funciones a las identidades principales.

Una entidad principal es un componente de NSX-T Data Center o una aplicación de terceros, como un producto de OpenStack. Con una identidad de entidades de seguridad, una entidad de seguridad puede utilizar el nombre de dicha identidad para crear un objeto y garantizar que solo una entidad con el mismo nombre de identidad pueda modificar o eliminar el objeto. La identidad de entidades de seguridad tiene las siguientes propiedades:

- Nombre

- Identificador de nodo: puede ser cualquier valor alfanumérico asignado a una identidad principal
- Certificado
- Función RBAC que indica los derechos de acceso de esta entidad de seguridad

Los usuarios (identidad local, remota o de entidades de seguridad) con la función de administrador empresarial pueden modificar o eliminar objetos que sean propiedad de las identidades de entidades de seguridad. Los usuarios (identidad local, remota o de entidades de seguridad) sin la función de administrador empresarial no pueden modificar ni eliminar objetos protegidos que sean propiedad de las identidades de entidades de seguridad, pero pueden modificar y eliminar objetos no protegidos.

Si el certificado de un usuario de identidad de entidad de seguridad caduca, debe importar un certificado nuevo y hacer una llamada API para actualizar el certificado de ese usuario (consulte el procedimiento a continuación). Para obtener más información sobre la API de NSX-T Data Center, acceda al vínculo del recurso de API disponible en <https://docs.vmware.com/es/VMware-NSX-T-Data-Center>.

El certificado de un usuario de identidad principal debe cumplir con los siguientes requisitos:

- Basado en SHA256.
- Algoritmo de mensaje RSA/DSA con un tamaño de clave mínimo de 2048 bits.
- No puede ser un certificado raíz.

Puede eliminar una identidad principal mediante la API. Sin embargo, la eliminación de una identidad principal no elimina automáticamente el certificado correspondiente. Debe eliminar el certificado manualmente.

Pasos para eliminar una identidad principal y su certificado:

- 1 Consulte los detalles de la identidad principal que desea eliminar y anote el valor de `certificate_id` en la respuesta.

```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 2 Elimine la identidad principal.

```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 3 Elimine el certificado utilizando el valor de `certificate_id` obtenido en el paso 1.

```
DELETE /api/v1/trust-management/certificates/<certificate_id>
```

Requisitos previos

- Si desea asignar funciones a los usuarios, compruebe que un host de vIDM esté asociado con NSX-T. Para obtener más información, consulte [Configurar la integración de VMware Identity Manager](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Usuarios**.
- 3 Para asignar funciones a los usuarios, seleccione **Agregar > Asignación de funciones**.
 - a Seleccione un usuario o un grupo de usuarios.
 - b Seleccione una función.
 - c Haga clic en **Guardar**.
- 4 Para agregar una identidad principal, seleccione **Agregar > Identidad principal con función**.
 - a Introduzca un nombre para la identidad principal.
 - b Seleccione una función.
 - c Escriba un identificador de nodo.
 - d Introduzca un certificado en formato PEM.
 - e Haga clic en **Guardar**.
- 5 (opcional) Si utiliza NSX Cloud, inicie sesión en el dispositivo de CSM, en lugar de en NSX Manager, y repita los pasos del 1 al 4.
- 6 Si el certificado de la identidad de entidad de seguridad caduca, realice los siguientes pasos:
 - a Importe un certificado nuevo y anote el identificador del certificado. Consulte [Importar un certificado](#).
 - b Haga la siguiente llamada API para obtener el identificador de la identidad de entidad de seguridad.


```
GET https://<nsx-mgr>/api/v1/trust-management/principal-identities
```
 - c Haga la siguiente llamada API para actualizar el certificado de la identidad de entidad de seguridad. Debe proporcionar el identificador del certificado importado y el identificador del usuario de identidad de entidad de seguridad.

Por ejemplo,

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?
action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

Restaurar y hacer copias de seguridad de NSX Manager

Si el clúster de NSX Manager deja de funcionar, o si se desea restaurar el entorno a un estado anterior, puede realizar la restauración desde una copia de seguridad. Mientras NSX Manager no funciona, el plano de datos no se ve afectado, pero no es posible hacer cambios en la configuración.

Existen dos tipos de copias de seguridad:

Copia de seguridad de los clústeres

Esta copia de seguridad incluye el estado deseado de la red virtual.

Copia de seguridad del nodo

Se trata de una copia de seguridad de los nodos de NSX Manager.

Existen dos métodos de copia de seguridad:

Manual

Se ejecuta manualmente la copia de seguridad en cualquier momento.

Automatizado

Las copias de seguridad automáticas se ejecutan según la programación que estableció.

Las copias de seguridad automatizadas se recomiendan especialmente para asegurarse de disponer de copias de seguridad actualizadas.

Puede volver a restaurar una configuración de NSX-T Data Center al estado capturado en cualquiera de las copias de seguridad. Al restaurar una copia de seguridad, debe restaurar a nuevos dispositivos de NSX Manager que ejecuten la misma versión de NSX Manager que el dispositivo del que se realizó la copia de seguridad.

Configurar copias de seguridad

Antes de que se puedan realizar las copias de seguridad, debe configurar un servidor de archivos de copia de seguridad. Una vez configurado este servidor, puede iniciar una copia de seguridad en cualquier momento o configurar una programación de copias de seguridad automáticas.

Requisitos previos

Verifique que tiene la huella digital SSH del servidor de archivos de las copias de seguridad. Solo una clave ECDSA con hash SHA256 (256 bits) se acepta como huella digital. Consulte [Buscar la huella digital SSH de un servidor remoto](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Copia de seguridad y restauración**.

- 3 Haga clic en **Editar** en la parte superior derecha de la página para configurar las copias de seguridad.
- 4 Introduzca la dirección IP o el nombre del host del servidor de los archivos de copia de seguridad.
- 5 Si es necesario, cambie el puerto predeterminado.
- 6 El campo de protocolo ya aparece completado. No cambie el valor.

SFTP es el único protocolo admitido.

- 7 Introduzca la contraseña y el nombre de usuario necesarios para iniciar sesión en el servidor de los archivos de copia de seguridad.

La primera vez que configure un servidor de archivos, debe proporcionar una contraseña. En adelante, si vuelve a configurar el servidor de archivos, y la dirección IP del servidor (o nombre de host), el puerto y el nombre de usuario son los mismos, no es necesario introducir otra vez la contraseña.

- 8 En el campo **Directorio de destino**, escriba la ruta de acceso absoluta donde se almacenarán las copias de seguridad.

El directorio ya debe existir y no puede ser /. Si tiene varias implementaciones de NSX-T Data Center, debe utilizar un directorio diferente para cada una. Si el servidor de archivos de copia de seguridad es un equipo Windows, siga utilizando la barra diagonal para especificar el directorio de destino. Por ejemplo, si el directorio de copia de seguridad del equipo Windows es `c:\SFTP_Root\backup`, especifique `/SFTP_Root/backup` como directorio de destino.

Nota El proceso de copia de seguridad generará un nombre para el archivo de copia de seguridad que puede ser bastante largo. En un servidor Windows, la longitud del nombre de ruta completo del archivo de copia de seguridad puede superar el límite establecido por Windows y provocar errores en las copias de seguridad. Para evitar este problema, consulte el artículo de la base de conocimientos <https://kb.vmware.com/s/article/76528>.

- 9 Para cifrar las copias de seguridad, haga clic en la opción **Cambiar frase de contraseña de cifrado** e introduzca la frase de contraseña de cifrado.

Necesitará esta frase de contraseña para restaurar una copia de seguridad. Si olvida la frase de contraseña, no podrá restaurar ninguna copia de seguridad.

- 10 Introduzca la huella digital SSH del servidor en el que se almacenan las copias de seguridad.

Puede dejar esta opción en blanco y aceptar o rechazar la huella digital proporcionada por el servidor.

- 11 Haga clic en la pestaña **Programar**.

- 12 Para habilitar las copias de seguridad automáticas, haga clic en la opción **Copia de seguridad automática**.

- 13 Haga clic en **Semanal** y establezca los días y la hora en que se realizará la copia de seguridad, o bien haga clic en **Intervalo** y establezca el intervalo entre una copia de seguridad y otra.

- 14 Al habilitar la opción **Detectar el cambio de configuración de NSX**, se activará una copia de seguridad de configuración completa no programada cuando detecte cualquier cambio relacionado con el tiempo de ejecución o que no sea de configuración, o bien cualquier cambio en la configuración de usuario.

Puede establecer el intervalo entre las copias de seguridad que se activan por los cambios de configuración. El valor predeterminado es 5 minutos.

Nota Esta opción puede generar una gran cantidad de copias de seguridad. Utilícela con precaución.

- 15 Haga clic en **Guardar**.

Resultados

Después de configurar un servidor de archivos de copia de seguridad, puede hacer clic en **Realizar copia de seguridad ahora** para iniciar una copia de seguridad en ese momento.

Eliminar las copias de seguridad antiguas

Las copias de seguridad pueden acumularse en el servidor de archivos de copia de seguridad y consumir una gran cantidad de almacenamiento. Puede ejecutar un script que se incluye en NSX-T Data Center para eliminar automáticamente las copias de seguridad antiguas.

Puede encontrar el script de Python `nsx_backup_cleaner.py` en el directorio `/var/vmware/nsx/file-store` en NSX Manager. Debe iniciar sesión como usuario raíz para acceder a este archivo. Normalmente, se programa una tarea en el servidor de archivos de copia de seguridad que ejecuta este script periódicamente para limpiar las copias de seguridad antiguas. En la siguiente información de uso, se describe cómo ejecutar el script:

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]

Required parameters:
  -d/--dir: Backup root directory
  -k/--retention-period: Number of days need to retain a backup file

Optional parameters:
  -l/--min-count: Minimum number of backup files to be kept, default value is 100
  -h/--help: Display help message
```

La antigüedad de una copia de seguridad se calcula como la diferencia entre la marca de tiempo de la copia de seguridad y la hora en que se ejecuta el script. Si este valor es mayor que el período de retención, se elimina la copia de seguridad si hay más copias en el disco que el número mínimo de copias de seguridad.

Para obtener más información sobre cómo configurar la ejecución periódica del script en un servidor Linux o Windows, consulte los comentarios al comienzo del script.

Lista de las copias de seguridad disponibles

El servidor de archivos de copia de seguridad almacena las copias de seguridad de todas las instancias de NSX Manager. Para obtener la lista de las copias de seguridad para que pueda encontrar la que desea restaurar, debe ejecutar el script `get_backup_timestamps.sh`.

El script se encuentra en NSX Manager. El nombre completo de la ruta de acceso es `/var/vmware/nsx/file-store/get_backup_timestamps.sh`. Este script se puede ejecutar en cualquier equipo con Linux o dispositivo de NSX-T Data Center. Como práctica recomendada, debe copiar este script después de instalar NSX-T Data Center en un equipo que no sea una instancia de NSX Manager para poder ejecutar este script incluso si todas las instancias de NSX Manager dejan de estar accesibles. Si necesita restaurar una copia de seguridad pero no tiene acceso a este script, puede instalar una instancia nueva de NSX Manager y ejecutar el script en ella.

Para copiar el script en otro equipo o en el servidor de archivos de copia de seguridad, inicie sesión en NSX Manager como administrador y ejecute un comando de la CLI. Por ejemplo:

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

El script es interactivo y le solicitará la información que especificó al configurar el servidor de archivos de copia de seguridad. Puede especificar el número de copias de seguridad que se debe mostrar. Cada copia de seguridad se muestra con una marca de tiempo, la dirección IP o el FQDN del nodo de NSX Manager si el nodo de NSX Manager está configurado para publicar su FQDN y el identificador del nodo. Por ejemplo,

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

Restaurar una copia de seguridad

Al restaurar una copia de seguridad, se restablece el estado que tenía la red en el momento en que se creó la copia de seguridad. También se restablecen las configuraciones guardadas por

NSX Manager y se aplican todos los cambios (por ejemplo, los nodos agregados o eliminados) del tejido realizados desde que se creó la copia de seguridad.

Debe restaurar la copia de seguridad en un nuevo dispositivo de NSX Manager.

Si tenía un clúster de NSX Manager al crear la copia de seguridad, también debe restaurar un clúster de NSX Manager. El proceso de restauración primero restaura un nodo de NSX Manager y, a continuación, le permitirá agregar los demás nodos de NSX Manager.

Importante Si algún nodo del clúster de NSX Manager aún está disponible, debe apagarlo antes de iniciar la restauración.

Requisitos previos

- Verifique que tiene la credencial de inicio de sesión en el servidor de archivos de las copias de seguridad.
- Verifique que tiene la huella digital SSH del servidor de archivos de las copias de seguridad. Solo una clave ECDSA con hash SHA256 (256 bits) se acepta como huella digital. Consulte [Buscar la huella digital SSH de un servidor remoto](#).
- Verifique que tiene la frase de contraseña del archivo de copia de seguridad.
- Para identificar qué copia de seguridad desea restaurar, siga el procedimiento descrito en [Lista de las copias de seguridad disponibles](#). Tome nota de la IP o el FQDN del nodo de NSX Manager que realizó la copia de seguridad.
- Si configura los nodos de NSX Manager para publicar su FQDN, debe configurar las entradas de búsqueda directa e inversa para los nodos de NSX Manager en el servidor DNS.

Procedimiento

- 1 Apague todos los nodos en el clúster de NSX Manager que va a restaurar.
- 2 Instale un nuevo nodo de NSX Manager en el que restaurar la copia de seguridad.

- Si la lista de copia de seguridad que va a restaurar contiene una dirección IP, deberá implementar el nuevo nodo de NSX Manager con la misma dirección IP. No configure el nodo de NSX Manager para publicar su FQDN.

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- Si la lista de la copia de seguridad que va a restaurar contiene un FQDN, deberá configurar el nuevo nodo de NSX Manager con este FQDN (consulte más información en la sección "Publicar los FQDN de las instancias de NSX Manager" en el tema "Instalación de NSX Manager" de la *Guía de instalación de NSX-T Data Center*). Además, si el nuevo nodo de NSX Manager tiene una dirección IP diferente a la original, deberá actualizar las entradas de búsqueda directa e inversa del servidor DNS para el nodo de NSX Manager con la nueva dirección IP.

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

Una vez que el nuevo nodo de NSX Manager se esté ejecutando y esté en línea, podrá continuar con la restauración.

- 3 En el explorador, inicie sesión con privilegios de administrador en la nueva instancia de NSX Manager.
- 4 Seleccione **Sistema > Copia de seguridad y restauración**.
- 5 Haga clic en la pestaña **Restaurar**.
- 6 Para configurar el servidor de archivos de copia de seguridad, haga clic en **Editar**.
- 7 Escriba el nombre de host o la dirección IP.
- 8 Cambie el número de puerto, si fuera necesario.
El valor predeterminado es 22.
- 9 Para iniciar sesión en el servidor, introduzca el nombre de usuario y la contraseña.
- 10 En el cuadro de texto **Directorio de destino**, introduzca la ruta de acceso absoluta del directorio donde se almacenan las copias de seguridad.
- 11 Introduzca la frase de contraseña que se usó para cifrar los datos de la copia de seguridad.
- 12 Introduzca la huella digital SSH del servidor en el que se almacenan las copias de seguridad.
- 13 Haga clic en **Guardar**.
- 14 Seleccione una copia de seguridad.
- 15 Haga clic en **Restaurar**.

Se muestra el estado de la operación de restauración. Si eliminó o agregó nodos de tejido o de transporte desde que se realizó la copia de seguridad, se le solicitará que haga ciertas acciones como, por ejemplo, iniciar sesión en un nodo y ejecutar un script.

Si la copia de seguridad incluye información acerca de un clúster de NSX Manager, se le pedirá que agregue nodos de NSX Manager. Si decide no agregar nodos de NSX Manager, podrá continuar con la restauración de todos modos.

Una vez finalizada la operación de restauración, la pantalla **Restauración completa** mostrará el resultado de la restauración, la marca de tiempo del archivo de copia de seguridad y la hora de inicio y finalización de la operación de restauración.

Si se produce un error en la restauración, la pantalla mostrará el paso en el que se produjo, por ejemplo, `Current Step: Restoring Cluster (DB)` o `Current Step: Restoring Node`. Si se produce un error en la restauración del clúster o en la del nodo, el error puede ser transitorio. En ese caso, no es necesario hacer clic en **Reintentar**. Puede reiniciar el administrador y la restauración continuará.

Para determinar si se produjo un error en la restauración del clúster o de un nodo, también puede consultar los archivos de registro. Ejecute `get log-file syslog` para ver el archivo de registro del sistema y busque las cadenas `Error` en la restauración del clúster y `Error` en la restauración del nodo.

Para reiniciar Manager, ejecute el comando `restart service manager`.

Para volver a arrancar Manager, ejecute el comando `reboot`.

- 16 Si solo tiene un nodo implementado, una vez que el nodo de NSX Manager restaurado esté activo y en funcionamiento, puede implementar nodos adicionales para formar un clúster de NSX Manager.

Consulte la *Guía de instalación de NSX-T Data Center* para obtener instrucciones.

- 17 Después de implementar el nuevo clúster de NSX Manager, elimine las máquinas virtuales originales del clúster de NSX Manager que apagó en el paso 1.

También debe reemplazar los certificados en el segundo y tercer nodo del clúster.

Resultados

Si agregó un administrador de equipos después de la copia de seguridad e intenta volver a agregar el administrador de equipos después de la restauración, recibirá un mensaje de error indicando que se produjo un error en el registro. Puede hacer clic en el botón **Resolver** para resolver el error y agregar correctamente el administrador de equipos. Para obtener más información, consulte [Agregar un administrador de equipos](#), el paso 4. Si desea quitar la información de NSX-T Data Center que se almacena en una instancia de vCenter Server, siga los pasos que se describen en [Quitar una extensión NSX-T Data Center de vCenter Server](#).

Copia de seguridad y restauración durante la actualización

El plano de administración deja de responder durante el proceso de actualización y es necesario restaurar una copia de seguridad tomada mientras la actualización estaba en curso.

Problema

El coordinador de actualización se actualizó y el plano de administración deja de responder. Tiene una copia de seguridad que se creó mientras la actualización estaba en curso.

Solución

- 1 Implemente el nodo del plano de administración con la misma dirección IP desde la que se creó la copia de seguridad.
- 2 Cargue el paquete de actualización que utilizó al principio del proceso de actualización.
- 3 Actualice el coordinador de actualización.
- 4 Restaure la copia de seguridad tomada durante el proceso de actualización.
- 5 Cargue un nuevo paquete de actualización si es necesario.
- 6 Continúe con el proceso de actualización.

Quitar una extensión NSX-T Data Center de vCenter Server

Al agregar un administrador de equipos, NSX Manager agrega su identidad como una extensión en vCenter Server. Si quita el administrador de equipo, la extensión de vCenter Server se elimina automáticamente. Si la extensión no se elimina por algún motivo, puede quitarla manualmente mediante el siguiente procedimiento.

Requisitos previos

Habilite el acceso al explorador de objetos administrados (Managed Object Browser, MOB) de vCenter Server mediante los pasos indicados en esta página: <https://kb.vmware.com/s/article/2042554>.

Procedimiento

- 1 Inicie sesión en el MOB: `https://<nombre de host de vCenter Server o dirección IP>/mob`.
- 2 Haga clic en el vínculo **content**, que es el valor de la propiedad **content** en la tabla Propiedades.
- 3 Haga clic en el vínculo **ExtensionManager**, que es el valor de la propiedad **extensionManager** en la tabla Propiedades.
- 4 Haga clic en el vínculo **UnregisterExtension** en la tabla Métodos.
- 5 Introduzca `com.vmware.nsx.management.nsx` en el campo de texto **Valor**.
- 6 Haga clic en el vínculo **Invocar método** que se encuentra en la parte derecha de la página, debajo de la tabla Parámetros.

El resultado del método indica `void`, pero la extensión se quitará.

- 7 Para asegurarse de que se quite la extensión, haga clic en el método **FindExtension** incluido en la página anterior e invóquelo introduciendo el mismo valor para la extensión.

El resultado debería ser `void`.

Administrar el clúster de NSX Manager

Si deja de funcionar, puede reiniciar NSX Manager. También puede cambiar la dirección IP de NSX Manager.

En un entorno de producción, se recomienda que el clúster de NSX Manager tenga tres miembros para proporcionar alta disponibilidad. Si elimina una instancia de NSX Manager e implementa una nueva, esta nueva instancia de NSX Manager puede tener la misma dirección IP o una diferente.

Nota El nodo principal de NSX Manager es el nodo que se crea primero antes de crear un clúster de administrador. Este nodo no se puede eliminar. Después de implementar dos nodos de NSX Manager más en la interfaz de usuario del nodo principal de NSX Manager para formar un clúster, solo los nodos del segundo y tercer administrador tendrán la opción (en el icono de la rueda dentada) de eliminarse. Para obtener información sobre cómo eliminar y agregar un nodo de NSX Manager, consulte [Cambiar la dirección IP de NSX Manager](#).

Ver la configuración y el estado del clúster de NSX Manager

La configuración y el estado del clúster de NSX Manager se puede ver en la interfaz de usuario de NSX Manager. Puede obtener información adicional mediante la CLI.

Procedimiento

- 1 En un explorador, inicie sesión con privilegios de usuario admin en NSX Manager en `https://nsx-manager-ip-address`.

- 2 Seleccione **Sistema > Información general**.

Se muestra el estado del clúster de NSX Manager.

- 3 Si desea ver información adicional sobre la configuración, ejecute el siguiente comando de la CLI:

```
manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Cluster Configuration Version: 3
Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9
Node Status: JOINED
  ENTITY                                UUID                                IP
ADDRESS      PORT      FQDN
  HTTPS                                5c8d01f1-f3ee-4f94-b517-a093d8fbfad3
10.160.71.225  443      ychin-nsxmanager-ob-12065118-1-F5
  CONTROLLER                                06fd0574-69c0-432e-a8af-53d140dbef8f
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5
  CLUSTER_BOOT_MANAGER                                da8d535e-7a0c-4dd8-8919-d88bdde006b8
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5
  DATASTORE                                3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4
10.160.71.225  9000      ychin-nsxmanager-ob-12065118-1-F5
  MANAGER                                eb5e8922-23bd-4c3a-ae22-d13d9195a6bc
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5
  POLICY                                f9da1039-08ad-4a20-bacc-5b91c5d67730
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5

Node UUID: 8ebb0642-201e-6a5f-dd47-a1e38542e672
Node Status: JOINED
  ENTITY                                UUID                                IP
```

ADDRESS	PORT	FQDN	
HTTPS			3757f155-8a5d-4b53-828f-d67041d5a210
10.160.93.240	443	ychin-nsxmanager-ob-12065118-2-F5	
CONTROLLER			7b1c9952-8738-4900-b68b-ca862aa4f6a9
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	
CLUSTER_BOOT_MANAGER			b5e12db1-5e0d-4e33-a571-6ba258dceb2e
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	
DATASTORE			bee1f629-4e23-4ab8-8083-9e0f0bb83178
10.160.93.240	9000	ychin-nsxmanager-ob-12065118-2-F5	
MANAGER			45ccd6e3-1497-4334-944c-e6bbcd5c723e
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	
POLICY			d5ba5803-b059-4fbc-897c-3aace8cf1219
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	
Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea			
Node Status: JOINED			
ENTITY			UUID
			IP
ADDRESS	PORT	FQDN	
HTTPS			bce3cc4c-7d60-45e2-aa7b-cdc75e445a14
10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5	
CONTROLLER			ced46f5c-9e52-4b31-a1cb-b3dead991c71
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	
CLUSTER_BOOT_MANAGER			88b70d31-3428-4ccc-ab57-55859f45030c
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	
DATASTORE			fb4aec3c-cae3-4386-b5b9-c0b99b7d9048
10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5	
MANAGER			82b07440-3ff6-4f67-a1c9-e9327d1686ad
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	
POLICY			61f21a78-a56c-4af1-867b-3f24132d53c7
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	

4 Si desea ver información adicional sobre el estado, ejecute el siguiente comando de la CLI:

```

manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
Group Status: STABLE

Members:
  UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP
8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP

Group Type: CLUSTER_BOOT_MANAGER
Group Status: STABLE

Members:
  UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5

```

```

10.160.71.225      UP
      8ebb0642-201e-6a5f-dd47-a1e38542e672      ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240      UP
      2e7e0642-df4a-b2ec-b9e8-633d1469f1ea      ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33       UP

Group Type: CONTROLLER
Group Status: STABLE

Members:
      UUID      FQDN
IP      STATUS
      7b1c9952-8738-4900-b68b-ca862aa4f6a9      ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240      UP
      ced46f5c-9e52-4b31-a1cb-b3dead991c71      ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33       UP
      06fd0574-69c0-432e-a8af-53d140dbef8f      ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225      UP

Group Type: MANAGER
Group Status: STABLE

Members:
      UUID      FQDN
IP      STATUS
      43cd0642-275c-af1d-fe46-1f5200f9e5f9      ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225      UP
      8ebb0642-201e-6a5f-dd47-a1e38542e672      ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240      UP
      2e7e0642-df4a-b2ec-b9e8-633d1469f1ea      ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33       UP

Group Type: POLICY
Group Status: STABLE

Members:
      UUID      FQDN
IP      STATUS
      43cd0642-275c-af1d-fe46-1f5200f9e5f9      ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225      UP
      8ebb0642-201e-6a5f-dd47-a1e38542e672      ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240      UP
      2e7e0642-df4a-b2ec-b9e8-633d1469f1ea      ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33       UP

Group Type: HTTPS
Group Status: STABLE

Members:
      UUID      FQDN
IP      STATUS
      43cd0642-275c-af1d-fe46-1f5200f9e5f9      ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225      UP

```

8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Apagar y encender el clúster de NSX Manager

Si necesita apagar el clúster de NSX Manager, siga el procedimiento que se indica a continuación.

Procedimiento

- 1 Para apagar un clúster de NSX Manager, desconecte un nodo de Manager a la vez. Puede iniciar sesión en la interfaz de línea de comandos (CLI) de un nodo de Manager como `admin` y ejecutar el comando `shutdown` o apagar la máquina virtual del nodo de Manager desde vCenter Server.

Asegúrese de que la máquina virtual esté apagada en vCenter Server antes de continuar con la siguiente.

- 2 Para encender un clúster de NSX Manager, encienda una máquina virtual de nodo de administrador a la vez en vCenter Server.

Asegúrese de que el nodo esté activo y en ejecución antes de continuar con el siguiente.

Reiniciar una instancia de NSX Manager

Puede reiniciar una instancia de NSX Manager con un comando de CLI para recuperarse de errores críticos.

Si necesita reiniciar varias instancias de NSX Manager, hágalo de a una por vez. Antes de reiniciar otra instancia, espere hasta que la instancia de NSX Manager reiniciada esté conectada.

Procedimiento

- 1 Inicie sesión en la CLI de NSX Manager.
- 2 Ejecute el siguiente comando.

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

Cambiar la dirección IP de NSX Manager

Puede cambiar la dirección IP de una instancia de NSX Manager en un clúster de NSX Manager. En esta sección se describen varios enfoques.

Por ejemplo, si tiene un clúster compuesto por el Administrador A, el Administrador B y el Administrador C, puede cambiar la dirección IP de uno o varios de ellos de las siguientes formas:

- Caso A:
 - El Administrador A tiene la dirección IP 172.16.1.11.

- El Administrador B tiene la dirección IP 172.16.1.12.
- El Administrador C tiene la dirección IP 172.16.1.13.
- Agregue el Administrador D con una nueva dirección IP, por ejemplo, 192.168.55.11.
- Elimine el Administrador A.
- Agregue el Administrador E con una nueva dirección IP, por ejemplo, 192.168.55.12.
- Elimine el Administrador B.
- Agregue el Administrador F con una nueva dirección IP, por ejemplo, 192.168.55.13.
- Elimine Administrador C.
- Caso B:
 - El Administrador A tiene la dirección IP 172.16.1.11.
 - El Administrador B tiene la dirección IP 172.16.1.12.
 - El Administrador C tiene la dirección IP 172.16.1.13.
 - Agregue el Administrador D con una nueva dirección IP, por ejemplo, 192.168.55.11.
 - Agregue el Administrador E con una nueva dirección IP, por ejemplo, 192.168.55.12.
 - Agregue el Administrador F con una nueva dirección IP, por ejemplo, 192.168.55.13.
 - Elimine los Administradores A, B y C.
- Caso C:
 - El Administrador A tiene la dirección IP 172.16.1.11.
 - El Administrador B tiene la dirección IP 172.16.1.12.
 - El Administrador C tiene la dirección IP 172.16.1.13.
 - Elimine el Administrador A.
 - Agregue el Administrador D con una nueva dirección IP, por ejemplo, 192.168.55.11.
 - Elimine el Administrador B.
 - Agregue el Administrador E con una nueva dirección IP, por ejemplo, 192.168.55.12.
 - Elimine Administrador C.
 - Agregue el Administrador F con una nueva dirección IP, por ejemplo, 192.168.55.13.

Los dos primeros casos requieren disco, CPU y RAM virtual adicional para las instancias adicionales de NSX Manager durante este cambio de dirección IP.

No se recomienda el caso C porque reduce temporalmente el número de instancias de NSX Manager, y la pérdida de uno de los dos administradores activos durante el cambio de dirección IP afectará a las operaciones de NSX-T. Este caso está indicado para una situación en la que no haya disco, CPU o memoria RAM virtual adicional y se requiere un cambio de dirección IP.

Nota Si utiliza la función VIP de clúster, debe utilizar la misma subred para las nuevas direcciones IP o deshabilitar la VIP del clúster durante los cambios de dirección IP, ya que la VIP del clúster requiere que todas las instancias de NSX Manager estén en la misma subred.

Requisitos previos

Familiarícese con el modo de implementar NSX Manager en un clúster. Para obtener más información, consulte la *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 Si la instancia de NSX Manager que desea quitar se implementó manualmente, siga estos pasos.
 - a Ejecute el siguiente comando de la CLI para desasociar NSX Manager del clúster.


```
detach node <node-id>
```
 - b Elimine la máquina virtual de NSX Manager.
- 2 Si la instancia de NSX Manager que desea eliminar se implementó automáticamente a través de la interfaz de usuario de NSX Manager, siga estos pasos.
 - a En un explorador, inicie sesión con privilegios de usuario admin en una instancia de NSX Manager desde `https://dirección-ip-nsx-manager`.
Esta instancia de NSX Manager no debe ser la que desea eliminar.
 - b En la pestaña **Sistemas**, haga clic en **Nodos de administración de NSX**.
Se muestra el estado del clúster de NSX Manager.
 - c Para la instancia de NSX Manager que desea eliminar, haga clic en el icono de engranaje y seleccione **Eliminar**.
- 3 Implemente una nueva instancia de NSX Manager.

Cambiar el tamaño de un nodo de NSX Manager

Puede cambiar el número de núcleos de CPU o la memoria de un nodo de NSX Manager en cualquier momento.

Tenga en cuenta que en condiciones de funcionamiento normales, los tres nodos de Manager deben tener el mismo número de núcleos de CPU y memoria. La falta de coincidencia de la CPU o la memoria entre diferentes instancias de NSX Manager en un clúster de administración de NSX solo puede producirse cuando se realiza la transición de un tamaño de NSX Manager a otro.

Si configuró la reserva de asignación de recursos para las máquinas virtuales de NSX Manager en vCenter Server, es posible que necesite ajustar la reserva. Para obtener más información, consulte la documentación de vSphere.

Requisitos previos

- Compruebe que el nuevo tamaño cumpla los requisitos del sistema para un nodo de Manager. Para obtener más información, consulte "Requisitos del sistema de NSX Manager" en la *Guía de instalación de NSX-T Data Center*.
- Familiarícese con el modo de implementar NSX Manager en un clúster. Para obtener más información, consulte la *Guía de instalación de NSX-T Data Center*.
- Para obtener más información sobre cómo eliminar un nodo de Manager de un clúster, consulte [Cambiar la dirección IP de NSX Manager](#).

Procedimiento

- 1 Implemente un nuevo nodo de administrador con el nuevo tamaño.
- 2 Agregue el tercer nodo de Manager al clúster.
- 3 Elimine un nodo de Manager anterior.
- 4 Repita los pasos del 1 al 3 para reemplazar los otros dos nodos anteriores de Manager.

Agregar y quitar un nodo de transporte de host ESXi en instancias de vCenter Server

Puede mover un nodo de transporte de host ESXi de una instancia de vCenter Server (VC) a otra y también de un clúster de NSX Manager a otro.

Escenario 1: VC1 conectado al clúster 1 de NSX Manager y VC2 conectado al clúster 2 de NSX Manager

Suponiendo que ESX1, un nodo de transporte de host ESXi, se encuentra en VC1, puede moverlo a VC2 siguiendo estos pasos:

- 1 Desinstale NSX de ESX1.
- 2 Mueva ESX1 a VC2.
- 3 Aplique un perfil de nodo de transporte a ESX1.

Escenario 2: VC1 y VC2 conectados a un clúster de NSX Manager

Suponiendo que ESX1, un nodo de transporte de host ESXi, se encuentra en VC1, puede moverlo a VC2 siguiendo estos pasos:

- 1 Desinstale NSX de ESX1.
- 2 Mueva ESX1 a VC2.
- 3 Aplique un perfil de nodo de transporte a ESX1.

Escenario 3: VC1 conectado al clúster 1 de NSX Manager

Suponiendo que ESX1, un nodo de transporte de host ESXi, se encuentra en VC1, puede moverlo al clúster 2 de NSX Manager como host independiente siguiendo estos pasos:

- 1 Desinstale NSX de ESX1.
- 2 Agregue ESX1 al clúster 2 de NSX Manager.

Reemplazar un nodo de transporte de NSX Edge en un clúster de NSX Edge

Puede reemplazar un nodo de transporte de NSX Edge en un clúster de NSX Edge mediante la API o la interfaz de usuario de NSX Manager.

Reemplazar un nodo de transporte de NSX Edge mediante la interfaz de usuario de NSX Manager

En el siguiente procedimiento se describe cómo reemplazar un nodo de transporte de NSX Edge en un clúster de NSX Edge mediante la interfaz de usuario de NSX Manager. Puede reemplazar el nodo de transporte de Edge independientemente de si se está ejecutando o no.

Si el nodo de Edge que se va a reemplazar no está en ejecución, el nuevo nodo de Edge puede tener la misma dirección IP de administración y la misma dirección IP de TEP. Si el nodo de Edge que se va a reemplazar se está ejecutando, el nuevo nodo de Edge debe tener una dirección IP de administración y una dirección IP de TEP diferentes.

Requisitos previos

Familiarícese con el procedimiento para instalar un nodo de NSX Edge, unir el nodo de Edge con el plano de administración y crear un nodo de transporte de NSX Edge. Para obtener más información, consulte la *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 Si desea que el nuevo nodo de transporte de Edge tenga las mismas configuraciones que el nodo de transporte de Edge que se reemplazará, realice la siguiente llamada API para buscar las configuraciones:

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Siga los procedimientos de la guía *Instalación de NSX-T Data Center* para instalar y configurar un nodo de transporte de Edge.

Si desea que este nodo de transporte de Edge tenga las mismas configuraciones que el nodo de transporte de Edge que se reemplazará, utilice las configuraciones obtenidas en el paso 1.

- 3 En NSX Manager, seleccione **Sistema > Tejido > Nodos > Clústeres de Edge**.
- 4 Seleccione un clúster de Edge haciendo clic en la casilla de verificación de la primera columna.

5 Haga clic en **Acciones > Reemplazar miembro de clúster de Edge**.

Se recomienda colocar el nodo de transporte en modo de mantenimiento. Si el nodo de transporte no se está ejecutando, puede ignorar esta recomendación de forma segura.

6 Seleccione el nodo que desea reemplazar de la lista desplegable.

7 Seleccione el nodo de reemplazo de la lista desplegable.

8 Haga clic en **Guardar**.

Reemplazar un nodo de transporte de NSX Edge mediante la API

En el siguiente procedimiento se describe cómo reemplazar un nodo de transporte de NSX Edge en un clúster de NSX Edge mediante NSX-T API. Puede reemplazar el nodo de transporte de Edge independientemente de si se está ejecutando o no.

Si el nodo de Edge que se va a reemplazar no está en ejecución, el nuevo nodo de Edge puede tener la misma dirección IP de administración y la misma dirección IP de TEP. Si el nodo de Edge que se va a reemplazar se está ejecutando, el nuevo nodo de Edge debe tener una dirección IP de administración y una dirección IP de TEP diferentes.

Requisitos previos

Familiarícese con el procedimiento para instalar un nodo de NSX Edge, unir el nodo de Edge con el plano de administración y crear un nodo de transporte de NSX Edge. Para obtener más información, consulte la *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 Si desea que el nuevo nodo de transporte de Edge tenga las mismas configuraciones que el nodo de transporte de Edge que se reemplazará, realice la siguiente llamada API para buscar las configuraciones:

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Siga los procedimientos de la guía de instalación de NSX-T Data Center para instalar y configurar un nodo de transporte de Edge.

Si desea que este nodo de transporte de Edge tenga las mismas configuraciones que el nodo de transporte de Edge que se reemplazará, utilice las configuraciones obtenidas en el paso 1.

- 3 Realice una llamada API para obtener el identificador del nuevo nodo de transporte y el nodo de transporte que se reemplazará. El campo `id` contiene el identificador del nodo de transporte. Por ejemplo,

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
```

```
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
  "display_name": "TN-edgenode-03a",

```

- 4 Realice una llamada API para obtener el identificador del clúster de NSX Edge. El campo `id` contiene el identificador del clúster de NSX Edge. Obtenga los miembros del clúster de NSX Edge en la matriz de `members`. Por ejemplo,

```
GET https://<nsx-manager-IP>/api/v1/edge-clusters
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {
      "member_index": 1,
      "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
    }
  ],

```

- 5 Haga que una API reemplace un nodo de transporte en un clúster de NSX Edge.
`member_index` debe coincidir con el índice del nodo de transporte que se va a reemplazar.

Por ejemplo, se produjo un error en el nodo de transporte `TN-edgenode-01a` (`73cb00c9-70d0-4808-abfe-a12a43251133`), que es reemplazado por el nodo de transporte `TN-edgenode-03a` (`890f0e3c-aa81-46aa-843b-8ac25fe30bd3`) en el clúster de NSX Edge `Edge-Cluster-1` (`9a302df7-0833-4237-af1f-4d826c25ad78`).

```
POST http://<nsx-manager-IP>/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

Recuperar NSX-T cuando se pierde vCenter Server y no se puede recuperar

Si se pierde vCenter Server (VC) y no se puede recuperar (por ejemplo, porque no hay ninguna copia de seguridad o porque esta está dañada), utilice el siguiente procedimiento para recuperar el entorno de NSX-T después de volver a implementar VC.

El nuevo VC debe tener el mismo FQDN y la misma dirección IP que el VC original. Además, debe tener los mismos clústeres que contengan los mismos hosts. Tenga cuidado con los hosts que tienen máquinas virtuales encendidas al agregarlas a VC. Asegúrese de que se agreguen a los clústeres correctos y no al centro de datos de VC.

Administrador de equipo

En NSX Manager, elimine el administrador de equipos anterior. A continuación, agregue el nuevo VC como administrador de equipos.

Nodos de transporte de host

En NSX Manager, los hosts aparecerán en los clústeres de VC correctos. No es necesario realizar ninguna acción.

Nodos de Edge

Debe reemplazar los nodos de Edge que se implementaron desde la interfaz de usuario de NSX Manager.

- 1 Siga el procedimiento descrito en [Reemplazar un nodo de transporte de NSX Edge mediante la interfaz de usuario de NSX Manager](#) para reemplazar un nodo de Edge.
- 2 Compruebe que las puertas de enlace (o enrutadores lógicos) y los túneles estén configurados en la nueva máquina virtual de Edge.
- 3 Para eliminar el nodo de Edge anterior, vaya a **Sistema > Tejido > Nodos de transporte de Edge**. Seleccione el nodo de Edge y haga clic en **Acciones > Eliminar**. Se pueden ignorar errores como "Error en el apagado".
- 4 En VC, apague la máquina virtual de Edge anterior y elimínela.
- 5 Repita los pasos anteriores para cada uno de los nodos de Edge.

NSX Manager

Debe reemplazar los NSX Manager que se implementaron desde la interfaz de usuario de NSX Manager. Por lo general, la segunda y la tercera instancia de NSX Manager se implementan de esta forma.

- 1 Inicie sesión en la primera interfaz de usuario de NSX Manager.

- 2 Vaya a **Sistema > Dispositivos** y seleccione el tercer NSX Manager. Haga clic en **Acciones > Eliminar**. Se producirá un error porque la máquina virtual de Manager no se puede apagar. La opción Forzar eliminación ahora estará disponible. Seleccione **Acciones > Forzar eliminación**.
- 3 Si no funciona, haga lo siguiente:
 - a Inicie sesión en la primera CLI de NSX Manager.
 - b Ejecute el comando `get cluster status` para obtener el UID del tercer NSX Manager.
 - c Ejecute el comando `detach node <node-uid>` para desasociar el tercer NSX Manager del clúster.
 - d Realice la siguiente llamada API para forzar la eliminación del tercer NSX Manager:

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
      action=delete&force_delete=true
```

- 4 En VC, apague y elimine el tercer NSX Manager.
- 5 Implemente un nuevo NSX Manager con la misma configuración que el tercer NSX Manager.
- 6 Repita los pasos anteriores para eliminar el segundo NSX Manager.
- 7 Implemente dos nuevos NSX Manager.

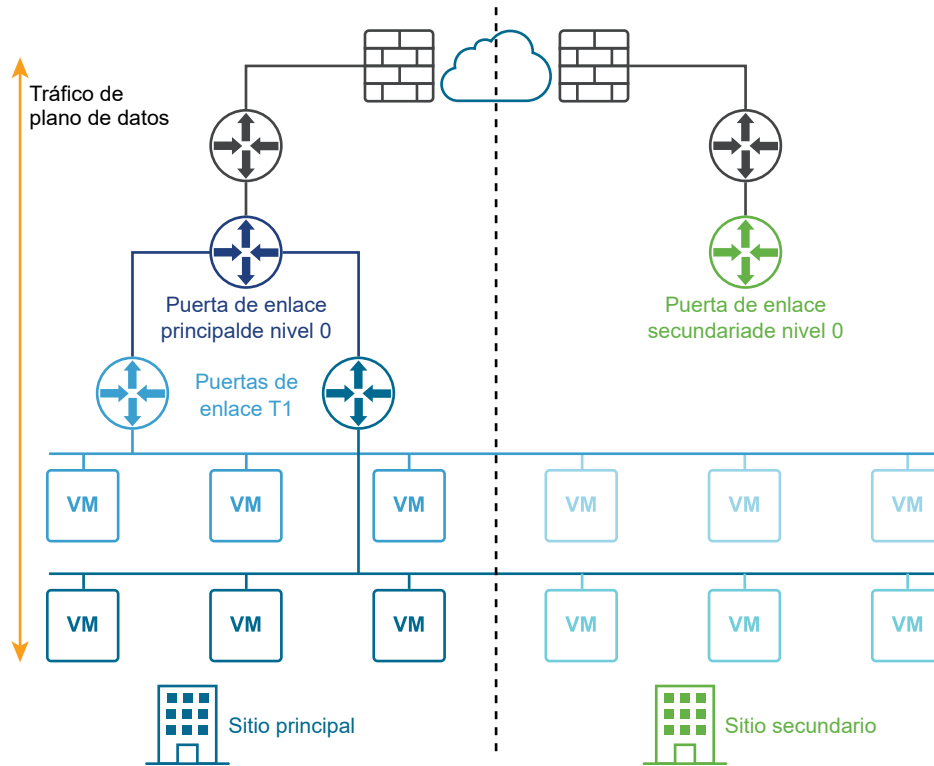
Implementación multisitio de NSX-T Data Center

NSX-T Data Center admite la implementación multisitio donde puede administrar todos los sitios de un clúster de NSX Manager.

Se admiten dos tipos de implementaciones multisitio:

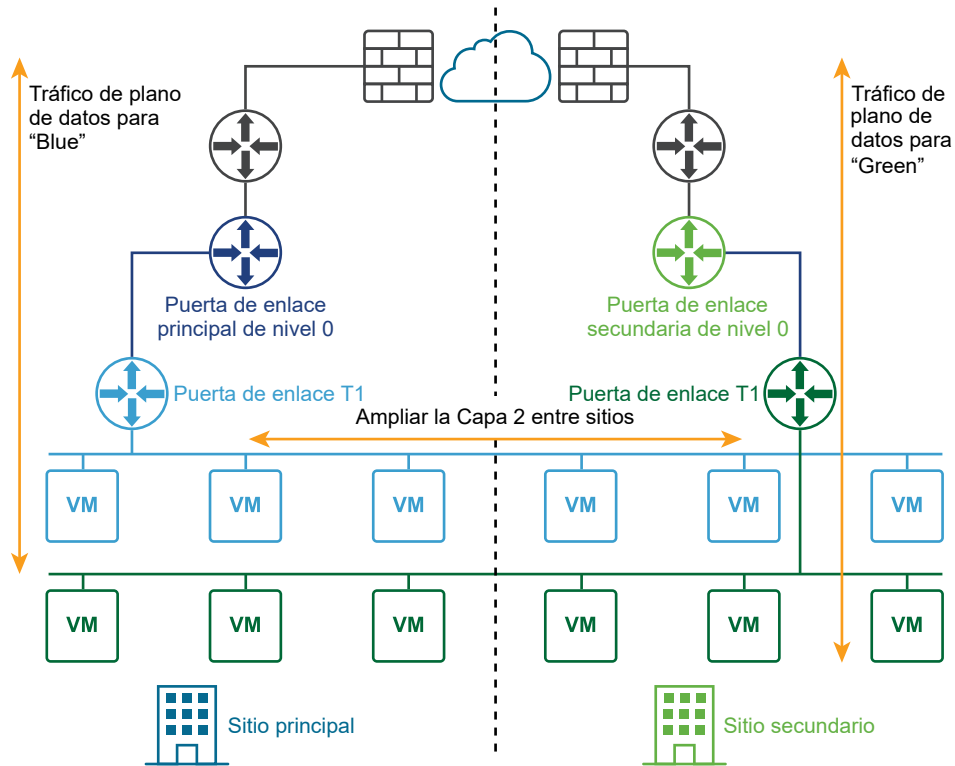
- Recuperación ante desastres
- Activo-activo

En el siguiente diagrama se muestra una implementación de recuperación ante desastres.



En una implementación activo-activo, todos los sitios están activos y el tráfico de Capa 2 cruza los límites del sitio. En una implementación de recuperación ante desastres, NSX-T Data Center en el sitio principal controla las redes de la empresa. El sitio secundario permanece inactivo para tomar el relevo si se produce un error grave en el sitio principal.

En el siguiente diagrama se muestra una implementación activo-activo.



Puede implementar dos sitios para la recuperación automática o manual/por script del plano de administración y del plano de datos.

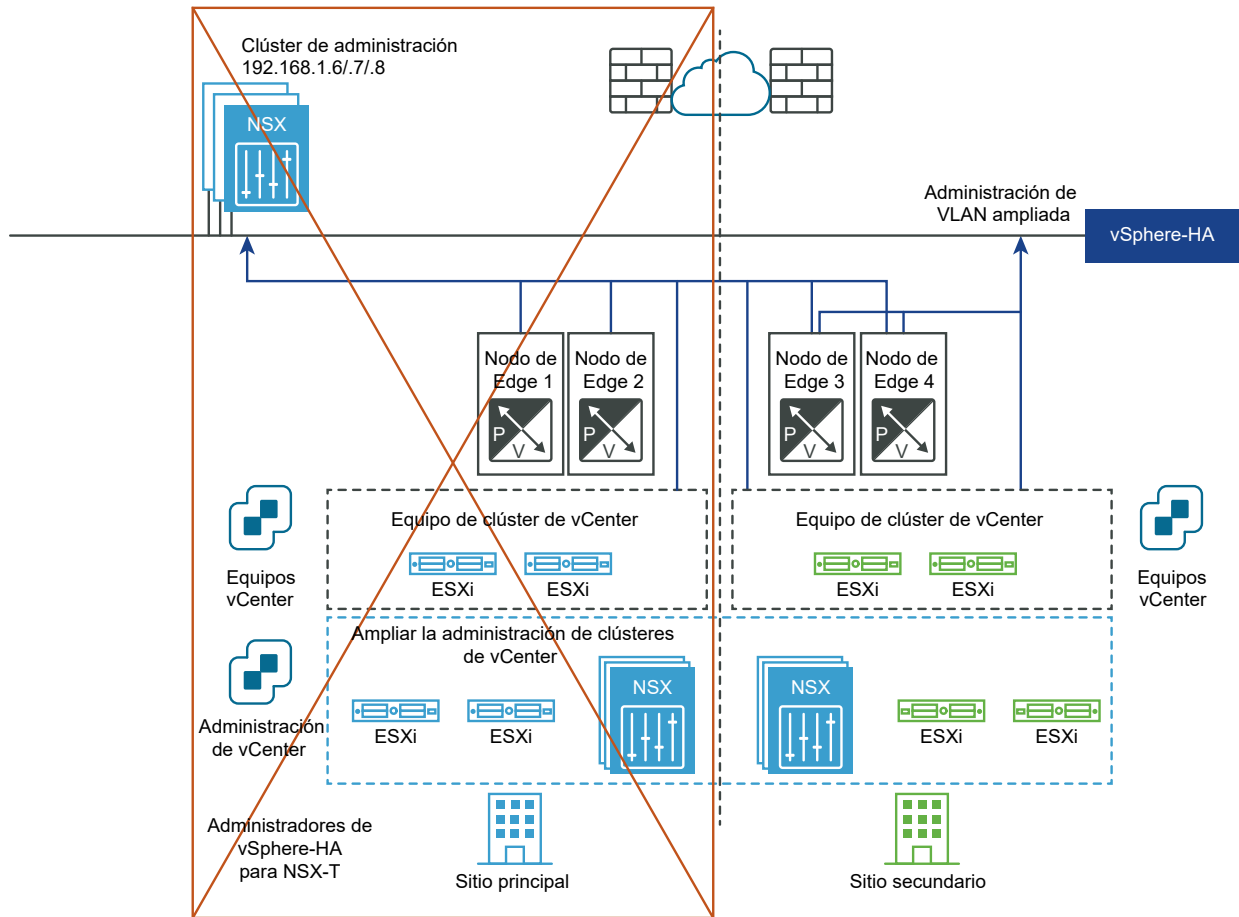
Recuperación automática del plano de administración

Requisitos:

- Un clúster de vCenter ampliado con HA en todos los sitios configurados.
- Una VLAN de administración ampliada.

El clúster de NSX Manager se implementa en la VLAN de administración y se encuentra físicamente en el sitio principal. Si se produce un error en el sitio principal, vSphere HA reiniciará las instancias de NSX Manager en el sitio secundario. Todos los nodos de transporte se reconectarán automáticamente a las instancias de NSX Manager reiniciadas. Este proceso dura unos 10 minutos. Durante este tiempo, el plano de administración no estará disponible, pero el plano de datos no se verá afectado.

En el siguiente diagrama se muestra la recuperación automática del plano de administración.



Recuperación automática del plano de datos

Requisitos:

- La latencia máxima entre los nodos de Edge es de 10 ms.
- El modo HA para la puerta de enlace de nivel 0 debe estar activo-en espera, y el modo de conmutación por error debe ser preferente.

Nota: El modo de conmutación por error de la puerta de enlace de nivel 1 puede ser preferente o no preferente.

Pasos de configuración:

- Mediante la API, cree dominios de errores para los dos sitios, por ejemplo `FD1A-Preferred_Sitel` y `FD2A-Preferred_Sitel`. En el parámetro `preferred_active_edge_services`, establezca `true` como sitio principal y `false` como sitio secundario.

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Sitel",
  "preferred_active_edge_services": "true"
}
```

```
POST /api/v1/failure-domains
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- Mediante la API, configure un clúster de Edge ampliado a los dos sitios. Por ejemplo, el clúster tiene los nodos de Edge EdgeNode1A y EdgeNode1B en el sitio principal, y los nodos de Edge EdgeNode2A y EdgeNode2B en el sitio secundario. Las puertas de enlace de nivel 0 y 1 activas se ejecutarán en EdgeNode1A y EdgeNode1B. Las puertas de enlace de nivel 0 y 1 en espera se ejecutarán en EdgeNode2A y EdgeNode2B.
- Usando la API, asocie cada nodo de Edge con el dominio de errores del sitio. En primer lugar, llame a la API GET /api/v1/transport-nodes/<transport-node-id> para obtener los datos sobre el nodo de Edge. Utilice el resultado de la API GET como entrada para la API PUT /api/v1/transport-nodes/<transport-node-id>, con la propiedad adicional failure_domain_id configurada correctamente. Por ejemplo,

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- Usando la API, configure el clúster de Edge para asignar nodos en función del dominio de errores. En primer lugar, llame a la API GET /api/v1/edge-clusters/<edge-cluster-id> para obtener los datos sobre el clúster de Edge. Utilice el resultado de la API GET como entrada para la API PUT /api/v1/edge-clusters/<edge-cluster-id>, con la propiedad adicional allocation_rules configurada correctamente. Por ejemplo,

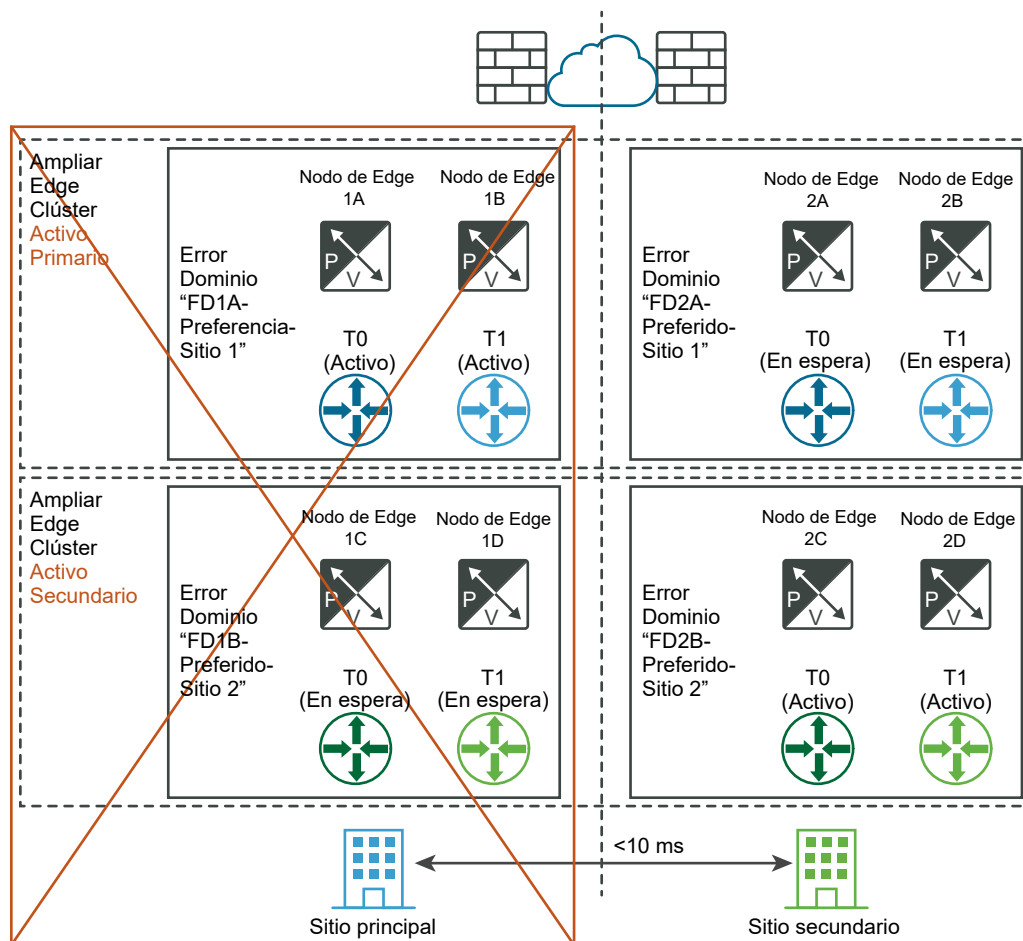
```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}
```

```
PUT /api/v1/edge-clusters/<edge-cluster-id>
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
  "allocation_rules": [
    {
      "action": {
        "enabled": true,
        "action_type": "AllocationBasedOnFailureDomain"
      }
    }
  ],
}
```

- Cree puertas de enlace de nivel 0 y 1 mediante la interfaz de usuario de NSX Manager o la API.

Cuando se produzca un error en un nodo de Edge del sitio principal, las puertas de enlace de nivel 0 y 1 alojadas en ese nodo se migrarán a un nodo de Edge en el sitio secundario.

En el siguiente diagrama se muestra la recuperación automática del plano de datos.



Recuperación manual/por script del plano de administración

Requisitos:

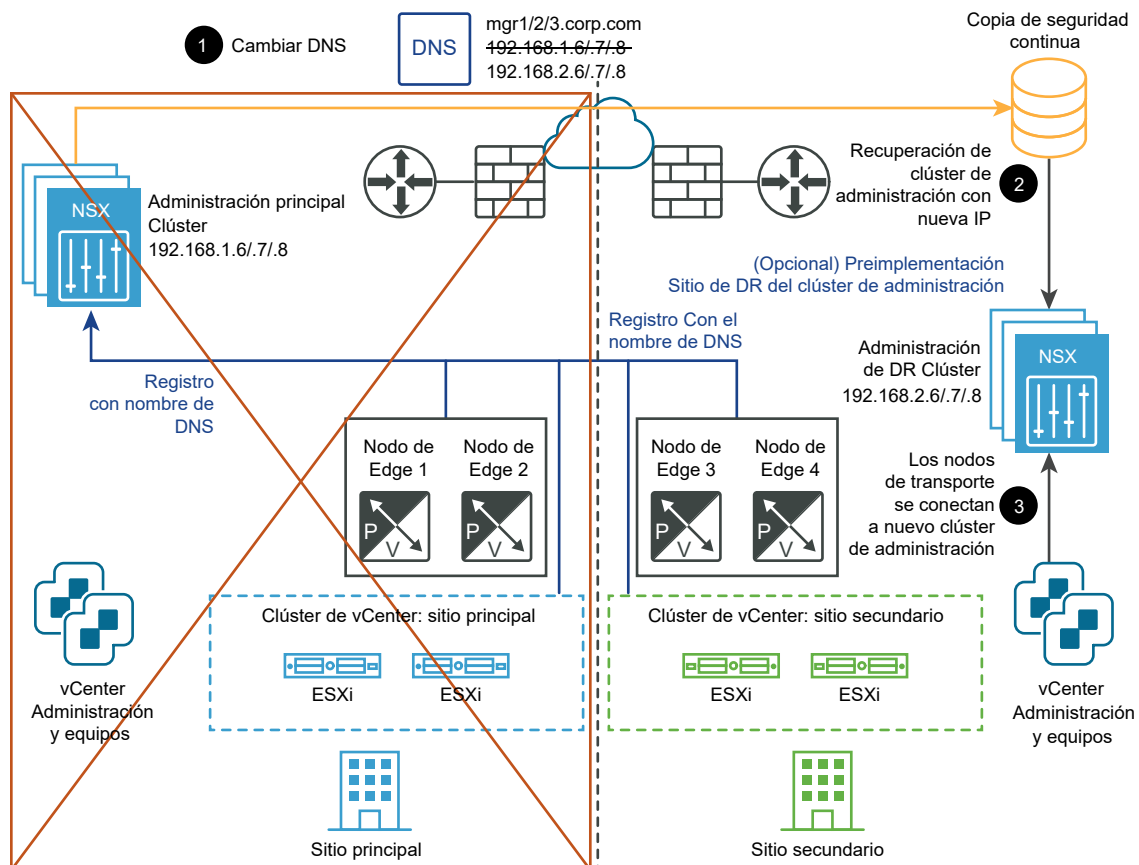
- DNS para NSX Manager con un TTL corto (por ejemplo, 5 minutos).
- Copia de seguridad continua.

No se requiere vSphere HA ni una VLAN de administración ampliada. Los administradores de NSX-T deben estar asociados a un nombre DNS con un TTL corto. Todos los nodos de transporte (hipervisores y nodos de Edge) deben conectarse a NSX Manager usando su nombre DNS. Para ahorrar tiempo, opcionalmente puede preinstalar un clúster de NSX Manager en el sitio secundario.

Los pasos de recuperación son:

- 1 Cambie el registro DNS para que el clúster de NSX Manager tenga diferentes direcciones IP.
- 2 Restaure el clúster de NSX Managera partir de una copia de seguridad.
- 3 Conecte los nodos de transporte al nuevo clúster de NSX Manager.

En el siguiente diagrama se muestra la recuperación manual/por script del plano de administración.



Recuperación manual/por script del plano de datos

Requisito:

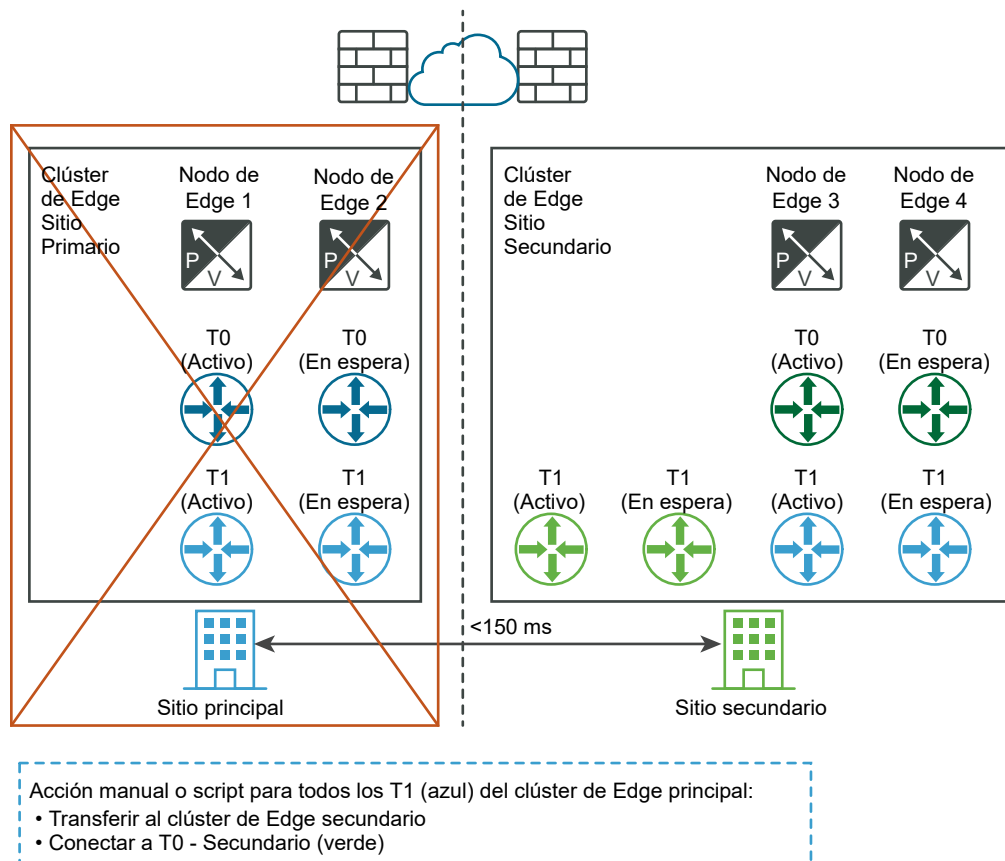
- La latencia máxima entre los nodos de Edge es de 150 ms.

Los nodos de Edge pueden ser máquinas virtuales o sin sistema operativo. La puerta de enlace de nivel 0 puede estar activa-en espera o activa-activa. Las máquinas virtuales de nodo de Edge se pueden instalar en diferentes instancias de vCenter Server. No se requiere vSphere HA.

Los pasos de recuperación son:

- 1 Cree una puerta de enlace de nivel 0 en espera en un clúster de Edge existente en el sitio de recuperación ante desastres (DR).
- 2 Use la API para mover las puertas de enlace de nivel 1 que están conectadas a una puerta de enlace de nivel 0 a la puerta de enlace de nivel 0 en el sitio de DR.
- 3 Use la API para mover las puertas de enlace de nivel 1 independientes al sitio de DR.
- 4 Usando la API, mueva los puentes puertas de nivel 2 al sitio de DR.

En el siguiente diagrama se muestra la recuperación manual/por script del plano de datos.



Requisitos para implementaciones multisitio

Comunicación entre sitios

- El ancho de banda debe ser 1 Gbps como mínimo y la latencia (RTT) debe ser inferior a 150 ms.
- La MTU debe ser de al menos 1.600. Se recomienda 9.000.

Configuración de NSX Manager

- La copia de seguridad automática cuando se modifica la configuración de NSX-T Data Center debe estar habilitada.
- NSX Manager se debe configurar para usar el FQDN.

Recuperación de plano de datos

- Si se debe utilizar el mismo proveedor de Internet cuando las direcciones IP públicas se exponen a través de servicios como NAT o el equilibrador de carga.
- El modo HA para la puerta de enlace de nivel 0 debe estar activo-en espera, y el modo de conmutación por error debe ser preferente.

Sistema de administración de nube

- El sistema de administración de nube (Cloud Management System, CMS) debe admitir un complemento de NSX-T Data Center. En esta versión, VMware Integrated OpenStack (VIO) y vRealize Automation (vRA) cumplen este requisito.

Limitaciones

- Sin capacidades de salida local. Todo el tráfico norte-sur debe realizarse dentro de un sitio.
- El software de recuperación ante desastres de equipos debe admitir NSX-T Data Center (por ejemplo, VMware SRM 8.1.2 o una versión posterior).

Configurar dispositivos

Se deben realizar algunas tareas de configuración del sistema con la API o la línea de comandos.

Para obtener información completa sobre la interfaz de línea de comandos, consulte la *referencia de la interfaz de línea de comandos de NSX-T Data Center*. Para obtener información completa sobre la API, consulte la *guía de la API de NSX-T Data Center*.

Tabla 21-7. Solicitudes de la API y comandos de configuración del sistema

Tarea	Línea de comandos (NSX Manager y NSX Edge)	Solicitud de la API (solo NSX Manager)
Establecer zona horaria del sistema	<code>set timezone <timezone></code>	<code>PUT https://<nsx-mgr>/api/v1/node</code>
Establecer servidor NTP	<code>set ntp-server <ntp-server></code>	<code>PUT https://<nsx-mgr>/api/v1/node/services/ntp</code>

Tabla 21-7. Solicitudes de la API y comandos de configuración del sistema (continuación)

Tarea	Línea de comandos (NSX Manager y NSX Edge)	Solicitud de la API (solo NSX Manager)
Establecer un servidor DNS	<code>set name-servers <dns-server></code>	<code>PUT https://<nsx-mgr>/api/v1/node/network/name-servers</code>
Establecer dominio de búsqueda de DNS	<code>set search-domains <domain></code>	<code>PUT https://<nsx-mgr>/api/v1/node/network/search-domains</code>

Agregar una clave de licencia y generar un informe de uso de licencias

Puede agregar claves de licencia y generar un informe de uso de licencias. El informe de uso es un archivo en formato CSV.

Están disponibles los siguientes tipos de licencias de no evaluación de NSX-T Data Center:

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office (ROBO)
- NSX Advanced (disponible desde NSX-T Data Center 2.5.1)
- NSX Enterprise (disponible desde NSX-T Data Center 2.5.1)

Al instalar NSX Manager, se activa una licencia de evaluación preinstalada. Esta licencia será válida durante 60 días. La licencia de evaluación proporciona todas las funciones de una licencia Enterprise. No puede instalar una licencia de evaluación ni quitar su asignación. Puede asignar una nueva licencia de evaluación cuando esté presente la licencia de evaluación predeterminada. La nueva licencia de evaluación sobrescribirá la licencia de evaluación predeterminada. También puede desasignar la licencia de evaluación no predeterminada. En ese caso, se restaurará la licencia de evaluación predeterminada.

Puede instalar una o varias licencias de no evaluación, pero solo puede instalar una clave por cada tipo. Al instalar una licencia Standard, Advanced o Enterprise, la licencia de evaluación dejará de estar disponible. También puede quitar la asignación de licencias de no evaluación. Si quita la asignación de todas las licencias de no evaluación, la licencia de evaluación se restaurará.

Si tiene varias claves del mismo tipo de licencia y desea combinarlas, debe acceder a la página <https://my.vmware.com> y utilizar la función Combinar claves. La interfaz de usuario de NSX Manager no ofrece esta función.

Si su licencia caduca en 60 días o si caducó, después de iniciar sesión en NSX Manager, aparecerá una ventana de notificación para informarle sobre la situación. También puede hacer clic en el icono de notificación situado en la esquina superior derecha de la ventana para ver la notificación.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Licencias > Agregar**.
- 3 Introduzca una clave de licencia.
- 4 Para generar un informe de uso de licencias, seleccione **Exportar > Informe de uso de licencias**.

El informe CSV especifica la máquina virtual, la CPU, el usuario simultáneo único, la vCPU y las cifras de uso principales de las siguientes funciones:

- Conmutación y enrutamiento
- Equilibrador de carga de NSX Edge
- VPN
- DFW
- Microsegmentación relacionada con el contexto: identificación de aplicación
- Microsegmentación relacionada con el contexto: firewall de identidad para host de sesión de escritorio remoto
- Inserción de servicios
- Firewall de identidad
- Introspección de invitado mejorada

Nota Las siguientes funciones están deshabilitadas en la versión Limited Export:

- IPsec VPN
 - Equilibrador de carga basado en HTTPS
-

Configurar certificados

Puede importar certificados, crear una solicitud de firma del certificado (CSR), generar certificados autofirmados e importar una lista de revocación de certificados (CRL).

Después de instalar NSX-T Data Center, el clúster y los nodos de NSX Manager tendrán certificados autofirmados. Para mejorar la seguridad, se recomienda reemplazar los certificados autofirmados por certificados firmados por una entidad de certificación.

Importar un certificado

Puede importar un certificado con una clave privada para sustituir un certificado autofirmado predeterminado después de activarlo.

Tenga en cuenta que solo se admiten certificados basados en RSA.

Requisitos previos

Compruebe que haya un certificado disponible.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 Seleccione **Importar > Importar certificado** y proporcione la información del certificado.

Opción	Descripción
Nombre	Asigne un nombre al certificado.
Contenido del certificado	Acceda al archivo de certificado en su equipo y agregue el archivo. El certificado no puede estar cifrado. Si se trata de un certificado firmado por una CA, asegúrese de incluir toda la cadena en este orden: certificado - intermedio - raíz.
Clave privada	Acceda al archivo de clave privada de su ordenador y agregue el archivo.
Frase de contraseña	Agregue una frase de contraseña para este certificado si está cifrado. En esta versión, este campo no se utiliza porque no se admite el certificado cifrado.
Descripción	Introduzca una descripción del contenido incluido en este certificado.
Certificado de servicio	Establézcalo en Sí para usar este certificado con servicios como un equilibrador de carga y una VPN. Establécalo en No si este certificado se utiliza con los nodos de NSX Manager.

- 4 Haga clic en **Importar**.

Crear un archivo de solicitud de firma del certificado

Una solicitud de firma del certificado (CSR) es un texto cifrado que contiene información específica, como el nombre de organización, el nombre común, la localidad y el país/región. El archivo CSR se envía a una entidad de certificación (CA) para solicitar un certificado de identidad digital.

Requisitos previos

- Recopile la información necesaria para rellenar el archivo CSR. Debe conocer el FQDN del servidor y la unidad de organización, la organización, la ciudad, el estado y el país/región.
- Compruebe que los pares de claves públicas y privadas están disponibles.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 Haga clic en la pestaña **CSR**.

4 Haga clic en **Generar CSR**.

5 Complete la información del archivo CSR.

Opción	Descripción
Nombre	Asigne un nombre al certificado.
Nombre común	Introduzca el nombre de dominio completo (FQDN) del servidor. Por ejemplo, test.vmware.com.
Nombre de organización	Introduzca el nombre de organización con los sufijos correspondientes. Por ejemplo, VMware Inc.
Unidad de organización	Introduzca el departamento de la organización que gestiona este certificado. Por ejemplo, el departamento de TI.
Localidad	Agregue la ciudad en la que se encuentra la organización. Por ejemplo, Palo Alto.
Estado	Agregue el estado en el que se encuentra la organización. Por ejemplo, California.
País/Región	Agregue el país/región donde se encuentra la organización. Por ejemplo, Estados Unidos (EE. UU.).
Algoritmo de mensaje	Establezca el algoritmo de cifrado para el certificado. El cifrado RSA se utiliza para firmas digitales y para cifrar el mensaje. Por lo tanto, es más lento que DSA a la hora de crear un token cifrado pero es más rápido a la hora de analizar y validar este token. Este cifrado es más lento a la hora de descifrar archivos y más rápido a la hora de cifrarlos. El cifrado DSA se utiliza para firmas digitales. Por lo tanto, es más rápido que RSA a la hora de crear un token cifrado pero es más lento a la hora de analizar y validar este token. Este cifrado es más rápido a la hora de descifrar archivos y más lento a la hora de cifrarlos.
Tamaño de clave	Establezca el tamaño de clave en bits del algoritmo de cifrado. El valor predeterminado (2.048) es adecuado a menos que necesite específicamente un tamaño de clave diferente. Muchas entidades de certificación necesitan un valor mínimo de 2.048. Los tamaños de claves mayores son más seguros pero tienen un mayor impacto en el rendimiento.
Descripción	Introduzca información específica que le ayude a identificar este certificado más adelante.

6 Haga clic en **Generar**.

Aparecerá una CSR personalizada en forma de vínculo.

7 Seleccione la CSR y haga clic en **Acciones**.

8 Seleccione **Descargar PEM de CSR**.

Puede guardar el archivo PEM de CSR para los registros y el envío de CA.

9 Utilice el contenido del archivo CSR para enviar una solicitud de certificado a la CA de acuerdo con el proceso de inscripción de CA.

Resultados

La CA crea un certificado de servidor según la información del archivo CSR, lo firma con su clave privada y le envía el certificado. La CA también le envía un certificado de CA raíz.

Importar un certificado de CA

Puede importar un certificado de CA firmado. Una vez importado y activado, NSX-T Data Center confiará en el resto de certificados firmados por esa CA.

Tenga en cuenta que solo se admiten certificados basados en RSA.

Requisitos previos

Compruebe que haya un certificado de CA disponible.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 Seleccione **Importar > Importar certificado de CA** y proporcione la información del certificado.

Opción	Descripción
Nombre	Asigne un nombre al certificado de CA.
Contenido del certificado	Acceda al archivo de certificado de CA de su ordenador y agregue el archivo.
Descripción	Introduzca un resumen del contenido incluido en este certificado de CA.
Certificado de servicio	Establézcalo en Sí para usar este certificado con servicios como un equilibrador de carga y una VPN. Establézcalo en No si este certificado se utiliza con los nodos de NSX Manager.

- 4 Haga clic en **Importar**.

Crear certificados de firma automática

Puede crear un certificado de firma automática. Sin embargo, es menos seguro que usar un certificado de confianza.

Al utilizar un certificado de firma automática, el usuario cliente recibe un mensaje de advertencia como, `Certificado de seguridad no válido`. El usuario cliente debe aceptar el certificado de firma automático cuando se conecte por primera vez al servidor para poder continuar. Permitir que los usuarios cliente seleccionen esta opción es menos seguro que otros métodos de autenticación.

Requisitos previos

Compruebe que una CSR esté disponible. Consulte [Crear un archivo de solicitud de firma del certificado](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 Haga clic en la pestaña **CSR**.
- 4 Seleccione una CSR.
- 5 Seleccione **Acciones > Autofirmar certificado para CSR**.
- 6 Introduzca el número de días de validez del certificado de firma automática.
El valor predeterminado es 10 años.
- 7 Haga clic en **Agregar**.

Resultados

El certificado de firma automática aparece en la pestaña **Certificados**.

Reemplazar el certificado de un nodo de NSX Manager o una IP virtual de clúster de NSX Manager

Puede reemplazar el certificado de un nodo de NSX Manager o la IP virtual (VIP) del clúster de NSX Manager mediante una llamada API.

Después de instalar NSX-T Data Center, el clúster y los nodos de NSX Manager tendrán certificados autofirmados. Para mejorar la seguridad, se recomienda reemplazar los certificados autofirmados por certificados firmados por una entidad de certificación y utilizar un certificado diferente para cada nodo.

Requisitos previos

Compruebe que haya un certificado disponible en NSX Manager. Consulte [Importar un certificado](#).

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 En la columna de identificadores, haga clic en el identificador del certificado que desee utilizar y cópielo de la ventana emergente.
Asegúrese de que cuando se importó este certificado, la opción **Certificado de servicio** se estableció en **No**.
- 4 Para reemplazar el certificado de un nodo de NSX Manager, utilice la llamada API `POST /api/v1/node/services/http?action=apply_certificate`. Por ejemplo,

`POST https://<nsx-mgr>/api/v1/node/services/http?action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f`

Nota: La cadena de certificados debe estar en el orden estándar de 'certificate - intermediate - root'.

Para obtener más información acerca de la API, consulte la *Referencia de API de NSX-T Data Center*.

- 5 Para reemplazar el certificado de la VIP del clúster de NSX Manager, utilice la llamada API POST `/api/v1/cluster/api-certificate?action=set_cluster_certificate`. Por ejemplo,

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

Nota: La cadena de certificados debe estar en el orden estándar de 'certificate - intermediate - root'.

Para obtener más información acerca de la API, consulte la *Referencia de API de NSX-T Data Center*. Este paso no es necesario si no configuró una VIP.

Importar una lista de revocación de certificados

Una lista de revocación de certificados (CRL) es una lista de suscriptores y del estado de sus certificados. Cuando un usuario potencial intenta acceder a un servidor, el servidor deniega el acceso según la entrada en la lista CRL para ese usuario en particular.

La lista contiene los siguientes elementos:

- Certificados revocados y motivos de las revocaciones.
- Fechas de emisión de los certificados.
- Entidades que emitieron los certificados.
- Fecha propuesta para la próxima versión.

Requisitos previos

Compruebe que haya disponible un CRL.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 Haga clic en la pestaña **CRL**.

4 Haga clic en **Importar** y agregue los detalles de la CRL.

Opción	Descripción
Nombre	Asigne un nombre a la CRL.
Contenido del certificado	<p>Copie todos los elementos de la CRL y péguelos en esta sección.</p> <p>Una CRL de muestra.</p> <pre> -----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEEMMAoGA1 UECBMD UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbMBkG A1UEAxMSU1NMZW51IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA OGCSqG SIB3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL-- </pre>
Descripción	Escriba un resumen de lo que se incluye en esta CRL.

5 Haga clic en **Importar**.

Resultados

La CRL importada aparece como un vínculo.

Cómo configurar NSX Manager para recuperar una lista de revocación de certificados

Puede utilizar la API para configurar NSX Manager y recuperar una lista de revocación de certificados (Certificate Revocation List, CRL). A continuación, puede comprobar la CRL mediante una llamada API a NSX Manager, en lugar de a la entidad de certificación.

Esta función ofrece las siguientes ventajas:

- Es más eficaz que la CRL se almacene en la memoria caché del servidor, que es NSX Manager.
- El cliente no necesita crear una conexión saliente con la entidad de certificación.

Puede utilizar las siguientes API relacionadas con las listas de revocación de certificados:

```

GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file

```


Puede administrar los puntos de distribución de la CRL y recuperar las CRL almacenadas en NSX Manager. Para obtener más información, consulte la *Referencia de API de NSX-T Data Center*.

Importar un certificado para una CSR

Puede importar un certificado firmado para una CSR.

Al utilizar un certificado de firma automática, el usuario cliente recibe un mensaje de advertencia como, *Certificado de seguridad no válido*. El usuario cliente debe aceptar el certificado de firma automático cuando se conecte por primera vez al servidor para poder continuar. Permitir que los usuarios cliente seleccionen esta opción es menos seguro que otros métodos de autenticación.

Requisitos previos

Compruebe que una CSR esté disponible. Consulte [Crear un archivo de solicitud de firma del certificado](#).

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Certificados**.
- 3 Haga clic en la pestaña **CSR**.
- 4 Seleccione una CSR.
- 5 Seleccione **Acciones > Importar certificado para CSR**.
- 6 Acceda al archivo del certificado firmado de su equipo y agregue el archivo.
- 7 Haga clic en **Agregar**.

Resultados

El certificado de firma automática aparece en la pestaña **Certificados**.

Almacenamiento de certificados públicos y claves privadas

Los certificados públicos y las claves privadas se almacenan en instancias de NSX Manager. Cuando se crea un equilibrador de carga o un servicio VPN que requiere una clave privada, NSX Manager envía una copia de la clave privada al nodo de Edge donde se ejecutan el equilibrador de carga o el servicio VPN.

Configuración basada en cumplimiento

NSX-T Data Center se puede configurar para que use los módulos criptográficos validados por FIPS 140-2 para que se ejecuten en un modo que cumpla los estándares FIPS. Los módulos se validan según los estándares FIPS 140-2 del programa de validación de módulos criptográficos (CMVP) de NIST.

Todas las excepciones al cumplimiento de FIPS se pueden obtener mediante el informe de cumplimiento. Consulte [Ver informe de estado de cumplimiento](#) para obtener más información.

En NSX-T Data Center 2.5 se usan los siguientes módulos validados:

- VMware OpenSSL FIPS Object Module 2.0.9: [certificado 2839](#)
- VMware OpenSSL FIPS Object Module 2.0.20-vmw: [certificado 3550](#)
- BC-FJA (Bouncy Castle FIPS Java API) 1.0.1: [certificado 3152](#)
- VMware IKE Crypto Module 1.1.0: [certificado 3435](#)
- VMware VPN Crypto Module 1.0: [certificado 3542](#)

Aquí puede consultar más información sobre los módulos criptográficos que VMware ha validado según en el estándar FIPS 140-2: <https://www.vmware.com/security/certifications/fips.html>.

De forma predeterminada, el equilibrador de carga utiliza módulos con el modo FIPS desactivado. Puede activar el modo FIPS para los módulos utilizados por el equilibrador de carga. Consulte [Configurar el modo de cumplimiento global de FIPS para el equilibrador de carga](#) para obtener más información.

Ver informe de estado de cumplimiento

Puede ver un informe de cumplimiento de las funciones de NSX-T Data Center. Puede utilizar el informe para configurar el entorno de NSX-T Data Center y cumplir las políticas de TI y los estándares de la industria.

El informe de cumplimiento incluye información sobre cada configuración que no cumple las políticas y los estándares.

Tabla 21-8. Información del informe de cumplimiento

Columna del informe de cumplimiento	Descripción	Ejemplo
Código de incumplimiento	Código para identificar el tipo de incumplimiento.	72301
Descripción	Descripción del tipo de incumplimiento.	El certificado no está firmado por una entidad de certificación.
Nombre de recurso	Nombre o identificador del recurso afectado.	nsx-manager-1
Tipo de recurso	Tipo de recurso afectado.	CertificateComplianceReporter
Recursos afectados	Número de recursos afectados. El número puede ser 0 si hay configuraciones infractoras, pero la función no se utilizará.	1

También puede obtener el informe mediante la API: `GET /policy/api/v1/compliance/status`.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 En la página **Inicio**, haga clic en **Paneles de control de supervisión > Informe de cumplimiento**.

Códigos de informe de estado de cumplimiento

A continuación, puede consultar más información sobre el significado del informe de estado de cumplimiento.

Tabla 21-9. Códigos del informe de cumplimiento

Código	Descripción	Origen del estado de cumplimiento	Corrección
72001	El cifrado está deshabilitado.	<p>Este estado se indica si una configuración de perfil de IPsec de VPN contiene los algoritmos de cifrado</p> <p>NO_ENCRYPTION, NO_ENCRYPTION_AUTH_AES_GMAC_128, NO_ENCRYPTION_AUTH_AES_GMAC_192 o NO_ENCRYPTION_AUTH_AES_GMAC_256.</p> <p>Este estado afecta a las configuraciones de sesión de VPN de IPsec que utilizan las configuraciones de no cumplimiento indicadas.</p>	<p>Para corregir este estado, agregue un perfil de IPsec de VPN que use algoritmos de cifrado en cumplimiento y utilícelo en todas las configuraciones de VPN. Consulte Agregar perfiles de IPsec.</p>
72011	Los mensajes vecinos BGP omiten la comprobación de integridad. No se ha definido ninguna autenticación de mensajes.	<p>Este estado se indica si no se configuró ninguna contraseña para los vecinos BGP.</p> <p>Este estado afecta a la configuración de vecinos BGP.</p>	<p>Para corregir este estado, configure una contraseña en el vecino BGP y actualice la configuración de la puerta de enlace de nivel 0 para que utilice la contraseña. Consulte Configurar BGP.</p>
72012	La comunicación con vecinos BGP utiliza una comprobación de integridad débil. MD5 se utiliza para la autenticación de mensajes.	<p>Este estado se indica si se utiliza la autenticación MD5 para la contraseña del vecino BGP.</p> <p>Este estado afecta a la configuración de vecinos BGP.</p>	<p>No hay ninguna corrección disponible, ya que NSX-T Data Center solo admite la autenticación MD5 para BGP.</p>

Tabla 21-9. Códigos del informe de cumplimiento (continuación)

Código	Descripción	Origen del estado de cumplimiento	Corrección
72021	Se utilizó SSL 3 para establecer la conexión segura del socket. Se recomienda utilizar TLS 1.1 o una versión posterior, y deshabilitar SSL 3 por completo, ya que tiene vulnerabilidades de protocolo.	<p>Este estado se indica si SSL 3 está configurado en el perfil SSL del cliente del equilibrador de carga, el perfil SSL del servidor del equilibrador de carga o el monitor HTTPS del equilibrador de carga.</p> <p>Este estado afecta a las siguientes configuraciones:</p> <ul style="list-style-type: none"> ■ Grupos de equilibradores de carga que están asociados con monitores HTTPS. ■ Servidores virtuales de equilibrador de carga que están asociados con perfiles SSL del cliente del equilibrador de carga o perfiles SSL del servidor. 	Para corregir este estado, configure un perfil SSL para que use TLS 1.1 o una versión posterior, y utilice este perfil en todas las configuraciones del equilibrador de carga. Consulte Agregar un perfil de SSL .
72022	Se utilizó TLS 1.0 utilizado para establecer la conexión segura del socket. Se recomienda utilizar TLS 1.1 o una versión posterior, y deshabilitar TLS 1.0 por completo, ya que tiene vulnerabilidades de protocolo.	<p>Este estado se indica si TLS 1.0 está configurado en el perfil SSL del cliente del equilibrador de carga, el perfil SSL del servidor del equilibrador de carga o el monitor HTTPS del equilibrador de carga.</p> <p>Este estado afecta a las siguientes configuraciones:</p> <ul style="list-style-type: none"> ■ Grupos de equilibradores de carga que están asociados con monitores HTTPS. ■ Servidores virtuales de equilibrador de carga que están asociados con perfiles SSL del cliente del equilibrador de carga o perfiles SSL del servidor. 	Para corregir este estado, configure un perfil SSL para que use TLS 1.1 o una versión posterior, y utilice este perfil en todas las configuraciones del equilibrador de carga. Consulte Agregar un perfil de SSL .

Tabla 21-9. Códigos del informe de cumplimiento (continuación)

Código	Descripción	Origen del estado de cumplimiento	Corrección
72023	Se utiliza un grupo Diffie-Hellman débil.	<p>Este error se indica si una configuración de perfil de IPsec o IKE de VPN incluye los siguientes grupos Diffie-Hellman: 2, 5, 14, 15 o 16. Los grupos 2 y 5 son grupos Diffie-Hellman débiles. Los grupos 14, 15 y 16 no son grupos débiles, pero no son compatibles con FIPS.</p> <p>Este estado afecta a las configuraciones de sesión de VPN de IPsec que utilizan las configuraciones indicadas como fuera de cumplimiento.</p>	Para corregir este estado, configure los perfiles de VPN para utilizar el grupo Diffie-Hellman 19, 20 o 21. Consulte Agregar perfiles .
72024	La configuración global de FIPS del equilibrador de carga está deshabilitada.	<p>Se indica este error si la configuración global de FIPS del equilibrador de carga está deshabilitada.</p> <p>Este estado afecta a todos los servicios del equilibrador de carga.</p>	Para corregir este estado, habilite FIPS para el equilibrador de carga. Consulte Configurar el modo de cumplimiento global de FIPS para el equilibrador de carga .
72200	No hay suficiente entropía real disponible.	<p>Este estado se indica cuando se utiliza un generador de números pseudoaleatorios para generar entropía en lugar de confiar en entropía generada por hardware.</p> <p>No se usa entropía generada por hardware porque el nodo de NSX Manager no dispone de la compatibilidad de aceleración de hardware necesaria para crear suficiente entropía real.</p>	<p>Para corregir este estado, es posible que deba utilizar hardware más reciente para ejecutar el nodo de NSX Manager. El hardware más reciente admite esta función.</p> <hr/> <p>Nota Si la infraestructura subyacente es virtual, no se obtendrá una entropía real.</p>

Tabla 21-9. Códigos del informe de cumplimiento (continuación)

Código	Descripción	Origen del estado de cumplimiento	Corrección
72201	Origen de entropía desconocido.	Este estado se indica cuando no hay ningún estado de entropía disponible para el nodo indicado.	Para corregir este estado, compruebe que el nodo indicado funciona correctamente.
72301	El certificado no está firmado por una entidad de certificación.	<p>Este estado se indica cuando uno de los certificados de NSX Manager no está firmado por una entidad de certificación. NSX Manager utiliza los siguientes certificados:</p> <ul style="list-style-type: none"> ■ Certificado Syslog. ■ Certificados de API para los nodos de NSX Manager individuales. ■ Certificado de clúster utilizado para la VIP de NSX Manager. 	Para corregir este estado, instale certificados firmados por una entidad de certificación. Consulte Configurar certificados .

Configurar el modo de cumplimiento global de FIPS para el equilibrador de carga

Existe una configuración global para que los equilibradores de carga cumplan el estándar FIPS. Esta opción está desactivada de forma predeterminada para mejorar el rendimiento.

Si se cambia la configuración global para que los equilibradores de carga cumplan el estándar FIPS, este cambio afectará a las nuevas instancias del equilibrador de carga, pero no a las instancias actuales.

Si la configuración global de FIPS para el equilibrador de carga (`lb_fips_enabled`) está establecida en `true`, las nuevas instancias del equilibrador de carga utilizarán módulos que cumplen con FIPS 140-2. Las instancias actuales del equilibrador de carga, en cambio, podrían estar utilizando módulos no conformes.

Para que el cambio se implemente en los equilibradores de carga actuales, debe desconectar el equilibrador de carga de la puerta de enlace de nivel 1 y volver a conectarlo.

Para comprobar el estado de cumplimiento de FIPS global del equilibrador de carga, utilice `GET /policy/api/v1/compliance/status`.

```
...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
```

```

        "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
        "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
        "target_type": "FipsGlobalConfig",
        "is_valid": true
    },
    "affected_resources": [
        {
            "path": "/infra/lb-services/LB_Service",
            "target_id": "/infra/lb-services/LB_Service",
            "target_display_name": "LB_1",
            "target_type": "LBService",
            "is_valid": true
        }
    ]
},
...

```

Nota El informe de cumplimiento muestra la configuración global de cumplimiento de FIPS del equilibrador de carga. Cada instancia del equilibrador de carga puede tener un estado de cumplimiento de FIPS distinto al de la configuración global.

Procedimiento

- 1 Recupere la configuración de FIPS global del equilibrador de carga.

GET <https://nsx-mgr1/policy/api/v1/infra/global-config>

Cuerpo de respuesta de ejemplo:

```

{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937915337,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 2
}

```

- 2 Cambie la configuración de FIPS global del equilibrador de carga.

La configuración global se utiliza cuando se crean nuevas instancias del equilibrador de carga. Cambiar la configuración no afecta a las instancias actuales del equilibrador de carga.

PUT <https://nsx-mgr1/policy/api/v1/infra/global-config>

Cuerpo de solicitud de ejemplo:


```
{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}
```


Cuerpo de respuesta de ejemplo:

```
{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}
```

- 3 Si desea que las instancias actuales del equilibrador de carga utilicen esta configuración global, debe desconectar el equilibrador de carga de la puerta de enlace de nivel 1 y volver a conectarlo.

Precaución Al desconectar un equilibrador de carga de la puerta de enlace de nivel 1, se interrumpe el tráfico en la instancia del equilibrador de carga.

- a Desplácese a **Redes > Equilibrio de carga**.
- b En el equilibrador de carga que desee desconectar, haga clic en el menú de tres puntos (⋮) y, a continuación, en **Editar**.
- c Haga clic en  y, a continuación, en **Guardar** para desconectar el equilibrador de carga de la puerta de enlace de nivel 1.

Nombre	Tamaño	Puerta de enlace de nivel 1
LB_1 *	Pequeño ▾	TLR1_LR 

- d Haga clic en el menú de tres puntos (⋮) y, a continuación, en **Editar**.
- e Seleccione la puerta de enlace correcta en el menú desplegable **Puerta de enlace de nivel 1** y, a continuación, haga clic en **Guardar** para volver a conectar el equilibrador de carga a la puerta de enlace de nivel 1.

Recopilar paquetes de soporte

Es posible recopilar paquetes de soporte de los clústeres y nodos de tejido y descargarlos en la máquina o cargarlos a un servidor de archivos.

Si decide descargar los paquetes en la máquina, obtendrá un único archivo de almacenamiento compuesto por un archivo de manifiesto y paquetes de soporte para cada nodo. Si opta por cargar los paquetes a un servidor de archivos, el archivo manifiesto y los paquetes individuales se cargan al servidor de archivos de forma independiente.

NSX Cloud Note Si desea recopilar el paquete de soporte para CSM, inicie sesión en CSM, vaya a **Sistema > Utilidades > Paquete de soporte** y haga clic en **Descargar**. El paquete de soporte para PCG está disponible en NSX Manager siguiendo estas instrucciones. El paquete de soporte para PCG también contiene registros para todas las máquinas virtuales de carga de trabajo.

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Paquete de soporte**
- 3 Seleccione los nodos de destino.

Los tipos de nodos disponibles son los **nodos de administración**, las **instancias de Edge**, los **hosts** y las **puertas de enlace de nube pública**.
- 4 (opcional) Especifique el número de días de antigüedad del registro para excluir aquellos que sean más antiguos que el número especificado.
- 5 (opcional) Alterne el conmutador que indica si incluir o excluir archivos básicos y registros de auditoría.

Nota Los archivos básicos y registros de auditoría incluyen información confidencial, como contraseñas o claves cifradas.

- 6 (opcional) Seleccione la casilla de verificación para cargar los paquetes a un servidor de archivos remoto.
- 7 Haga clic en **Iniciar recopilación de paquetes** para comenzar a recopilar paquetes de soporte.

En función del número de registros, cada nodo puede tardar varios minutos.
- 8 Supervise el estado del procedimiento de recopilación.

La pestaña de estado muestra el progreso de la recopilación de paquetes de soporte.

- 9 Haga clic en **Descargar** para descargar el paquete si la opción para enviarlo a un servidor de archivos remoto no está configurada.

Se puede producir un error en la recopilación del paquete para un nodo de Manager si no hay suficiente espacio de disco. Si se produce un error, compruebe si hay paquetes de soporte antiguos en el nodo con errores. Inicie sesión en la interfaz de usuario de NSX Manager del nodo de Manager con errores a través de su dirección IP e inicie la recopilación de paquetes desde ese nodo. Cuando NSX Manager lo solicite, descargue el paquete anterior o elimínelo.

Mensajes de registro y códigos de error

Los componentes de NSX-T Data Center escriben en los archivos de registro en el directorio `/var/log`. En los dispositivos de NSX-T y los hosts de KVM, los mensajes de syslog de NSX cumplen con RFC 5424. En hosts ESXi, los mensajes de syslog se ajustan a RFC 3164.

Ver registros

En NSX-T, los mensajes de syslog de dispositivos se encuentran en `/var/log/syslog`. En los hosts de KVM, los mensajes de syslog se encuentran en `/var/log/vmware/nsx-syslog`.

En los dispositivos de NSX-T, puede ejecutar el siguiente comando de la CLI de NSX-T para ver los registros:

```
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log |
node-mgmt.log | policy.log | syslog> [follow]
```

Los archivos de registro son:

Nombre	Descripción
auth.log	Registro de autorización
controlador	Registro del controlador
controller-error	Registro de errores de controlador
http.log	Registro del servicio HTTP
kern.log	Registro del kernel
manager.log	Registro del servicio de Manager
node-mgmt.log	Registro de administración de nodos
policy.log	Registro del servicio de directivas
syslog	Registro del sistema

En los hipervisores, puede utilizar comandos de Linux como `tac`, `tail`, `grep` y `more` para ver los registros.

Cada mensaje contiene información de componentes (`comp`) y subcomponentes (`subcomp`) para ayudar a identificar el origen del mensaje.

NSX-T Data Center genera registros con el recurso `local6`, que tiene un valor numérico de 22.

El registro de auditoría forma parte de syslog. Los mensajes de registro de auditoría pueden identificarse mediante la cadena `audit="true"` en el campo `structured-data`. Por ejemplo:

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true"
comp="nsx-manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy"
username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo",
Operation status="success"
```

Cada llamada de API produce un mensaje de registro de auditoría. Un registro de auditoría asociado con una llamada de API contiene la siguiente información:

- Un parámetro de ID de entidad `entId` para identificar el objeto de la API.
- Un parámetro de ID de solicitud `req-id` para identificar una llamada de API concreta.
- Un parámetro de ID de solicitud externa `ereqId` si la llamada de API contiene el encabezado `X-NSX-EREQID:<string>`.
- Un parámetro de usuario externo `euser` si la llamada de API contiene el encabezado `X-NSX-EUSER:<string>`.

RFC 5424 y RFC 3164 definen los siguientes niveles de gravedad:

Nivel de gravedad	Descripción
0	Emergencia: el sistema no se puede utilizar
1	Alerta: se debe realizar una acción inmediatamente
2	Gravedad: condiciones graves
3	Error: condiciones de error
4	Advertencia: condiciones de advertencia
5	Notificación: indica una condición normal, pero importante
6	Informativo: mensajes informativos
7	Depuración: mensajes de nivel de depuración

Todos los registros con un nivel de gravedad de emergencia, alerta, gravedad o error contienen un código de error único en la parte de datos estructurados del mensaje de registro. El código de error está compuesto por una cadena y un número decimal. La cadena representa un módulo específico.

Formatos de mensajes de registro

Para obtener más información sobre RFC 5424, consulte <https://tools.ietf.org/html/rfc5424>. Para obtener más información sobre RFC 3164, consulte <https://tools.ietf.org/html/rfc3164>.

RFC 5424 define el siguiente formato para los mensajes de registro:

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

Un mensaje de registro de ejemplo:

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker
'10.160.108.196'. Marking broker unhealthy.
```

Códigos de error

Para obtener una lista de los códigos de error, consulte el artículo 71077 de la base de conocimientos [Códigos de error de NSX-T Data Center 2.x](#).

Configurar registros remotos

Puede configurar dispositivos e hipervisores NSX-T Data Center para enviar mensajes de registro a un servidor de registro remoto.

El registro remoto es compatible con NSX Manager, NSX Edge y los hipervisores. Es necesario configurar el registro remoto en cada nodo de forma individual.

En un host de KVM, el paquete de instalación de NSX-T Data Center configura automáticamente el daemon rsyslog al colocar los archivos de configuración en el directorio `/etc/rsyslog.d`.

Requisitos previos

- Familiarícese con el comando de la CLI `set logging-server`. Para obtener más información, consulte la *referencia de la CLI de NSX-T*.
- Si utiliza los protocolos TLS o LI-TLS en la CLI de NSX para configurar una conexión segura a un servidor de registro, los certificados del servidor y del cliente deben almacenarse en `/image/vmware/nsx/file-store` en cada dispositivo de NSX-T Data Center. Tenga en cuenta que los certificados en el almacén de archivos solo son necesarios si el exportador está configurado mediante la CLI de NSX. Si utiliza la API, no es necesario usar el almacén de archivos. Una vez completada la configuración del exportador de Syslog, debe eliminar todos los certificados y las claves de esta ubicación para evitar posibles vulnerabilidades de seguridad.
- Para configurar una conexión segura a un servidor de registro, compruebe que el servidor esté configurado con certificados firmados por una entidad de certificación. Por ejemplo, si tiene un servidor de Log Insight `vrli.prome.local` como servidor de registro, puede ejecutar el siguiente comando desde un cliente para ver la cadena de certificados en el servidor:

```
root@caserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
```

```
2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
   i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE
```

Procedimiento

- 1 Para configurar un registro remoto en un dispositivo de NSX-T Data Center, ejecute el siguiente comando para configurar un servidor de registro y los tipos de mensajes que se pueden enviar a dicho servidor. Pueden especificarse varios recursos o identificadores de mensajes en una lista separada por comas, sin espacios.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility
<facility>] [messageid <messageid>] [serverca <filename>] [clientca <filename>]
[certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

Puede ejecutar el comando varias veces para agregar varias configuraciones. Por ejemplo:

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid
SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

Para reenviar únicamente los registros de auditoría al servidor remoto, especifique `audit="true"` en el parámetro `structured-data`. Por ejemplo:

```
set logging-server <server-ip> proto udp level info structured-data audit="true"
```

- 2 Para configurar el registro remoto seguro mediante el protocolo LI-TLS, especifique el parámetro `proto li-tls`. Por ejemplo:

```
set logging-server vrli.prome.local proto li-tls level info messageid
SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-
full-chain.crt
```

Si la configuración es correcta, recibirá un mensaje sin texto. Para ver el contenido de la cadena de certificados del servidor (intermedio seguido de la raíz), inicie sesión como `root` y ejecute el siguiente comando:

```
root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-
chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
```

```

Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

Los registros de las condiciones correctas y de error se encuentran en `/var/log/loginsight-agent/liagent_2020-MM-DD-<núm-archivo>.log`. Si la configuración es correcta, podrá ver la configuración de Log Insight con el siguiente comando:

```

root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrli.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" )}

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog
extract_sd=yes

[update]
auto_update=no

```

3 Para configurar el registro remoto seguro mediante el protocolo TLS, especifique el parámetro `proto tls`. Por ejemplo:

```
set logging-server vrli.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem
```

Tenga en cuenta lo siguiente:

- Para el parámetro `serverCA`, solo se requiere el certificado raíz, no la cadena completa.
- Si `clientCA` es diferente de `serverCA`, solo se requerirá el certificado raíz.
- El certificado debe contener la cadena completa de NSX Manager (debe ser compatible con NDcPP - ECU, BASIC y CDP (CDP - esta comprobación se puede ignorar))

Puede inspeccionar el contenido de cada certificado. Por ejemplo:

```
root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
    MD5: 36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
    SHA1: D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
    SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
    MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
```

```

SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

Ejemplos de inicio de sesión correcto en /var/log/syslog:

```

<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result: {'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514

```


Ejemplos de error de registro en /var/log/syslog:

```
<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green Intermediate Certification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-
manager" subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"]
Certificate trust check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied
key', 'status': 'ERROR'}
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-
manager" subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"]
Failed to create certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED
```

Puede comprobar si el certificado y la clave privada coinciden mediante el siguiente comando. Si coinciden, el resultado será `writing RSA key`. Cualquier otro resultado significará que no coinciden. Por ejemplo:

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key
```

Ejemplo de una clave privada dañada:

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
```

```

140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCWd2d2rZ09cUZV10P9
< kIYBb5RMFC7Z1OUtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDFASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----

```

Ejemplo de un certificado y una clave privada válida, pero que no coinciden:

```

root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCWd2d2rZ09cUZV10P9
< kIYBb5RMFC7Z1OUtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDFASmrj8CAwEAAQ==
---
> MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX2l6u5Jl4/X/pUDI/YHmIf06bsZlr/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KWVFe3gw3homHU39q4pQjsJsxTcTE3oDMLIY0nWJ0PRUst3DffYUH1L
> W0NUN9yDN+fa12Uf021iuDqVy9V8AH3ON6fu+QCA8nt71zkzeTxSA0ldpl2NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r300itnyAzEGLaRT3//PKfe0Oe
> HCdxGMLrUtMqxIItJahEsqvMufyqNYecVscYXLHPelizKCsQfy8c08LnznG8VAdc
> YILSn3uYGZap6aF1SgVxsvZicwvYnssmgE13Af0nScmfM96k9h5joHVEkWK6O8v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektr8HdMHQit5uvmMRY3S5zow

```

```
> FtvfSDfWxxKyTy6GBrpP+8F+Jq91yGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hbvXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmMveinDhU35IqWEXHAWcCAwEAAQ==
```

- 4 Para ver la configuración de registro, ejecute el comando `get logging-server`. Por ejemplo,

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

- 5 Para borrar la configuración del registro remoto, ejecute el siguiente comando:

```
nsx> clear logging-servers
```

- 6 Para configurar el registro remoto en un host ESXi:

- a Ejecute los siguientes comandos para configurar syslog y enviar un mensaje de prueba:

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b Puede ejecutar el siguiente comando para ver la configuración:

```
esxcli system syslog config get
```

- 7 Para configurar el registro remoto en un host de KVM:

- a Edite el archivo `/etc/rsyslog.d/10-vmware-remote-logging.conf` para su entorno.
- b Agregue la siguiente línea al archivo:

```
*.* @<ip>:514;RFC5424fmt
```

- c Ejecute el siguiente comando:

```
service rsyslog restart
```

Identificadores de mensajes de registro

En un mensaje de registro, el campo de identificador de mensaje identifica el tipo de mensaje. Puede usar el parámetro `messageid` en el comando `set logging-server` para filtrar los mensajes de registro que se envían a un servidor de registro.

Tabla 21-10. Identificadores de mensajes de registro

identificador de mensaje	Ejemplos
FABRIC	<p>Nodo de host</p> <p>Preparación del host</p> <p>Nodo de Edge</p> <p>Zona de transporte</p> <p>Nodo de transporte</p> <p>Perfiles de vínculo de carga</p> <p>Perfiles de clúster</p> <p>Clúster de Edge</p>
SWITCHING	<p>Conmutador lógico</p> <p>Puertos del conmutador lógico</p> <p>Perfiles de conmutación</p> <p>Funciones de seguridad del conmutador</p>
ROUTING	<p>Enrutador lógico</p> <p>Puertos del enrutador lógico</p> <p>Enrutamiento estático</p> <p>Enrutamiento dinámico</p> <p>NAT</p>
FIREWALL	<p>Reglas de firewall</p> <p>Secciones de reglas de firewall</p>
FIREWALL-PKTLOG	<p>Registros de conexión de firewall</p> <p>Registros de paquete de firewall</p>
GROUPING	<p>Conjuntos de direcciones IP</p> <p>Conjuntos de direcciones MAC</p> <p>grupos NSGroup</p> <p>servicios NSService</p> <p>Grupos de NSService</p> <p>Grupo de VNI</p> <p>Grupo de direcciones IP</p>
DHCP	<p>Retransmisión DHCP</p>
SYSTEM	<p>Administración de dispositivos (syslog remoto, ntp, etc.)</p> <p>Administración de clústeres</p> <p>Administración de confianza</p> <p>Licencias</p> <p>Usuarios y funciones</p> <p>Administración de tareas</p> <p>Instalar</p> <p>Actualización (actualizaciones de paquetes de hosts, NSX Manager y NSX Edge)</p> <p>Realización</p> <p>Etiquetas</p>

Tabla 21-10. Identificadores de mensajes de registro (continuación)

identificador de mensaje	Ejemplos
MONITORING	SNMP Conexión de puertos Traceflow
-	El resto de los mensajes de registro

Solucionar problemas de syslog

Si el servidor de registros remoto no recibe registros, realice los siguientes pasos.

- Compruebe la dirección IP del servidor de registros remoto.
- Verifique que la configuración del parámetro `level` sea correcta.
- Verifique que la configuración del parámetro `facility` sea correcta.
- Si el protocolo es TLS, establézcalo como UDP para determinar si hay un error de coincidencia de certificado.
- Si el protocolo es TLS, compruebe que el puerto 6514 esté abierto en ambos extremos.
- Quite el filtro de identificadores de mensajes y compruebe si el servidor recibe registros.
- Reinicie el servicio rsyslog con el comando `restart service rsyslogd`.

Configurar el registro serie en una máquina virtual de dispositivo

Puede configurar el registro serie en una máquina virtual de dispositivo para capturar los mensajes de registro cuando la máquina virtual se bloquea.

Procedimiento

- 1 Inicie sesión en la máquina virtual como `root`.
- 2 Edite `/etc/default/grub`.
- 3 Busque el parámetro `GRUB_CMDLINE_LINUX_DEFAULT` y anéxele `console=ttyS0 console=tty0`.
- 4 Ejecute el comando `update-grub2`.
- 5 Compruebe que el archivo `/boot/grub/grub.cfg` tiene el cambio realizado en el paso 3.
- 6 Apague la máquina virtual.
- 7 Edite el archivo de configuración (`.vmx`) de la máquina virtual y agregue las siguientes líneas:

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsrRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

8 Encienda la máquina virtual (VM).

Resultados

Si se produce un error en el kernel de la máquina virtual, puede encontrar el archivo `serial.out` que contiene los mensajes de registro en la misma ubicación que el archivo `.vmtx`.

Programa de mejora de la experiencia de cliente

NSX-T Data Center participa en el programa de mejora de la experiencia de cliente (CEIP) de VMware.

Los detalles relacionados con los datos recopilados mediante el CEIP, así como los fines para los que VMware los utiliza, se pueden encontrar en el Centro de seguridad y confianza en <https://www.vmware.com/solutions/trustvmware/ceip.html>.

Si desea unirse o abandonar el CEIP de NSX-T Data Center o editar la configuración del programa, consulte [Editar la configuración del programa de mejora de la experiencia de cliente](#).

Editar la configuración del programa de mejora de la experiencia de cliente

Al instalar o actualizar NSX Manager, puede decidir participar en el CEIP y configurar los ajustes de recopilación de datos.

También puede editar la configuración existente del CEIP para unirse al programa o abandonarlo, definir la frecuencia y los días de recopilación de la información y establecer la configuración del servidor proxy.

Requisitos previos

- Compruebe que NSX Manager esté conectado y se pueda sincronizar con el hipervisor.
- Compruebe que NSX-T Data Center esté conectado a una red pública para cargar datos.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Sistema > Programa de cliente**.
- 3 Haga clic en **Editar** en la sección del programa de mejora de la experiencia de cliente.
- 4 En el cuadro de diálogo Editar programa de experiencia de cliente, seleccione la casilla **Unirse al programa de mejora de la experiencia de cliente de VMware**.
- 5 Active o desactive el conmutador **Programación** para deshabilitar o habilitar la recopilación de datos.

La programación está habilitada de manera predeterminada.

- 6 (opcional) Configure la recopilación de datos y cargue la configuración de periodicidad.

7 Haga clic en **Guardar**.

Agregar etiquetas a un objeto

Puede agregar etiquetas a objetos para que las búsquedas se realicen fácilmente. Cuando especifique una etiqueta, también puede especificar un ámbito.

Nota sobre NSX Cloud Si utiliza NSX Cloud, consulte la sección sobre [Funciones de NSX-T Data Center admitidas por NSX Cloud](#) para obtener una lista de las entidades lógicas generadas automáticamente, las funciones admitidas y configuraciones requeridas para NSX Cloud.

La mayoría de objetos puede tener hasta 30 etiquetas. En lo que respecta a los siguientes objetos, la cifra máxima de etiquetas es inferior debido a las etiquetas que se crean y utilizan de forma interna.

Tabla 21-11. Número máximo de etiquetas para los objetos creados mediante la pestaña Opciones avanzadas de redes y seguridad

Objeto	Número máximo de etiquetas
máquina virtual	25
Puerto lógico	29

Tabla 21-12. Número máximo de etiquetas para los objetos creados mediante las pestañas Redes, Seguridad o Inventario

Objeto	Número máximo de etiquetas
Grupo	29
Segmento	27
Puerto de segmento	29
Puerto de enrutador lógico	30 (número de etiquetas)
Regla NAT	27
Sesión de VPN de IPSec	29

Tabla 21-13. Número máximo de etiquetas para los objetos de Cloud Service Manager

Objeto	Número máximo de etiquetas
Perfil de supervisión de estado de BFD, zona de transporte, perfil de conmutador de host de vínculo superior, nodo de transporte y clúster de Edge	23

Tabla 21-14. Número máximo de etiquetas para los objetos de administrador de nube pública

Objeto	Número máximo de etiquetas
Perfil de supervisión de estado de BDF, zona de transporte, conmutador lógico, nodo, nodo de transporte, clúster de Edge, enrutador lógico, puerto de vínculo superior de enrutador lógico, ruta estática, perfil de DHCP, NSGroup y lista de reglas de sección de firewall	23
Regla NAT	20
Conjunto de direcciones IP, NSGroup	22

Procedimiento

- 1 En un explorador, acceda a <https://<dirección-ip-de-nsx-manager>> e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Edite un objeto.
Por ejemplo, vaya a la pestaña **Segmentos** y edite un segmento.
- 3 Vaya al campo **Etiquetas** y agregue etiquetas.
Cada etiqueta tiene un valor de etiqueta, que es obligatorio, y un valor de alcance, que es opcional. La longitud máxima de una etiqueta es de 256 caracteres. La longitud máxima de un ámbito es de 128 caracteres.
- 4 Haga clic en **Guardar**.

Buscar la huella digital SSH de un servidor remoto

Algunas solicitudes de API que implican copiar archivos de un servidor remoto o copiarlos en él necesitan que proporcione la huella digital SSH del servidor remoto en el cuerpo de la solicitud. La huella digital SSH se obtiene de una clave de host del servidor remoto.

Para conectarse a través de SSH, NSX Manager y el servidor remoto deben tener un tipo de clave de host en común. Si hay varios tipos de claves de host en común, se utilizará la preferida según la configuración HostKeyAlgorithm de NSX Manager.

La huella digital de un servidor remoto le ayudará a confirmar que está conectado al servidor correcto y le protegerá frente a ataques de tipo "man-in-the-middle". Puede pedir al administrador de un servidor remoto si puede proporcionar la huella digital SSH del servidor, o bien puede conectarse al servidor remoto para buscar la huella digital. Conectarse al servidor mediante una consola es más seguro que mediante la red.

La siguiente tabla muestra qué admite NSX Manager, siguiendo un orden de mayor a menos preferencia.

Tabla 21-15. Claves de host de NSX Manager ordenadas por preferencia

Tipos de claves de host que admite NSX Manager	Ubicación predeterminada de la clave
ECDSA (256 bits)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

Procedimiento

- 1 Inicie sesión en el servidor remoto como usuario raíz.
Iniciar sesión con una consola es más seguro que mediante la red.
- 2 Incluya los archivos de claves públicas en el directorio `/etc/ssh`.

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root  93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

- 3 Compare las claves disponibles con las que NSX Manager admite.
En este ejemplo, ED25519 es la única clave admitida.
- 4 Obtenga la huella digital de la clave.

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed
's/ .*$/' | xxd -r -p | base64 | sed 's/./44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

Ver datos de aplicaciones que se ejecutan en máquinas virtuales

Puede consultar información acerca de las aplicaciones que se ejecutan en máquinas virtuales que sean miembros de un grupo NSGroup. Esta es una función de vista previa técnica.

Procedimiento

- 1 En un explorador, acceda a `https://<dirección-ip-de-nsx-manager>` e inicie sesión en NSX Manager con privilegios de administrador.
- 2 Seleccione **Opciones avanzadas de redes y seguridad > Inventario > Grupos**.
- 3 Haga clic en el nombre de un grupo NSGroup.
- 4 Haga clic en la pestaña **Aplicaciones**.
- 5 Haga clic en **RECOPILAR DATOS DE LA APLICACIÓN**.

Este proceso puede tardar unos minutos. Al finalizar el proceso, se muestra la siguiente información:

- El número total de procesos.

- Círculos que representan los diversos niveles, por ejemplo, el nivel de web, el nivel de base de datos o el nivel de aplicación. También se muestra el número de procesos de cada nivel.

6 Haga clic en un círculo para obtener más información acerca de los procesos de ese nivel.

Configurar un equilibrador de carga externo

Puede configurar un equilibrador de carga externo para distribuir el tráfico a las instancias de NSX Manager en un clúster de administrador.

Un clúster de NSX Manager no requiere un equilibrador de carga externo. La dirección IP virtual (VIP) de NSX Manager proporciona resistencia en caso de que falle el nodo de Manager, pero tiene las siguientes limitaciones:

- La VIP no realiza el equilibrio de carga entre instancias de NSX Manager.
- La VIP requiere que todas las instancias de NSX Manager estén en la misma subred.
- La recuperación de la VIP tarda entre 1 y 3 minutos en el caso de que falle el nodo de Manager.

Un equilibrador de carga externo puede ofrecer las siguientes ventajas:

- Equilibrio de carga entre las instancias de NSX Manager.
- Las instancias de NSX Manager pueden encontrarse en subredes diferentes.
- Tiempo de recuperación rápido en caso de que falle el nodo de Manager.

Tenga en cuenta que un equilibrador de carga externo no funcionará con la VIP de NSX Manager. No configure una VIP de NSX Manager si utiliza un equilibrador de carga externo.

Al acceder a NSX Manager desde un navegador a través de un equilibrador de carga externo, deberá habilitar la persistencia de la sesión en el equilibrador de carga.

Al acceder a NSX Manager desde un cliente de API a través de un equilibrador de carga externo, hay cuatro métodos de autenticación disponibles (consulte la guía de la API de *NSX-T Data Center* para obtener más información):

- Autenticación básica HTTP: no se requiere persistencia de la sesión del equilibrador de carga.
- Autenticación de certificado de cliente: no se requiere persistencia de la sesión del equilibrador de carga.
- Autenticación en vIDM: no se requiere persistencia de la sesión del equilibrador de carga.
- Autenticación basada en sesiones: se requiere persistencia de la sesión del equilibrador de carga.

Recomendación:

- Configure una única dirección IP en el equilibrador de carga externo para el acceso mediante navegador y API. El equilibrador de carga debe tener habilitada la persistencia de la sesión.

NSX Cloud permite administrar y proteger el inventario de nube pública mediante el uso de NSX-T Data Center.

Consulte [Instalar componentes de NSX Cloud](#) en la *Guía de instalación de NSX-T Data Center* para obtener información sobre el flujo de trabajo de implementación de NSX Cloud.

Consulte también: [nube pública](#).

Este capítulo incluye los siguientes temas:

- [Un paseo rápido por Cloud Service Manager](#)
- [Detección de amenazas mediante la directiva de cuarentena de NSX Cloud](#)
- [Modo forzado de NSX](#)
- [Modo forzado de nube nativa](#)
- [Funciones de NSX-T Data Center admitidas por NSX Cloud](#)
- [Preguntas frecuentes](#)

Un paseo rápido por Cloud Service Manager

Cloud Service Manager (CSM) proporciona un endpoint de administración de un panel centralizado para el inventario de nube pública.

La interfaz de CSM se divide en las siguientes categorías:

- **Buscar:** puede utilizar el cuadro de texto de búsqueda para explorar las cuentas de nube pública o las construcciones relacionadas.
- **Nubes:** el inventario de nube pública se administra a través de las secciones dentro de esta categoría.
- **Sistema:** puede acceder a **Configuración**, **Utilidades** y **Usuarios** para Cloud Service Manager en esta categoría.

Para realizar operaciones de nube pública, vaya a la subsección **Nubes** de CSM.

Para realizar operaciones del sistema, como copias de seguridad, restauración, actualización y administración de usuarios, vaya a la subsección **Sistema**.

Nubes

Estas son las secciones en **Nubes**:

Nubes > Información general

Para acceder a su cuenta de nube pública, haga clic en **Nubes**.

Información general: cada mosaico de esta pantalla representa su cuenta de nube pública con el número de cuentas, regiones, VPC o VNet e instancias (máquinas virtuales de carga de trabajo) que contiene.

Puede realizar las siguientes tareas:

Agregar una suscripción o cuenta de nube pública	<p>Puede agregar una o varias suscripciones o cuentas de nube pública. Esto le permite ver el inventario de nube pública en CSM, e indica el número de máquinas virtuales que están administradas por NSX-T Data Center y su estado.</p> <p>Consulte Agregar una cuenta de nube pública en la <i>Guía de instalación de NSX-T Data Center</i> para obtener instrucciones detalladas.</p>
Implementar o anular la implementación de NSX Public Cloud Gateway	<p>Puede implementar o anular la implementación de una o dos (para High Availability) PCG. También puede anular la implementación de PCG desde CSM.</p> <p>Consulte Implementar PCG o Anular implementación de PCG en la <i>Guía de instalación de NSX-T Data Center</i> para obtener instrucciones detalladas.</p>
Habilitar o deshabilitar la directiva de cuarentena	<p>Puede habilitar o deshabilitar la directiva de cuarentena. Consulte Detección de amenazas mediante la directiva de cuarentena de NSX Cloud para obtener detalles.</p>
Cambiar entre la vista de cuadrícula y la de tarjeta	<p>Las tarjetas muestran un resumen del inventario. La cuadrícula muestra más detalles. Haga clic en los iconos para cambiar entre los tipos de vista.</p>

CSM proporciona una visión holística de todas sus cuentas de nube pública que se han conectado con NSX Cloud presentando su inventario de nube pública de distintas formas:

- Puede ver el número de regiones en las que está trabajando.
- Puede ver el número de VPC o VNet por región.
- Puede ver el número de máquinas virtuales de carga de trabajo por VPC o VNet.

Hay cuatro pestañas en **Nubes**.

Nubes > {Su nube pública} > Cuentas

La sección Cuentas de CSM proporciona información sobre las cuentas de nube pública que ya se han agregado.

Cada tarjeta representa una cuenta de nube pública del proveedor de nube que seleccionó en la sección Nubes.

En esta sección, puede realizar las siguientes acciones:

- Agregar una cuenta

- Editar una cuenta
- Eliminar una cuenta
- Volver a sincronizar una cuenta

Nubes > {Su nube pública} > Regiones

La sección Regiones muestra el inventario de una región seleccionada.

Puede filtrar las regiones según la cuenta de nube pública. Cada región tiene VPC o VNet e instancias. Si se han implementado PCG, se mostrarán aquí como **puertas de enlace** con un indicador de estado de PCG.

Nubes > {Su nube pública} > VPC o VNet

La sección VPC o VNet muestra el inventario de la nube pública.

Puede filtrar el inventario por cuenta y región.

- Cada tarjeta representa una VPC o una VNet.
- Puede haber una o dos instancias de PCG (para HA) implementadas en las VPC o las VNet de tránsito.
- Puede vincular las VPC o las VNet de equipo a las VPC o las VNet de tránsito.
- Para ver más detalles de cada VPC o VNet, cambie a la vista de cuadrícula.

Nota En la vista de cuadrícula, puede ver tres pestañas: **Información general**, **Instancias** y **Segmentos**.

- En **Descripción general** se incluyen las opciones de Acciones que se describen en el siguiente paso.
 - En **Instancias** se muestra una lista de instancias de en la VPC/VNet.
 - **Segmentos** muestra segmentos superpuestos en NSX-T. Esta función no se admite en la versión actual de NSX Cloud. No etiquete las máquinas virtuales de carga de trabajo en AWS o Microsoft Azure con las etiquetas que se muestran en esta pantalla.
-
- Haga clic en **Acciones** para acceder a las siguientes opciones:
 - **Editar configuración** (solo disponible para las VPC o las VNet de tránsito):
 - Habilite o deshabilite la directiva de cuarentena si utiliza Modo forzado de NSX .
 - Proporcione un grupo de seguridad de reserva que se requiere para retirar la VPC la VNet de NSX Cloud en Modo forzado de NSX . Consulte [Impacto de la directiva de cuarentena cuando se deshabilita](#).
 - Cambie la selección del servidor proxy.
 - **Vincular a VPC o VNet de tránsito**: esta opción solo está disponible para las VPC o las VNet en las que no se implementó ninguna instancia de PCG. Haga clic para seleccionar una VPC o una VNet de tránsito a las que desea establecer un vínculo.

- **Implementar puerta de enlace de NSX Cloud:** esta opción solo está disponible para las VPC o las VNet en las que no se implementó ninguna instancia de PCG. Haga clic en esta opción para iniciar la implementación de PCG en esta VPC o VNet y que sea una VPC o VNet autoadministrada o de tránsito. Consulte **Implementar o vincular puertas de enlace de nube pública de NSX** en la *Guía de instalación de NSX-T Data Center* para obtener instrucciones detalladas.

Nubes > {Su nube pública} > Instancias

La sección Instancias muestra detalles de las instancias en la VPC o VNet.

Puede filtrar el inventario de instancias por cuenta, región, VPC o VNet.

Cada tarjeta representa una instancia (máquina virtual de carga de trabajo) y muestra un resumen.

Para obtener detalles sobre la instancia, haga clic en la tarjeta o cambie a la vista de cuadrícula.

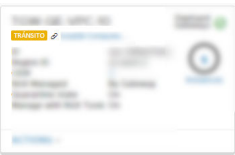

Puede agregar instancias a la lista blanca de CSM o eliminarlas. Consulte [Incluir máquinas virtuales en la lista blanca](#) para obtener información detallada.

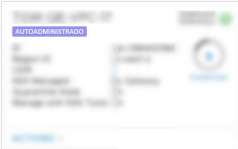
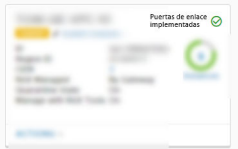
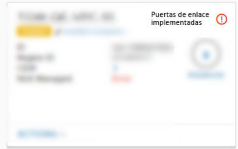
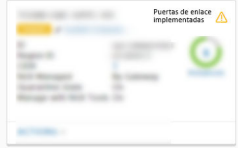
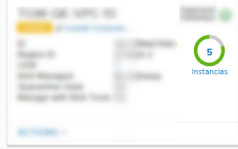
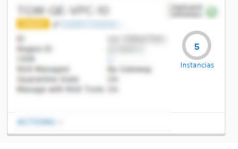
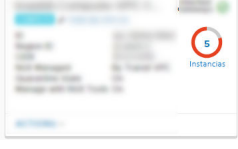
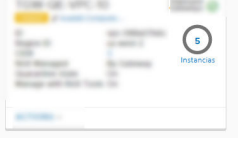
Iconos de CSM



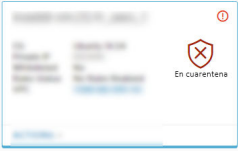
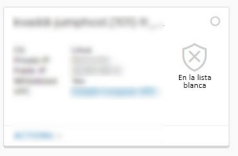
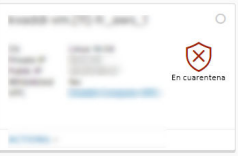
CSM muestra el estado de las construcciones de nube pública mediante iconos descriptivos.

Nota En Modo forzado de nube nativa: la directiva de cuarentena siempre está habilitada y todas las máquinas virtuales siempre están administradas por NSX. En este modo, solo se aplican los estados en los que la directiva de cuarentena está habilitada para las máquinas virtuales administradas por NSX.

En Modo forzado de NSX : la directiva de cuarentena se puede deshabilitar y es posible tener máquinas virtuales sin administrar en VPC/VNet. Todos los estados relevantes se aplican a este modo.

Sección e icono de CSM	Descripción
VPC/VNet	
	VPC o VNet de tránsito
	VPC o VNet de equipo

Sección e icono de CSM	Descripción
	VPC/VNet autoadministrada
	VPC/VNet que muestra instancias de PCG en estado correcto
	VPC/VNet que muestra instancias de PCG en estado de error
	VPC/VNet que muestra una instancia de PCG en estado de error y otra en estado correcto.
	VPC/VNet que muestra máquinas virtuales administradas por NSX.
	VPC/VNet que muestra máquinas virtuales sin administrar.
	VPC/VNet que muestra las máquinas virtuales con errores.
	VPC/VNet que muestra máquinas virtuales apagadas.
Instancias	

Sección e icono de CSM	Descripción
	Máquinas virtuales administradas por NSX sin errores.
	Las máquinas virtuales administradas por NSX con errores y la directiva de cuarentena están deshabilitadas.
	Las máquinas virtuales administradas por NSX con errores y la directiva de cuarentena están habilitadas.
	Máquinas virtuales no administradas en la lista blanca.
	Máquinas virtuales no administradas en cuarentena.

Sistema

Estas son las secciones en **Sistema**:

Sistema > Configuración

Estas opciones se configuran por primera vez al instalar CSM. Puede editarlas a partir de ese momento.

Unirse a CSM con NSX Manager

Debe conectar el dispositivo CSM con NSX Manager para permitir que estos componentes se comuniquen entre sí.

Requisitos previos

- NSX Manager debe estar instalado y debe tener el nombre de usuario y la contraseña de la cuenta de administrador para iniciar sesión en NSX Manager.
- CSM debe estar instalado y debe tener la función Administrador empresarial asignada en CSM.

Procedimiento

- 1 En un explorador, inicie sesión en CSM.
- 2 Cuando se le solicite en el Asistente de instalación, haga clic en **Iniciar instalación**.
- 3 Introduzca los siguientes detalles en la pantalla de credenciales de NSX Manager:

Opción	Descripción
Nombre de host de NSX Manager	Introduzca el nombre de dominio totalmente cualificado (FQDN) de NSX Manager, si está disponible. También puede introducir la dirección IP de NSX Manager.
Credenciales administrativas	Introduzca el nombre de usuario administrador empresarial y la contraseña de NSX Manager.
Huella digital del administrador	Si lo desea, introduzca el valor de huella digital de NSX Manager. Si deja este campo en blanco, el sistema identificará la huella digital y la mostrará en la pantalla siguiente.

- 4 (opcional) Si no se ha proporcionado un valor de huella digital para NSX Manager, o si el valor no es correcto, aparecerá la pantalla **Verificar huella digital**. Marque la casilla de verificación para aceptar la huella digital detectada por el sistema.
- 5 Haga clic en **Conectar (Connect)**.

Nota Si esta opción no aparece en el Asistente de configuración, o si desea cambiar la instancia de NSX Manager asociada, inicie sesión en CSM, haga clic en **Sistema > Configuración**, y luego haga clic en **Configurar** en el panel titulado **Nodo de NSX asociado**.

CSM verifica la huella digital de NSX Manager y establece la conexión.

- 6 (opcional) Configure el servidor proxy. Consulte las instrucciones en [\(Opcional\) Configurar servidores proxy](#).

(Opcional) Configurar servidores proxy

Si quiere enrutar y supervisar todo el tráfico de HTTP/HTTPS asociado a Internet a través de un servidor proxy HTTP confiable, puede configurar hasta cinco servidores proxy en CSM.

Todas las comunicaciones de nube pública desde PCG y CSM se enrutan a través del servidor proxy seleccionado.

La configuración de proxy de PCG es independientes de la configuración de proxy de CSM. Puede optar por no tener ningún servidor proxy o por tener otro distinto en PCG.

Se pueden elegir los siguientes niveles de autenticación:

- Autenticación basada en credenciales
- Autenticación basada en certificados para la interceptación de HTTPS
- Ninguna autenticación

Procedimiento

- 1 Haga clic en **Sistema > Configuración**. A continuación, haga clic en **Configurar** en el panel **Servidores proxy**.

Nota También puede proporcionar estos detalles cuando use el Asistente de instalación de CSM, que aparece cuando se instala por CSM primera vez.

- 2 Introduzca los siguientes detalles en la pantalla Configurar servidores proxy:

Opción	Descripción
Predeterminado	Utilice este botón de radio para indicar el servidor proxy predeterminado.
Nombre del perfil	Indique un nombre de perfil de servidor proxy. Esta opción es obligatoria.
Servidor proxy	Introduzca la dirección IP del servidor proxy. Esta opción es obligatoria.
Puerto	Introduzca el puerto del servidor proxy. Esta opción es obligatoria.
Autenticación	Opcional. Si desea configurar más autenticación, active esta casilla de verificación e indique un nombre de usuario y una contraseña válidos.
Nombre de usuario	Esta opción es obligatoria si se ha activado la casilla de verificación Autenticación.
Contraseña	Esta opción es obligatoria si se ha activado la casilla de verificación Autenticación.
Certificado	Opcional. Si quiere proporcionar un certificado de autenticación para la interceptación de HTTPS, active esta casilla de verificación y copie y pegue el certificado en el cuadro de texto que aparece.
Sin proxy	Seleccione esta opción si no quiere usar ninguno de los servidores proxy configurados.

Sistema > Utilidades

Las siguientes utilidades están disponibles.

Copia de seguridad y restauración

Siga las mismas instrucciones para hacer copias de seguridad y restaurar CSM, como lo haría para NSX Manager. Consulte [Restaurar y hacer copias de seguridad de NSX Manager](#) para obtener detalles.

Paquete de soporte

Haga clic en **Descargar** para recuperar el paquete de soporte de CSM. Esto se usa para la solución de problemas de r. Consulte la *Guía de solución de problemas de NSX-T Data Center* para obtener más información.

Sistema > Usuarios

Los usuarios se administran mediante el control de acceso basado en funciones (RBAC).

Consulte [Administrar las cuentas de usuarios y el control de acceso basado en funciones](#) para obtener detalles.

Detección de amenazas mediante la directiva de cuarentena de NSX Cloud

La función Directiva de cuarentena de NSX Cloud proporciona un mecanismo de detección de amenazas para las máquinas virtuales de carga de trabajo administradas por NSX.

La directiva de cuarentena se implementa de forma diferente en los dos modos de administración de máquinas virtuales.

Tabla 22-1. Implementación de la directiva de cuarentena en Modo forzado de NSX y en Modo forzado de nube nativa

Configuraciones relacionadas con la directiva de cuarentena	En Modo forzado de NSX	En Modo forzado de nube nativa
Estado predeterminado	Deshabilitado al implementar PCG con NSX Tools. Puede habilitarlo desde la pantalla de implementación de PCG o más tarde. Consulte Cómo habilitar o deshabilitar la directiva de cuarentena .	Siempre habilitado. No se puede deshabilitar.
Grupos de seguridad creados automáticamente exclusivos de cada modo	Todas las máquinas virtuales administradas por NSX que estén en buen estado se asignan al grupo de seguridad <code>vm-underlay-sg</code> .	Se crean grupos de seguridad de <code>nsx-<NSX GUID></code> y se aplican a las máquinas virtuales de carga de trabajo administradas por NSX que coinciden con una directiva de firewall distribuido en NSX Manager
Los grupos de seguridad de nube pública creados automáticamente son comunes para ambos modos:	<p>Los grupos de seguridad de gw se aplican a las interfaces de PCG correspondientes en AWS y Microsoft Azure.</p> <ul style="list-style-type: none"> ■ <code>gw-mgmt-sg</code> ■ <code>gw-uplink-sg</code> ■ <code>gw-vtep-sg</code> <p>Los grupos de seguridad de vm se aplican a las máquinas virtuales administradas por NSX en función de su estado actual y de si la directiva de cuarentena está habilitada o deshabilitada:</p> <ul style="list-style-type: none"> ■ <code>vm-quarantine-sg</code> en Microsoft Azure y <code>default</code> en AWS. <p>Nota En AWS, el grupo de seguridad de <code>default</code> ya existe. No lo crea NSX Cloud.</p>	

Recomendación general para Modo forzado de NSX :

Comenzar con *deshabilitado* para las implementaciones de tipo **Brownfield**: la directiva de cuarentena está deshabilitada de forma predeterminada. Cuando ya ha configurado máquinas virtuales en el entorno de nube pública, utilice el modo deshabilitado para la directiva de cuarentena hasta que integre sus máquinas virtuales de la carga de trabajo. Esto garantiza que las máquinas virtuales existentes no se ponen automáticamente en cuarentena.

Comenzar con *habilitado* para las implementaciones de tipo **Greenfield**: para las implementaciones de tipo greenfield, se recomienda habilitar la directiva de cuarentena para permitir que NSX Cloud administre la detección de amenazas de las máquinas virtuales.

Directiva de cuarentena en Modo forzado de NSX

Habilitar la directiva de cuarentena es opcional en Modo forzado de NSX .

Cómo habilitar o deshabilitar la directiva de cuarentena

En Modo forzado de NSX , puede elegir entre dos formas diferentes para habilitar la directiva de cuarentena.

La primera posibilidad para habilitar la directiva de cuarentena es implementar PCG en una VPC o VNet de tránsito o vincular una VPC o VNet de cómputo a una de tránsito. Mueva el control deslizante **Directiva de cuarentena en VPC/VNet asociada** del estado predeterminado **Deshabilitado** a **Habilitado**. Consulte **Implementar PCG** en la *Guía de instalación de NSX-T Data Center*.

También puede habilitar la directiva de cuarentena más adelante siguiendo los pasos que se indican a continuación.

Requisitos previos

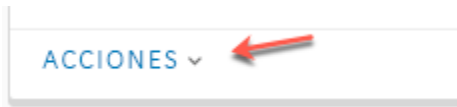
Si habilita la directiva de cuarentena después de implementar o vincularse a una PCG, debe tener una o varias VPC o VNet de de cómputo o de tránsito integradas en Modo forzado de NSX , es decir, que eligió utilizar NSX Tools para administrar sus máquinas virtuales de carga de trabajo.

Procedimiento

- 1 Inicie sesión en CSM y vaya a la nube pública:
 - a Si utiliza AWS, vaya a **Nubes > AWS > VPC**. Haga clic en la VPC de tránsito o de equipo.
 - b Si utiliza Microsoft Azure, vaya a **Nubes > Azure > VNets**. Haga clic en la VNet de tránsito o de equipo.

- 2 Habilite la opción mediante cualquiera de las siguientes acciones:

- En la vista de mosaico, haga clic en **ACCIONES > Editar configuración**.

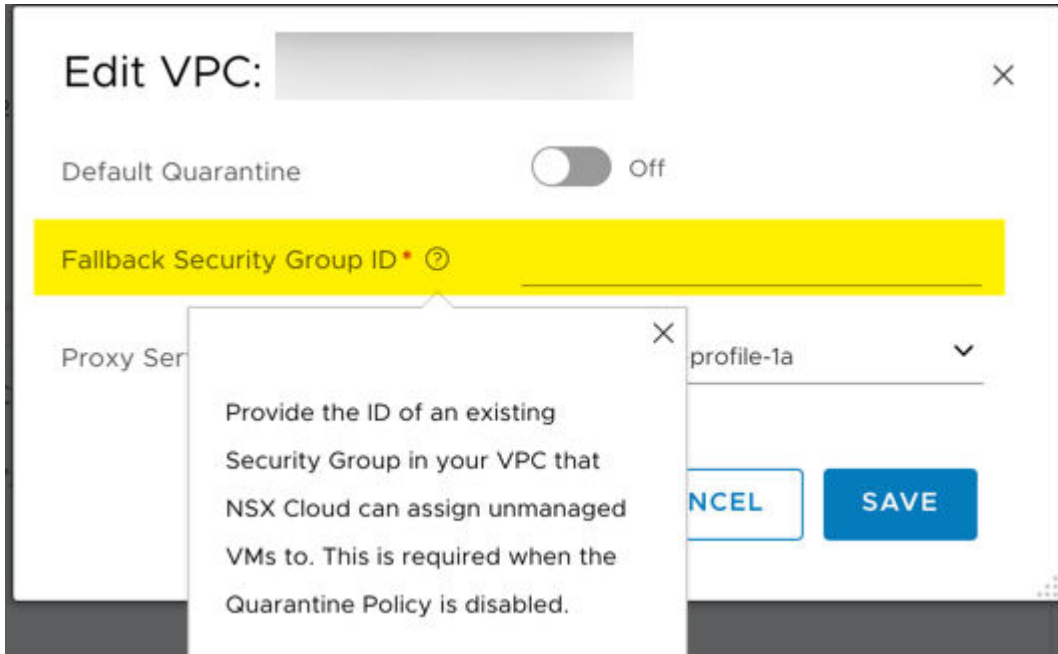


- Si se encuentra en la vista de cuadrícula, seleccione la casilla situada junto a la instancia de VPC o VNet y haga clic en **ACCIONES > Editar configuración**.
- ◆ Si se encuentra en la página de la instancia de VPC o VNet, haga clic en el icono **ACCIONES** para acceder a **Editar configuraciones**.



- 3 Active o desactive **Cuarentena predeterminada** para habilitarla o deshabilitarla.
- 4 Si desactiva la directiva de cuarentena, debe proporcionar un grupo de seguridad de reserva.

Nota El grupo de seguridad de reserva debe ser un grupo de seguridad existente definido por el usuario en la nube pública. No puede usar cualquier grupo de seguridad de NSX Cloud como grupo de seguridad de reserva.



- Todas las máquinas virtuales no administradas en esta VPC o VNet recibirán la asignación del grupo de seguridad de reserva cuando se deshabilite la directiva de cuarentena.
- Todas las máquinas virtuales administradas conservarán el grupo de seguridad asignado por NSX Cloud. La primera vez que esas máquinas virtuales se desetiqueten y dejen de estar administradas después de deshabilitar la directiva de cuarentena, también recibirán el grupo de seguridad de reserva que se les asignó.

- 5 Haga clic en **Guardar**.

Impacto de la directiva de cuarentena cuando se deshabilita

NSX Cloud no administra los grupos de seguridad de la nube pública de máquinas virtuales sin etiquetar cuando la directiva de cuarentena está deshabilitada.

Sin embargo, para las máquinas virtuales etiquetadas con `nsx.network=default` en la nube pública, NSX Cloud asigna los grupos de seguridad adecuados según el estado de la máquina virtual. Este comportamiento es similar a cuando la directiva de cuarentena está habilitada, pero las reglas de los grupos de seguridad de cuarentena (`vm-quarantine-sg` en Microsoft Azure y `default` en AWS) son menos restrictivas. Cualquier cambio manual realizado en los grupos de seguridad de máquinas virtuales etiquetadas se revertirá al grupo de seguridad asignado por NSX Cloud en un plazo de dos minutos.

Nota Si no desea que NSX Cloud asigne grupos de seguridad a las máquinas virtuales administradas por NSX (etiquetadas), agréguelas a la lista blanca de CSM. Consulte [Incluir máquinas virtuales en la lista blanca](#).

En la siguiente tabla se muestra cómo administra NSX Cloud los grupos de seguridad de la nube pública de máquinas virtuales de carga de trabajo cuando la directiva de cuarentena está deshabilitada.

Tabla 22-2. Asignación de NSX Cloud de grupos de seguridad de nube pública cuando la directiva de cuarentena está deshabilitada

¿La máquina virtual está etiquetada con <code>nsx.network=default</code> en la nube pública?	¿La máquina virtual está en la lista blanca?	Grupo de seguridad de nube pública de la máquina virtual cuando la directiva de cuarentena está deshabilitada y explicación
Etiquetada	No está en la lista blanca	<ul style="list-style-type: none"> ■ Si la máquina virtual no tiene amenazas: <code>vm-underlay-sg</code> ■ Si la máquina virtual tiene posibles amenazas (consulte la nota): <code>vm-quarantine-sg</code> en Microsoft Azure; <code>default</code> en AWS <p>Nota La asignación de grupos de seguridad de nube pública se activa durante los 90 segundos siguientes a la aplicación de la etiqueta <code>nsx.network=default</code> a las máquinas virtuales de la carga de trabajo. Debe instalar NSX Tools para que NSX administre las máquinas virtuales. Hasta que se instale NSX Tools, las máquinas virtuales de carga de trabajo etiquetadas se ponen en cuarentena.</p>
No etiquetada	No está en la lista blanca	Conserva el grupo de seguridad de nube pública existente porque NSX Cloud no realiza ninguna acción en las máquinas virtuales sin etiquetar.

Tabla 22-2. Asignación de NSX Cloud de grupos de seguridad de nube pública cuando la directiva de cuarentena está deshabilitada (continuación)

¿La máquina virtual está etiquetada con <i>nsx.network=default</i> en la nube pública?	¿La máquina virtual está en la lista blanca?	Grupo de seguridad de nube pública de la máquina virtual cuando la directiva de cuarentena está deshabilitada y explicación
Etiquetada	En la lista blanca	Conserva el grupo de seguridad de nube pública existente porque NSX Cloud no realiza ninguna acción en las máquinas virtuales incluidas en la lista blanca.
No etiquetada		

En la siguiente tabla se muestra cómo administra NSX Cloud los grupos de seguridad de nube pública de las máquinas virtuales si la directiva de cuarentena estaba habilitada antes, pero ahora está deshabilitada con un grupo de seguridad de reserva configurado para controlar las asignaciones de grupos de seguridad en esta VPC/VNet.

Tabla 22-3. Asignación de NSX Cloud de grupos de seguridad de nube pública cuando la directiva de cuarentena está deshabilitada, pero estaba habilitada primero

¿La máquina virtual está etiquetada con <i>nsx.network=default</i> en la nube pública?	¿La máquina virtual está en la lista blanca?	Grupo de seguridad de nube pública existente de la máquina virtual cuando la directiva de cuarentena está habilitada	Grupo de seguridad de nube pública de la máquina virtual después de deshabilitar la directiva de cuarentena y proporcionar un grupo de seguridad de reserva.
No etiquetada	No está en la lista blanca	vm-quarantine-sg (Microsoft Azure) o default (AWS)	A esta máquina virtual se le asigna el grupo de seguridad de reserva que proporcionó al deshabilitar la directiva de cuarentena porque no está etiquetado y no se considera que esté administrado por NSX, por lo que NSX Cloud revierte el grupo de seguridad al que asignó esta máquina virtual cuando se deshabilita la directiva de cuarentena.
Etiquetada	No está en la lista blanca	vm-underlay-sg o vm-quarantine-sg (Microsoft Azure) o default (AWS)	Conserva el grupo de seguridad asignado a NSX Cloud, ya que es coherente para las máquinas virtuales etiquetadas en los modos de cuarentena habilitado o deshabilitado.
Etiquetada	En la lista blanca	Cualquier grupo de seguridad de nube pública existente	Conserva el grupo de seguridad de nube pública existente porque NSX Cloud no realiza ninguna acción en las máquinas virtuales incluidas en la lista blanca.
No etiquetada			

Nota Si tiene una máquina virtual en la lista blanca en cualquiera de los grupos de seguridad asignados a NSX Cloud, deberá moverla manualmente al grupo de seguridad de reserva designado.

Impacto de la directiva de cuarentena cuando se habilita

NSX Cloud administra el grupo de seguridad de nube pública de todas las máquinas virtuales de carga de trabajo en esta VPC/VNet cuando la directiva de cuarentena está habilitada.

Cualquier cambio manual realizado en los grupos de seguridad se revertirá al grupo de seguridad asignado por NSX Cloud en un plazo de dos minutos. Si no desea que NSX Cloud asigne grupos de seguridad a las máquinas virtuales, agréguelas a la lista blanca en CSM. Consulte [Incluir máquinas virtuales en la lista blanca](#).

Nota Al quitar la máquina virtual de la lista blanca, esta se revierte al grupo de seguridad asignado por NSX Cloud.

Tabla 22-4. Asignación de NSX Cloud de grupos de seguridad de nube pública cuando la directiva de cuarentena está habilitada

¿La máquina virtual está etiquetada con <i>nsx.network=default</i> en la nube pública?	¿La máquina virtual está en la lista blanca?	Grupo de seguridad de nube pública de la máquina virtual cuando la directiva de cuarentena está habilitada y explicación
Etiquetada	No está en la lista blanca	<ul style="list-style-type: none"> ■ Si la máquina virtual no tiene amenazas: <i>vm-underlay-sg</i> ■ Si la máquina virtual tiene posibles amenazas (consulte la nota): <i>vm-quarantine-sg</i> en Microsoft Azure; <i>default</i> en AWS <p>Nota La asignación de grupos de seguridad de nube pública se activa durante los 90 segundos siguientes a la aplicación de la etiqueta <i>nsx.network=default</i> a las máquinas virtuales de la carga de trabajo. Debe instalar NSX Tools para que NSX administre las máquinas virtuales. Hasta que se instale NSX Tools, las máquinas virtuales de carga de trabajo etiquetadas se ponen en cuarentena.</p>
No etiquetada	No está en la lista blanca	<i>vm-quarantine-sg</i> en Microsoft Azure; <i>default</i> en AWS. Las máquinas virtuales sin etiquetar se consideran no administradas y, por lo tanto, NSX Cloud las pone en cuarentena.

Tabla 22-4. Asignación de NSX Cloud de grupos de seguridad de nube pública cuando la directiva de cuarentena está habilitada (continuación)

¿La máquina virtual está etiquetada con <i>nsx.network=default</i> en la nube pública?	¿La máquina virtual está en la lista blanca?	Grupo de seguridad de nube pública de la máquina virtual cuando la directiva de cuarentena está habilitada y explicación
Etiquetada	En la lista blanca	Conserva el grupo de seguridad de nube pública existente porque NSX Cloud no realiza ninguna acción en las máquinas virtuales incluidas en la lista blanca.
No etiquetada		

En la tabla siguiente, se captura el impacto en las asignaciones de grupos de seguridad si la directiva de cuarentena se había deshabilitado primero y luego se habilitó:

Tabla 22-5. Asignación de NSX Cloud de grupos de seguridad de nube pública cuando la directiva de cuarentena está habilitada, pero estaba deshabilitada primero

¿La máquina virtual está etiquetada con <i>nsx.network=default</i> en la nube pública?	¿La máquina virtual está en la lista blanca?	Grupo de seguridad de nube pública existente de la máquina virtual cuando la directiva de cuarentena está deshabilitada	Grupo de seguridad de nube pública de la máquina virtual después de que la directiva de cuarentena habilita
No etiquetada	No está en la lista blanca	Cualquier grupo de seguridad de nube pública existente	vm-quarantine-sg (Microsoft Azure) o default (AWS)
Etiquetada	No está en la lista blanca	vm-underlay-sg o vm-quarantine-sg (Microsoft Azure) o default (AWS)	Conserva el grupo de seguridad asignado a NSX Cloud porque es coherente para las máquinas virtuales etiquetadas en los modos de cuarentena habilitado o deshabilitado.
Etiquetada	En la lista blanca	Cualquier grupo de seguridad de nube pública existente.	Conserva el grupo de seguridad de nube pública existente porque NSX Cloud no realiza ninguna acción en las máquinas virtuales incluidas en la lista blanca.
No etiquetada			

Directiva de cuarentena en Modo forzado de nube nativa

La directiva de cuarentena siempre está habilitada en Modo forzado de nube nativa.

Tabla 22-6. Asignación de grupos de seguridad de nube pública en Modo forzado de nube nativa

¿La máquina virtual forma parte de una directiva de seguridad de NSX-T válida?	¿La máquina virtual está en la lista blanca?	Descripción y grupo de seguridad de nube pública de la máquina virtual
Sí, la máquina virtual coincide con una directiva de seguridad de NSX-T válida	No está en la lista blanca	Grupo de seguridad de nube pública creado por NSX Cloud denominado como <code>nsx-{NSX-GUID}</code> , que es el grupo de seguridad de nube pública correspondiente para la directiva de seguridad de NSX-T.
No, la máquina virtual no tiene ninguna directiva de firewall de NSX-T válida	No está en la lista blanca	<p><code>vm-quarantine-sg</code> en Microsoft Azure o <code>default</code> en AWS porque este es el comportamiento de detección de amenazas de NSX Cloud. En Modo forzado de nube nativa, los grupos de seguridad creados por NSX Cloud (<code>vm-quarantine-sg</code> en Microsoft Azure o <code>default</code> en AWS) imitan la directiva de seguridad de nube pública predeterminada.</p> <p>Nota En CSM, la máquina virtual muestra un estado de error.</p>
Sí, la máquina virtual tiene una directiva de seguridad de NSX-T válida	En la lista blanca	Conserva el grupo de seguridad de nube pública existente porque NSX Cloud no realiza ninguna acción en las máquinas virtuales incluidas en la lista blanca.
No, la máquina virtual no tiene ninguna directiva de seguridad de NSX-T válida		

Incluir máquinas virtuales en la lista blanca

La lista blanca es una opción disponible en CSM para todas las máquinas virtuales de carga de trabajo en el inventario de nube pública.

La lista blanca funciona en ambos modos de administración de máquinas virtuales: Modo forzado de NSX y Modo forzado de nube nativa.

¿Por qué hay que incluir las máquinas virtuales en la lista blanca?

- En Modo forzado de NSX : Si tiene la directiva de cuarentena habilitada y necesita verificar cualquier directiva de DFW específica con aplicaciones existentes en la máquina virtual, incluya esa máquina virtual en la lista blanca antes de incorporarla con NSX Cloud.
- En Modo forzado de NSX o Modo forzado de nube nativa:
 - Si tiene máquinas virtuales con errores y desea acceder a ellas para resolver los errores, debe incluir estas máquinas virtuales en la lista blanca para poder sacarlas del estado de cuarentena y utilizar las herramientas de depuración según sea necesario.
 - Incluya en la lista blanca las máquinas virtuales de su inventario de nube pública que no desee que administre NSX-T, como el reenviador de DNS, el servidor proxy, etc.

Cómo agregar máquinas virtuales de la lista blanca o quitarlas de ella

Siga estas instrucciones para agregar máquinas virtuales a la lista blanca o quitarlas de ella.

Requisitos previos

Debe tener una o varias cuentas de nube pública agregadas a CSM.

Procedimiento

- 1 Inicie sesión en CSM usando una cuenta de administrador de organización y vaya a su cuenta de nube pública.
 - a Si utiliza AWS, vaya a **Nubes > AWS > VPC > Instancias**.
 - b Si utiliza Microsoft Azure, vaya a **Nubes > Azure > VNets > Instancias**.
- 2 Si está en el modo de mosaico, cámbielo al modo de cuadrícula haciendo clic en el selector de modo situado en la esquina derecha de la vista de instancias.
- 3 Seleccione las máquinas virtuales (instancias) que desee incluir en la lista blanca o quitar de la lista blanca.
- 4 Haga clic en **Acciones** y seleccione **Añadir a la lista blanca** o **Eliminar de la lista blanca**.
- 5 Vuelva a la pestaña Cuentas, seleccione el mosaico de la cuenta y haga clic en **Acciones > Volver a sincronizar una cuenta**.

Resultados

Cada máquina virtual agregada a la lista blanca permanece en el grupo de seguridad que se asignó antes de la lista blanca. Ahora puede aplicar cualquier grupo de seguridad a la máquina virtual según considere necesario. NSX Cloud ignorará las máquinas virtuales de la lista blanca independientemente del estado de la directiva de cuarentena.

Si quita una máquina virtual de la lista blanca en Modo forzado de nube nativa o quita una máquina virtual administrada por NSX de la lista blanca en Modo forzado de NSX , NSX Cloud iniciará la asignación de grupos de seguridad a esa máquina virtual en función de su estado.

Modo forzado de NSX

En Modo forzado de NSX , es decir, mediante NSX Tools, primero debe incorporar las máquinas virtuales etiquetándolas en la nube pública e instalando en ellas NSX Tools, antes de iniciar la administración de estas máquinas virtuales mediante NSX-T Data Center.

Sistemas operativos admitidos actualmente para máquinas virtuales de carga de trabajo

Se trata de la lista de sistemas operativos compatibles actualmente con NSX Cloud para las máquinas virtuales de carga de trabajo en Modo forzado de NSX .

Actualmente, se admiten los siguientes sistemas operativos:

Nota Consulte la sección de problemas conocidos de NSX Cloud en las *Notas de la versión de NSX-T Data Center* para conocer las excepciones. Para los sistemas operativos compatibles, se asume que utiliza las versiones de kernel de Linux estándar. No se admiten las imágenes de Marketplace de nube pública con kernels personalizados, como el kernel de Linux ascendente con orígenes modificados.

- Red Hat Enterprise Linux (RHEL) 7.2, 7.3, 7.4, 7.5, 7.6
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6

Nota No se admite el kernel RHEL Extended Update Support (EUS) en RHEL y CentOS.

Nota NSX Cloud admite únicamente imágenes del catálogo de CentOS cuyas versiones de distribución coincidan con las versiones de kernel secundarias previstas. Por ejemplo, se espera que las versiones de distribución y sus versiones de kernel correspondientes sean las siguientes:

Versión de RHEL	Versión del kernel
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

- Ubuntu 14.04, 16.04, 18.04
- Microsoft Windows Server 2016 - Versión basada en servicio, Experiencia de escritorio (1709, 1803, 1809)
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 versiones 1809, 1803, 1709 (solo se admite en Microsoft Azure en la versión NSX Cloud actual)

Incorporación de máquinas virtuales a Modo forzado de NSX

Consulte en este flujo de trabajo un resumen de los pasos necesarios para incorporar y administrar máquinas virtuales de carga de trabajo desde la nube pública en Modo forzado de NSX .

Tabla 22-7. Flujo de trabajo del día N para incorporar máquinas virtuales de carga de trabajo en NSX Cloud

Tarea	Instrucciones
<input type="checkbox"/> Etiquete las máquinas virtuales de carga de trabajo con el par clave-valor nsx.network=default .	Siga las instrucciones que se indican en la documentación de la nube pública para colocar las máquinas virtuales de carga de trabajo.
<input type="checkbox"/> Instale NSX Tools en sus máquinas virtuales de carga de trabajo de Linux y Windows.	Consulte Instalar NSX Tools
Nota Si la opción Instalar NSX Tools automáticamente está habilitada en CSM para las VNet de Microsoft Azure, NSX Tools se instalará automáticamente.	
<input type="checkbox"/> (Opcional) En CSM, quite de la lista blanca todas las máquinas virtuales que desee que administre NSX.	Consulte Cómo agregar máquinas virtuales de la lista blanca o quitarlas de ella .
Nota La lista blanca es un paso manual que se recomienda aplicar en el flujo de trabajo de 0 días nada más agregar el inventario de nube pública en CSM. No es necesario que quite las máquinas virtuales de la lista blanca si no agregó ninguna.	

Etiquetar máquinas virtuales en la nube pública

Aplique la etiqueta **nsx.network=default** a las máquinas virtuales que desea administrar con NSX-T Data Center.

Procedimiento

- 1 Inicie sesión en la cuenta de nube pública y vaya a la VPC o VNet donde quiere que NSX-T Data Center administre las máquinas virtuales de carga de trabajo.
- 2 Seleccione las máquinas virtuales que desea administrar con NSX-T Data Center.
- 3 Agregue los siguientes detalles de etiqueta en las máquinas virtuales y guarde los cambios.

```
Key: nsx.network
Value: default
```

Nota Aplique esta etiqueta en el nivel de máquina virtual.

Resultados

Es posible que ya haya incorporado las VPC/VNet en las que aplicó las etiquetas **nsx.network=default** a las máquinas virtuales de carga de trabajo. También puede incorporar estas VPC/VNet después de aplicar la etiqueta. La incorporación correcta de VPC/VNet hace que las máquinas virtuales de carga de trabajo se consideren administradas por NSX.

Pasos siguientes

Instale NSX Tools en estas máquinas virtuales. Consulte [Instalar NSX Tools](#).

Si utiliza Microsoft Azure, tiene la opción de instalar NSX Tools automáticamente en las máquinas virtuales etiquetadas. Consulte [Instalar NSX Tools automáticamente](#) para obtener detalles.

Instalar NSX Tools

Instalar NSX Tools en máquinas virtuales de carga de trabajo

Hay varias opciones disponibles para instalar NSX Tools:

- Descargue e instale NSX Tools en máquinas virtuales de carga de trabajo individuales. Las máquinas virtuales Linux y Windows tienen algunas variaciones.
- Utilice imágenes replicables con NSX Tools instalado en ellas mediante el método compatible de la nube pública (por ejemplo, crear una AMI en AWS o una imagen administrada en Microsoft Azure).
- Solo AWS: al iniciar las máquinas virtuales, introduzca el comando de instalación y la ubicación de descarga de NSX Tools en **Datos de usuario**.
- Solo Microsoft Azure: habilite la instalación automática de NSX Tools cuando implemente PCG en una VNet de Microsoft Azure o cuando vincule a una VNet de tránsito, o bien editando la configuración de una VNet de tránsito o de equipo.

Nota Si tiene máquinas virtuales de carga de trabajo en la lista blanca en las que desea instalar NSX Tools, asegúrese de que los siguientes puertos estén abiertos en los grupos de seguridad que haya asignado a dichas máquinas virtuales:

- UDP 6081 entrante: para paquetes de datos de superposición. Se debe permitir para la dirección IP de VTEP de la PCG (Activo/En espera) (interfaz de eth1).
 - TCP 5555 saliente: para paquetes de control. Se debe permitir para la dirección IP de administración de la PCG (Activo/En espera) (interfaz de eth0).
 - TCP 8080: para la instalación o actualización de la dirección IP de administración de la PCG.
 - TCP 80: para descargar cualquier dependencia de terceros durante la instalación de NSX Tools.
 - UDP 67 y 68: para paquetes DHCP.
 - UDP 53: para la resolución de DNS.
-

Instalar NSX Tools en máquinas virtuales Linux

Para instalar NSX Tools en máquinas virtuales de carga de trabajo Linux, siga estas instrucciones.

Consulte [Sistemas operativos admitidos actualmente para máquinas virtuales de carga de trabajo](#) para obtener una lista de distribuciones de Linux compatibles actualmente.

Nota Para verificar la suma de comprobación de este script, vaya a **Descargas de VMware > Controladores y herramientas > Scripts de NSX Cloud**.

Requisitos previos

Necesita los siguientes comandos para ejecutar el script de instalación de NSX Tools:

- **wget**
- **nslookup**
- **dmidecode**

Procedimiento

- 1 Inicie sesión en CSM y vaya a la nube pública:
 - a Si utiliza AWS, vaya a **Nubes > AWS > VPC**. Haga clic en una VPC de tránsito o de equipo.
 - b Si utiliza Microsoft Azure, vaya a **Nubes > Azure > VNets**. Haga clic en la instancia de VNet en la que una o un par de instancias de PCG están implementadas y en ejecución.

Nota: La VPC o VNet es el lugar donde hay una o un par de instancias de PCG implementadas y en ejecución. La VPC/VNet de equipo es aquella vinculada a una de tránsito, y puede usar las instancias de PCG implementadas allí.

- 2 En la sección **Descarga e instalación de NSX Tools** de la pantalla, tome nota de lo que aparece en **Ubicación de descarga** y **Comando de instalación en Linux**.

Nota Para las VNet, el sufijo DNS en el comando de instalación se genera de forma dinámica para que coincida con la configuración de DNS que se selecciona al implementar PCG. Para las VNet de tránsito, el parámetro `-dnsServer <dns-server-ip>` es opcional. Para las VNet de equipo, debe proporcionar la dirección IP del reenviador de DNS para completar este comando.

- 3 Inicie sesión en la máquina virtual de la carga de trabajo de Linux con privilegios de superusuario.
- 4 Utilice `wget` o una opción equivalente para descargar el script de instalación en la máquina virtual Linux desde la **ubicación de descarga** que anotó desde CSM. El script de instalación se descarga en el directorio donde se ejecuta el comando `wget`.

Nota Para verificar la suma de comprobación de este script, vaya a **Descargas de VMware > Controladores y herramientas > Scripts de NSX Cloud**.

- 5 Cambie permisos en el script de instalación para hacerlo ejecutable si es necesario y ejecútelo:

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

Nota: En Red Hat Enterprise Linux y sus derivados, no se admite SELinux. Para instalar NSX Tools, deshabilite SELinux.

- 6 Se pierde la conectividad con la máquina virtual de Linux después de que comience la instalación de NSX Tools. Mensajes como los siguientes aparecen en la pantalla:
`Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` Para completar el proceso de incorporación, vuelva a iniciar sesión en la máquina virtual.

Resultados

NSX Tools se instala en la máquina virtual de carga de trabajo.

Nota

- Una vez que NSX Tools se instale correctamente, el puerto 8888 aparece como abierto en la máquina virtual de carga de trabajo, pero está bloqueado para las máquinas virtuales en el modo de subordinación y solo debe utilizarse cuando sea necesario para la solución de problemas avanzada. Puede acceder a las máquinas virtuales de carga de trabajo a través del puerto 8888 mediante una jumphost si la jumphost también se encuentra en la misma VPC que las máquinas virtuales de carga de trabajo a las que desea acceder.
 - El script utiliza `eth0` como la interfaz predeterminada.
-

Pasos siguientes

Administrar máquinas virtuales en Modo forzado de NSX

Instalar NSX Tools en máquinas virtuales Windows

Siga estas instrucciones para instalar NSX Tools en máquinas virtuales de carga de trabajo Windows.

Consulte [Sistemas operativos admitidos actualmente para máquinas virtuales de carga de trabajo](#) para obtener una lista de las versiones de Microsoft Windows compatibles actualmente.

Nota Para verificar la suma de comprobación de este script, vaya a **Descargas de VMware > Controladores y herramientas > Scripts de NSX Cloud**.

Procedimiento

- 1 Inicie sesión en CSM y vaya a la nube pública:
 - a Si utiliza AWS, vaya a **Nubes > AWS > VPC**. Haga clic en una VPC de tránsito o de equipo.
 - b Si utiliza Microsoft Azure, vaya a **Nubes > Azure > VNet**s. Haga clic en la instancia de VNet en la que una o un par de instancias de PCG están implementadas y en ejecución.

Nota: La VPC o VNet es el lugar donde hay una o un par de instancias de PCG implementadas y en ejecución. La VPC/VNet de equipo es aquella vinculada a una de tránsito, y puede usar las instancias de PCG implementadas allí.

- En la sección **Descarga e instalación de NSX Tools** de la pantalla, tome nota de lo que aparece en **Ubicación de descarga** y **Comando de instalación** en **Windows**.

Nota Para las VNet, el sufijo DNS en el comando de instalación se genera de forma dinámica para que coincida con la configuración de DNS que se selecciona al implementar PCG. Para las VNet de tránsito, el parámetro `-dnsServer <dns-server-ip>` es opcional. Para las VNet de equipo, debe proporcionar la dirección IP del reenviador de DNS para completar este comando.

- Conéctese a la máquina virtual de carga de trabajo de Windows como administrador.
- Descargue el script de instalación en la máquina virtual de Windows desde la **ubicación de descarga** que anotó desde CSM. Puede utilizar cualquier explorador (por ejemplo, Internet Explorer) para descargar el script. Se descarga en el directorio de descargas predeterminado de su explorador; por ejemplo, *C:\Descargas*.

Nota Para verificar la suma de comprobación de este script, vaya a **Descargas de VMware > Controladores y herramientas > Scripts de NSX Cloud**.

Nota:

- Abra un símbolo del sistema de PowerShell y vaya al directorio que contiene el script descargado.
- Utilice el **comando de instalación** que tomó de CSM para ejecutar el script descargado.

Por ejemplo:

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

Nota El argumento de archivo necesita la ruta de acceso completa a menos que se encuentre en el mismo directorio o si el script de PowerShell ya está en la ruta de acceso. Por ejemplo, si descarga el script en *C:\Downloads* y no está actualmente en ese directorio, el script debe contener la ubicación: *powershell -file 'C:\Downloads\nsx_install.ps1' ...*

- El script se ejecuta y, cuando se haya completado, muestra un mensaje que indica si NSX Tools se instaló correctamente.

Nota El script considera la interfaz de red principal como el valor predeterminado.

Pasos siguientes

Administrar máquinas virtuales en Modo forzado de NSX

Generar imágenes replicables

Puede generar una AMI en AWS o una imagen administrada en Microsoft Azure de una máquina virtual con el agente NSX instalado.

Con esta función, puede iniciar varias máquinas virtuales con el agente configurado y en ejecución.

Hay dos formas en las que puede generar una imagen AMI/administrada (la "imagen" en el resto de este tema) de una máquina virtual con el agente NSX instalado:

- **Generar imagen con un agente NSX sin configurar:** puede generar una imagen de una máquina virtual que tiene el agente NSX instalado, pero no está configurado con la opción `-noStart`. Esta opción permite obtener e instalar el paquete del agente NSX, pero no se inician las instancias de NSX Services. Además, no se realizan configuraciones de NSX, como la generación de certificados.
- **Generar imagen después de eliminar configuraciones de agentes NSX existentes:** puede eliminar las configuraciones de una máquina virtual existente administrada por NSX y usarlas para generar una imagen.

Generación de AMI con un agente NSX sin configurar

Puede generar una AMI de una máquina virtual con el agente NSX instalado y sin configurar.

Para generar una imagen de una máquina virtual que tiene el agente NSX instalado mediante la opción `-noStart`, haga lo siguiente:

Procedimiento

- 1 Copie y pegue el comando de instalación del agente NSX desde CSM. Consulte las instrucciones en [Instalar NSX Tools](#)
 - a Edite el comando para Windows de la siguiente manera:

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <> -noStart true
```

- b Edite el comando para Linux de la siguiente manera:

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 Vaya a esta máquina virtual en la nube pública y cree una imagen.

Generación de una imagen después de eliminar las configuraciones existentes del agente NSX

Puede generar una imagen de una máquina virtual que tiene un agente NSX configurado.

Para eliminar las configuraciones de una máquina virtual existente administrada por NSX y usarlas para generar las imágenes, haga lo siguiente:

Procedimiento

- 1 Elimine las configuraciones del agente NSX desde una máquina virtual de Windows o Linux:
 - a Inicie sesión en la máquina virtual de carga de trabajo, preferiblemente mediante un host intermedio.
 - b Abra la CLI de NSX-T:

```
sudo nsxcli
```

- c Introduzca los siguientes comandos:

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

- 2 Ubique esta máquina virtual en la nube pública y crear una imagen.

Instalar NSX Tools automáticamente

Actualmente solo se admite para Microsoft Azure.

En Microsoft Azure, NSX Tools se instala automáticamente si se cumplen los siguientes criterios:

- Las extensiones de máquina virtual de Azure se instalan en las máquinas virtuales de la VNet agregada a NSX Cloud. Para obtener más información, consulte la [documentación de Microsoft Azure sobre extensiones de máquina virtual](#).
- El grupo de seguridad que se aplica a las máquinas virtuales de Microsoft Azure debe permitir el acceso para instalar NSX Tools. Si la directiva de cuarentena está habilitada, puede agregar a la lista blanca las máquinas virtuales de CSM antes de la instalación y quitarlas de la lista blanca posteriormente.
- Las máquinas virtuales etiquetadas con la clave `nsx.network` y el valor `default`.

Para habilitar esta función:

- 1 Desplácese hasta **Nubes > Azure > VNet**.
- 2 Seleccione la VNet en cuyas máquinas virtuales desea instalar CSM automáticamente.
- 3 Habilite la opción mediante cualquiera de las siguientes acciones:
 - En la vista de mosaico, haga clic en **ACCIONES > Editar configuración**.



- Si se encuentra en la vista de cuadrícula, active la casilla situada junto a la instancia de VNet y haga clic en **ACCIONES > Editar configuración**.



- Si se encuentra en la pestaña VNet, haga clic en el icono ACCIONES para acceder a **Editar**



- 4 Mueva el control deslizante que hay junto a **Instalar NSX Tools automáticamente** a la posición ACTIVADO.

Nota Si se produce un error en la instalación de NSX Tools, haga lo siguiente:

- 1 Inicie sesión en el portal de Microsoft Azure y vaya a la máquina virtual donde falló la instalación de NSX Tools.
- 2 Vaya a las extensiones de la máquina virtual y desinstale la extensión llamada `VMwareNsxAgentInstallCustomScriptExtension`.
- 3 Quite la etiqueta `nsx.network=default` de esta máquina virtual.
- 4 Vuelva a agregar la etiqueta `nsx.network=default` en esta máquina virtual.

En unos tres minutos, NSX Tools se instala en esta máquina virtual.

Instalar NSX Tools con datos de usuario en AWS

Cuando se inicia una nueva máquina virtual de carga de trabajo en una VPC de AWS, puede instalar NSX Tools proporcionando las instrucciones de descarga e instalación de NSX Tools en el campo Datos de usuario.

Copie las instrucciones de descarga e instalación de NSX Tools de CSM y pegue los datos del usuario cuando inicie una nueva máquina virtual de carga de trabajo.

Procedimiento

- 1 Inicie sesión en la consola de AWS y comience el proceso de inicio de una nueva máquina virtual de carga de trabajo.
- 2 En otra ventana del navegador, inicie sesión en CSM.
 - a Vaya a **Nubes > AWS > VPC**

Nota La VPC o VNet es el lugar donde hay una o un par de instancias de PCG implementadas y en ejecución. La VPC/VNet de equipo es aquella vinculada a una de tránsito, y puede usar las instancias de PCG implementadas allí.

- b Haga clic en una VPC de tránsito o de equipo.
 - c Desde la sección **Descarga e instalación de NSX Tools** de la pantalla, copie la **Ubicación de descarga** y el **Comando de instalación en Linux o Windows**, según el sistema operativo que utilice para la máquina virtual de carga de trabajo.
- 3 En AWS, en los pasos para iniciar una nueva instancia de máquina virtual de carga de trabajo, pegue la ubicación de descarga y el comando de instalación como **Texto** en la sección Detalles avanzados de Datos de usuario.

Resultados

La máquina virtual de carga de trabajo se inicia y NSX Tools se instala automáticamente en ella.

Desinstalar NSX Tools

Utilice estos comandos específicos del sistema operativo para desinstalar NSX Tools.

Desinstalar NSX Tools de una máquina virtual Windows

Nota Si desea ver otras opciones disponibles para el script de instalación, utilice `-help`.

- 1 Inicie sesión remota en la máquina virtual mediante RDP.
- 2 Ejecute el script de instalación con la opción de desinstalación:

```
\nsx_install.ps1 -operation uninstall
```

Desinstalar NSX Tools de una máquina virtual Linux

Nota Si desea ver otras opciones disponibles para el script de instalación, utilice `--help`.

- 1 Inicie sesión remota en la máquina virtual mediante SSH.
- 2 Ejecute el script de instalación con la opción de desinstalación:

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

Grupos de seguridad tras la incorporación en Modo forzado de NSX

Las siguientes configuraciones de los grupos de seguridad se realizan automáticamente:

Si la directiva de cuarentena está habilitada:

- Las máquinas virtuales en buen estado administradas por NSX se mueven a `vm-underlay-sg` en la nube pública.
- Las máquinas virtuales no administradas o las máquinas virtuales administradas por NSX con errores se mueven al grupo de seguridad de `default` en AWS y al grupo de seguridad de red `vm-quarantine-sg` en Microsoft Azure.
- Las máquinas virtuales incluidas en la lista blanca no se ven afectadas.

Si la directiva de cuarentena está deshabilitada:

- Las máquinas virtuales en buen estado administradas por NSX se mueven a `vm-underlay-sg` en la nube pública.
- Las máquinas virtuales administradas por NSX con errores se mueven al grupo de seguridad de `default` en AWS y al grupo de seguridad de red `vm-quarantine-sg` en Microsoft Azure.
- Las máquinas virtuales sin administrar e incluidas en la lista blanca no se verán afectadas.

Administrar máquinas virtuales en Modo forzado de NSX

Siga estos pasos para empezar a administrar máquinas virtuales integradas correctamente en Modo forzado de NSX .

Tabla 22-8. Flujo de trabajo de microsegmentación para las máquinas virtuales de carga de trabajo administradas por NSX en Modo forzado de NSX

Tarea	Instrucciones
<input type="checkbox"/> Para permitir el acceso de entrada a las máquinas virtuales de carga de trabajo, cree reglas de firewall distribuido (DFW) según sea necesario.	Consulte Estrategia de conectividad predeterminada para las máquinas virtuales de carga de trabajo administradas por NSX en Modo forzado de NSX .
<input type="checkbox"/> Agrupe sus máquinas virtuales de carga de trabajo con etiquetas de la nube pública o etiquetas de NSX-T Data Center, y configure la microsegmentación.	Consulte Configurar la microsegmentación de las máquinas virtuales de carga de trabajo en Modo forzado de NSX . Consulte también: Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública

Estrategia de conectividad predeterminada para las máquinas virtuales de carga de trabajo administradas por NSX en Modo forzado de NSX

Cuando implementa la PCG en la VPC o la VNet de tránsito, o bien cuando vincula una VPC o una VNet de equipo a una de tránsito, NSX Cloud crea unas directivas de seguridad y unas reglas de DFW predeterminadas para las máquinas virtuales de carga de trabajo administradas por NSX.

Las dos reglas sin estado son para acceso DHCP y no afectan el acceso a las máquinas virtuales de carga de trabajo.

Las dos reglas con estado son las siguientes:

Las reglas de DFW que NSX Cloud crea según la directiva: <code>cloud-stateful-cloud-<VPC/VNet ID></code>	Propiedades
<code>cloud-<VPC/VNet ID>-managed</code>	Permite acceder a las máquinas virtuales dentro de la misma VPC o la misma VNet.
<code>cloud-<VPC/VNet ID>-inbound</code>	Bloquea el acceso a máquinas virtuales administradas por NSX desde cualquier lugar fuera de la VPC o VNet.

Nota No edite ninguna de las reglas predeterminadas.

Puede crear una copia de la regla entrante existente, ajustar los orígenes y destinos, y establecer el valor en **Permitir**. Coloque la regla **Permitir** por encima de la regla **Rechazar** predeterminada. También puede agregar nuevas directivas y reglas. Consulte [Agregar un firewall distribuido](#) para obtener instrucciones.

Configurar la microsegmentación de las máquinas virtuales de carga de trabajo en Modo forzado de NSX

Es posible configurar la microsegmentación para las máquinas virtuales de la carga de trabajo administradas.

Siga estos pasos para aplicar reglas de firewall distribuido a las máquinas virtuales de carga de trabajo administradas por NSX:

- 1 Cree grupos con nombres de máquina virtual, etiquetas u otros criterios de pertenencia; por ejemplo, niveles **web**, **app** o **DB**. Para obtener instrucciones, consulte [Agregar un grupo](#).

Nota Puede utilizar cualquiera de las siguientes etiquetas para los criterios de pertenencia. Consulte [Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública](#) para obtener detalles.

- etiquetas definidas por el sistema
 - etiquetas de la VPC o VNet que son detectadas por NSX Cloud
 - o sus propias etiquetas personalizadas
-

Nota Las reglas de DFW dependen de las etiquetas asignadas a las máquinas virtuales. Dado que cualquiera con los permisos de nube pública adecuados puede modificar estas etiquetas, NSX-T Data Center asume que se puede confiar en dichos usuarios y que la responsabilidad de garantizar y auditar que las máquinas virtuales estén etiquetadas correctamente en todo momento recae en el administrador de red de la nube pública.

- 2 Cree una regla y una directiva de firewall distribuido de este a oeste, y aplíquelas al grupo que creó. Consulte [Agregar un firewall distribuido](#).

Esta microsegmentación surte efecto cuando el inventario se resincroniza de forma manual desde CSM o, en aproximadamente tres minutos, cuando se extraen los cambios en CSM desde la nube pública.

Modo forzado de nube nativa

En Modo forzado de nube nativa, todas las máquinas virtuales de carga de trabajo están administradas automáticamente por NSX. Siga el flujo de trabajo descrito aquí para empezar a administrar estas máquinas virtuales con NSX-T Data Center.

Nota Todos los sistemas operativos son compatibles con las máquinas virtuales de carga de trabajo en Modo forzado de nube nativa.

Administrar máquinas virtuales en Modo forzado de nube nativa

En Modo forzado de nube nativa, NSX Cloud utiliza grupos y reglas de firewall distribuido de NSX-T Data Center para crear grupos de seguridad de aplicaciones y de red en Microsoft Azure y grupos de seguridad en AWS.

Todas las máquinas virtuales de carga de trabajo de las VPC/Vnet integradas en Modo forzado de nube nativa están administradas por NSX.

Siga este flujo de trabajo:

Tabla 22-9. Flujo de trabajo de microsegmentación para las máquinas virtuales de carga de trabajo en Modo forzado de nube nativa

Tarea	Instrucciones
<input type="checkbox"/> Cree uno o varios grupos en NSX Manager para incluir las máquinas virtuales de carga de trabajo de nube pública.	<p>Consulte Configurar la microsegmentación de las máquinas virtuales de carga de trabajo en Modo forzado de nube nativa</p> <p>Consulte también: Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública</p>
<input type="checkbox"/> Cree una o varias directivas de seguridad en NSX Manager que se apliquen a los grupos que creó para las máquinas virtuales de carga de trabajo de nube pública.	
<input type="checkbox"/> Quite las máquinas virtuales de carga de trabajo de la lista blanca de CSM si desea administrarlas con las directivas de seguridad de NSX-T.	
<input type="checkbox"/> Resincronice su cuenta de nube pública en CSM.	
<input type="checkbox"/> En su VPC/VNet, cambie a la vista de detalles en CSM para solucionar problemas de directivas de seguridad en caso de que haya algún error.	Consulte Limitaciones actuales y errores comunes

Configurar la microsegmentación de las máquinas virtuales de carga de trabajo en Modo forzado de nube nativa

Consulte este flujo de trabajo para configurar la directiva de seguridad en NSX Manager para las máquinas virtuales de carga de trabajo en Modo forzado de nube nativa, es decir, sin instalar NSX Tools en las máquinas virtuales de carga de trabajo.

Requisitos previos

Debe tener una VPC o VNet de proceso o de equipo en Modo forzado de nube nativa.

Procedimiento

- 1 En NSX Manager, edite o cree grupos para las máquinas virtuales de carga de trabajo. Por ejemplo, los nombres de máquinas virtuales que comienzan por web, app, db pueden ser tres grupos distintos. Consulte instrucciones en [Agregar un grupo](#). Consulte también [Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública](#) para obtener información sobre el uso de etiquetas de nube pública para crear grupos con las máquinas virtuales de carga de trabajo.

Las máquinas virtuales de carga de trabajo que coinciden con los criterios se agregan al grupo. Las máquinas virtuales que no coinciden con ningún criterio de agrupamiento se colocan en el grupo de seguridad de `default` en AWS y en el grupo de seguridad de red `vm-quarantine-sg` en Microsoft Azure.

Nota No puede usar los grupos creados automáticamente por NSX Cloud.

Nota Las reglas de DFW dependen de las etiquetas asignadas a las máquinas virtuales. Dado que cualquiera con los permisos de nube pública adecuados puede modificar estas etiquetas, NSX-T Data Center asume que se puede confiar en dichos usuarios y que la responsabilidad de garantizar y auditar que las máquinas virtuales estén etiquetadas correctamente en todo momento recae en el administrador de red de la nube pública.

- 2 En NSX Manager, cree reglas de firewall distribuido (DFW) con los grupos en los campos **Origen**, **Destino** o **Se aplica a**. Consulte instrucciones en [Agregar un firewall distribuido](#).

Nota Solo se admiten las directivas con estado para las máquinas virtuales de carga de trabajo de nube pública. Las directivas sin estado se pueden crear en NSX Manager, pero no coincidirán con ningún grupo que contenga máquinas virtuales de carga de trabajo de nube pública.

- 3 En CSM, quite de la lista blanca las máquinas virtuales que desea que administre NSX. Consulte instrucciones en [Cómo agregar máquinas virtuales de la lista blanca o quitarlas de ella](#).

Nota La lista blanca es un paso manual que se recomienda aplicar en el flujo de trabajo de 0 días nada más agregar el inventario de nube pública en CSM. Si no tiene ninguna máquina virtual en la lista blanca, no es necesario que las elimine.

- 4 Para los grupos y las reglas de DFW que encuentran una coincidencia en la nube pública, ocurrirá automáticamente lo siguiente:
 - a En AWS, NSX Cloud crea un nuevo grupo de seguridad denominado `nsx-<NSX_GUID>`.
 - b En Microsoft Azure, NSX Cloud crea un grupo de seguridad de aplicaciones (ASG) que se corresponde con el grupo creado en NSX Manager, así como un grupo de seguridad de red (NSG) correspondiente a las reglas de DFW que coinciden con las máquinas virtuales de carga de trabajo agrupadas.

Nota NSX Cloud sincroniza NSX Manager y las reglas de DFW y los grupos de nube pública cada 30 segundos.

- 5 Resincronice la cuenta de nube pública en CSM:
 - a Inicie sesión en CSM y vaya a su cuenta de nube pública.
 - b En su cuenta de nube pública, haga clic en **Acciones > Volver a sincronizar una cuenta**. Espere a que se complete la resincronización.
 - c Vaya a la VPC o VNet y haga clic en el indicador de error de color rojo. Accederá a la vista de instancias.
 - d Cambie la vista a Detalles si está en modo de cuadrícula y haga clic en **Error** en la columna Realización de reglas para ver errores, si hubiera alguno.

Pasos siguientes

Consulte [Limitaciones actuales y errores comunes](#).

Limitaciones actuales y errores comunes

Consulte estas limitaciones conocidas y errores comunes para solucionar problemas relacionados con la administración de las máquinas virtuales de carga de trabajo de nube pública en Modo forzado de nube nativa.

Nota La nube pública establece los siguientes límites:

- El número de grupos de seguridad que se pueden aplicar a una máquina virtual de carga de trabajo.
- El número de reglas que se pueden aplicar a una máquina virtual de carga de trabajo.
- El número de reglas que se pueden aplicar por grupo de seguridad.
- El ámbito de la asignación del grupo de seguridad. Por ejemplo, el ámbito del grupo de seguridad de red (NSG) en Microsoft Azure se limita a esa región, mientras que el ámbito del grupo de seguridad (SG) en AWS se limita a esa VPC.

Consulte la documentación de nube pública para obtener más información sobre estos límites.

Limitaciones actuales

La versión actual tiene las siguientes limitaciones de las reglas de DFW para las máquinas virtuales de carga de trabajo:

- No se admiten los grupos anidados.
- No se admiten los grupos que no tengan una dirección IP o una máquina virtual como miembro (por ejemplo, no se admiten los criterios de segmentos o puertos lógicos basados en puertos).
- No se admite el origen y el destino como dirección IP ni como grupo basado en CIDR.
- No se admite el origen y el destino con el valor "CUALQUIERA".
- El grupo **Applied_To** solo puede ser el origen o el destino, o bien los grupos de origen más destino. No se admiten otras opciones.
- Solo se admite la aplicación de reglas de VPC o VNet local. Puede crear grupos en NSX Manager que se expandan en VPC/VNet. Sin embargo, la aplicación de estas reglas solo funcionará en la VPC/VNet. No se aplican las reglas de DFW entre distintas VPC y VNet.
- Se admiten los protocolos TCP y UDP.

Nota Solo en AWS:

Las reglas de denegación creadas para las máquinas virtuales de carga de trabajo en las VPC de AWS no se aplican en AWS porque en AWS todo se incluye en la lista negra de forma predeterminada. Esto da lugar a los siguientes resultados en NSX-T Data Center:

- Si hay una regla de denegación entre VM1 y VM2, no se permite el tráfico entre VM1 y VM2 debido al comportamiento predeterminado de AWS, no debido a la regla de denegación. La regla de denegación no se aplicó en AWS.
- Suponiendo que se crearon las dos reglas siguientes en NSX Manager para las mismas máquinas virtuales, teniendo la regla 1 una prioridad más alta que la regla 2:
 - a VM1 to VM2 DENY SSH
 - b VM1 to VM2 Allow SSH

La regla de denegación se ignora porque no se aplicó en AWS y, por lo tanto, se aplicó la regla de permiso SSH. Esto es contrario a la expectativa, pero es una limitación debido al comportamiento predeterminado de AWS.

Errores comunes y su resolución

Error: No se aplicó ninguna directiva de NSX a la máquina virtual.

Si ve este error, no se aplicó ninguna de las reglas de DFW a la máquina virtual especificada. Edite la regla o el grupo en NSX Manager para incluir esta máquina virtual.

Error: Regla de NSX sin estado no admitida.

Si ve este error, significa que agregó reglas de DFW para máquinas virtuales de carga de trabajo de nube pública en una directiva de seguridad sin estado. Esto no está admitido. Cree una nueva o utilice una directiva de seguridad existente en el modo con estado.

Funciones de NSX-T Data Center admitidas por NSX Cloud

NSX Cloud crea una topología de red para la VPC o la VNet de nube pública mediante la generación de entidades de redes lógicas en NSX-T Data Center.

Utilice esta lista como referencia para conocer qué se genera automáticamente y cómo se deben utilizar las funciones de NSX-T Data Center tal como se aplican a la nube pública.

Configuraciones de NSX Manager

Consulte "Entidades lógicas de NSX-T creadas automáticamente" en la *Guía de instalación de NSX-T Data Center* para obtener más información sobre las entidades lógicas que se crean después de implementar un PCG correctamente.

Importante No modifique ni elimine ninguna de estas entidades creadas automáticamente.

Nota Si no puede acceder a algunas funciones en las máquinas virtuales de carga de trabajo de Windows, compruebe que la configuración del firewall de Windows se ha realizado correctamente.

Tabla 22-10.

Función de NSX-T Data Center	Detalles	Nota de NSX Cloud
Segmentos o conmutadores lógicos	Consulte Capítulo 4 Segmentos	Se crea un segmento para cada subred de nube pública a la que se asocia una máquina virtual administrada. Este es un segmento híbrido.
Puertas de enlace o enrutadores lógicos	Consulte Capítulo 2 Puertas de enlace de nivel 0 y Capítulo 3 Puerta de enlace de nivel 1 .	Cuando se implementa una PCG en una VPC o VNet de tránsito, NSX Cloud crea un enrutador lógico de nivel 0 automáticamente. Se crea un enrutador de nivel 1 para cada VPC o VNet de equipo cuando se vincula a una VPC o VNet de tránsito

Tabla 22-10. (continuación)

Función de NSX-T Data Center	Detalles	Nota de NSX Cloud
IPFIX	Consulte Configurar IPFIX .	<ul style="list-style-type: none"> ■ IPFIX se admite en NSX Cloud solo en el puerto UDP 4739. ■ Conmutador e IPFIX de DFW: si el recopilador se encuentra en la misma subred que la máquina virtual de Windows donde se aplicó el perfil de IPFIX, se requiere una entrada de ARP estática para el recopilador en la máquina virtual de Windows, ya que Windows descarta silenciosamente los paquetes UDP cuando no se encuentra ninguna entrada de ARP.
Reflejo del puerto	Consulte Supervisar las sesiones de creación de reflejo del puerto .	<p>En la versión actual, el reflejo del puerto solo se admite en AWS.</p> <ul style="list-style-type: none"> ■ Para NSX Cloud, configure el reflejo del puerto en Herramientas > Sesión de creación de reflejo de puerto. ■ Se admite solo el reflejo de puertos de L3SPAN. ■ El recopilador debe estar en la misma instancia de VPC que la máquina virtual de carga de trabajo de origen.
Firewall de puerta de enlace	Consulte Configurar un firewall de puerta de enlace .	Solo se admite en las puertas de enlace de nivel 0.

Agrupar las máquinas virtuales utilizando NSX-T Data Center y etiquetas de nube pública

NSX Cloud permite utilizar las etiquetas de nubes públicas asignadas a las máquinas virtuales de la carga de trabajo.

NSX Manager utiliza etiquetas para agrupar las máquinas virtuales, como las nubes públicas. Por lo tanto, para facilitar el agrupamiento de máquinas virtuales, NSX Cloud extrae en NSX Manager las etiquetas de nube pública aplicadas a las máquinas virtuales de carga de trabajo, siempre y cuando cumplan con el tamaño predefinido y los criterios de palabras reservadas.

Nota Las reglas de DFW dependen de las etiquetas asignadas a las máquinas virtuales. Dado que cualquiera con los permisos de nube pública adecuados puede modificar estas etiquetas, NSX-T Data Center asume que se puede confiar en dichos usuarios y que la responsabilidad de garantizar y auditar que las máquinas virtuales estén etiquetadas correctamente en todo momento recae en el administrador de red de la nube pública.

Terminología de etiquetas

Una **etiqueta** en NSX Manager hace referencia a lo que se conoce como **valor** en un contexto de nube pública. La **clave** de una etiqueta de nube pública se conoce como **ámbito** en NSX Manager.

Componentes de etiquetas en NSX Manager	Componentes equivalentes de etiquetas en la nube pública
Ámbito	Clave
Etiqueta	Valor

Tipos de etiquetas y limitaciones

NSX Cloud permite tres tipos de etiquetas para las máquinas virtuales de la nube pública administradas por NSX.

- **Etiquetas de sistema:** estas etiquetas están definidas por el sistema y no se pueden agregar, editar ni eliminar. NSX Cloud utiliza las siguientes etiquetas del sistema:
 - azure:subscription_id
 - azure:region
 - azure:vm_rg
 - azure:vnet_name
 - azure:vnet_rg
 - azure:transit_vnet_name
 - azure:transit_vnet_rg
 - aws:account
 - aws:availabilityzone
 - aws:region
 - aws:vpc
 - aws:subnet
 - aws:transit_vpc
- **Etiquetas detectadas:** las etiquetas que se hayan agregado a las máquinas virtuales en la nube pública son detectadas por NSX Cloud automáticamente y se muestran para las máquinas virtuales de la carga de trabajo en el inventario de NSX Manager. Estas etiquetas no se pueden modificar desde NSX Manager. No hay ningún límite para el número de etiquetas detectadas. Las etiquetas con el prefijo `dis:azure:` indican que se las detecta desde Microsoft Azure y las etiquetas con el prefijo `dis:aws` indican que se las detecta desde AWS.

Cuando realiza cambios en las etiquetas en la nube pública, los cambios se reflejan en NSX Manager en tres minutos.

Esta característica está habilitada de forma predeterminada. Puede habilitar o deshabilitar la detección de las etiquetas de Microsoft Azure o AWS en el momento de agregar la cuenta de AWS o la suscripción a Microsoft Azure.

- **Etiquetas de usuario:** puede crear hasta 25 etiquetas de usuario. Tiene privilegios para agregar, editar y eliminar las etiquetas de usuario. Para obtener más información acerca de cómo administrar etiquetas de usuario, consulte [Administrar las etiquetas de una máquina virtual](#).

Tabla 22-11. Resumen de los tipos de etiquetas y limitaciones

Tipo de etiqueta	Ámbito de etiqueta o prefijo predeterminado	Limitaciones	Administrador empresarial Privilegios	Auditor Privilegios
Definida por el sistema	Etiquetas del sistema completas: <ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availability zone 	<p>Ámbito (clave): 20 caracteres</p> <p>Etiqueta (valor): 65 caracteres</p> <p>Máximo posible: 5</p>	Solo lectura	Solo lectura
Detectada	<p>Prefijo de etiquetas de Microsoft Azure que se importan desde su VNet:</p> <p>dis:azure:</p> <p>Prefijo de las etiquetas de AWS que se importaron desde la VPC:</p> <p>dis:aws:</p>	<p>Ámbito (clave): 20 caracteres</p> <p>Etiqueta (valor): 65 caracteres</p> <p>Máximo permitido: sin límite</p> <hr/> <p>Nota Los límites de caracteres excluye el prefijo dis:<nombre de nube pública>. Las etiquetas que superen estos límites no se reflejan en NSX Manager.</p> <hr/> <p>Se omiten las etiquetas con el prefijo nsx.</p>	Solo lectura	Solo lectura
Usuario	<p>Las etiquetas de usuario pueden tener cualquier ámbito (clave) y valor en el número permitido de caracteres, excepto:</p> <ul style="list-style-type: none"> ■ el prefijo de ámbito (clave) dis:azure: o dis:aws: 	<p>Ámbito (clave): 30 caracteres</p> <p>Etiqueta (valor): 65 caracteres</p> <p>Máximo permitido: 25</p>	Agregar/editar/eliminar	Solo lectura

Tabla 22-11. Resumen de los tipos de etiquetas y limitaciones (continuación)

Tipo de etiqueta	Ámbito de etiqueta o prefijo predeterminado	Limitaciones	Administrador empresarial Privilegios	Auditor Privilegios
	■ el mismo ámbito (clave) que las etiquetas del sistema			

Ejemplos de etiquetas detectadas

Nota Las etiquetas están en el formato **clave=valor** para la nube pública y **ámbito=etiqueta** en NSX Manager.

Tabla 22-12.

Etiqueta de nube pública para la máquina virtual de carga de trabajo	¿Detectada por NSX Cloud?	Etiqueta de NSX Manager equivalente para la VM de la carga de trabajo
Name=Developer	Sí	dis:azure:Name=Developer
ValidDisTagKeyLength=ValidDisTagValue	Sí	dis:azure:ValidDisTagKeyLength=ValidDisTagValue
Abcdefghijklmnopqrstuvwxyz=value2	No (la clave supera los 20 caracteres)	ninguna
tag3=AbcdefghijklmnopqrstuvwxyzAb2369Ohgjjuytreswqacvbcdefghijklmnopqrstuvwxyz	No (el valor supera 65 caracteres)	ninguna
nsx.name=Tester	No (clave con el prefijo nsx)	ninguna

Cómo utilizar las etiquetas en NSX Manager

- Consulte [Administrar las etiquetas de una máquina virtual](#).
- Consulte [Buscar objetos](#).
- Consulte [Agregar un grupo](#).
- Consulte [Configurar la microsegmentación de las máquinas virtuales de carga de trabajo en Modo forzado de NSX](#).

Uso de los servicios nativos de la nube

Los siguientes servicios nativos de la nube se pueden usar con las máquinas virtuales de carga de trabajo de nube pública en NSX Manager.

Cuando se implementa PCG, se crea un grupo en NSX Manager para cada servicio de nube nativa compatible.

Se crean los siguientes grupos para los servicios de nube pública compatibles actualmente:

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

Para utilizar estos servicios nativos de nube, cree directivas de DFW que contengan el grupo de servicios de nube nativa en los campos de origen o destino de la regla según sea necesario.

Las reglas de DFW se aplican en las máquinas virtuales que no están en los servicios nativos de la nube.

Nota En Modo forzado de NSX , es decir, al administrar las cargas de trabajo con NSX Tools, actualmente no se admiten los servicios nativos de nube de Microsoft Azure.

Limitaciones actuales

ENDPOINT			Regla de DFW con servicio como DESTINO		Regla de DFW con servicio como ORIGEN	
Nube pública	Servicio	Ámbito	¿Se aplica en la máquina virtual?	¿Se aplica en el servicio?	¿Se aplica en el servicio?	¿Se aplica en la máquina virtual?
Microsoft Azure	Almacenamiento de BLOB	Global	Sí	No	No	Sí
	Base de datos Cosmos					
	SQL					
	Equilibrador de carga					
AWS	S3	VPC local	Sí	No	No	Sí
	Base de datos de Dynamo					
	RDS					
	ELB					

Inserción de servicios para la nube pública

NSX Cloud admite el uso de servicios de terceros en la nube pública para las máquinas virtuales de carga de trabajo administradas por NSX.

Si desea utilizar la inserción de servicios para las máquinas virtuales de carga de trabajo de la nube pública, debe alojar el dispositivo de servicio en la nube pública y no en NSX-T Data Center. Se recomienda alojar el dispositivo de servicio en una VPC o VNet de tránsito.

Para poder habilitar la inserción de servicios, debe tener la instancia de PCG implementada en una VPC o VNet de tránsito.

A continuación se proporciona una descripción general de las configuraciones que se realizan por única vez con el fin de permitir la inserción de servicios para las máquinas virtuales de carga de trabajo administradas por NSX.

Tabla 22-13. Descripción general de las configuraciones requeridas en la inserción de servicios para máquinas virtuales de carga de trabajo administradas por NSX en la nube pública

¿Con qué frecuencia?	Tarea	Instrucciones
Una vez para la configuración inicial	Configure el dispositivo de servicio en la nube pública, preferiblemente en una VPC o VNet de tránsito (donde implementó la instancia de PCG).	Consulte las instrucciones específicas del dispositivo de servicio de terceros y la nube pública.
	Registre el servicio de terceros en NSX-T Data Center.	Consulte Crear la definición de servicio y el endpoint virtual correspondiente
	Cree un endpoint de instancia virtual del servicio mediante una dirección IP de servicio virtual (Virtual Service IP, VSIP) /32 que el dispositivo de servicio utilizará únicamente para la inserción de servicios. La VSIP no debe entrar en conflicto con el rango de CIDR de las VPC o las VNet. Esta VSIP se anuncia a través de BGP ante la instancia de PCG.	Consulte Crear la definición de servicio y el endpoint virtual correspondiente
	Cree un túnel VPN de IPSec entre el dispositivo de servicio y la instancia de PCG.	Consulte Configurar una sesión de VPN de IPSec

Tabla 22-13. Descripción general de las configuraciones requeridas en la inserción de servicios para máquinas virtuales de carga de trabajo administradas por NSX en la nube pública (continuación)

¿Con qué frecuencia?	Tarea	Instrucciones
	Configure BGP entre la PCG y el dispositivo de servicio, y anuncie la VSIP desde el dispositivo de servicio y la ruta predeterminada (0.0.0.0/0) desde la PCG.	Consulte Configurar BGP y la redistribución de rutas
	Nota En la versión actual, solo se admite la inserción de servicios para el tráfico de norte a sur.	
¿Cómo y cuándo se requiere?	Una vez finalizadas las configuraciones que se realizan por única vez, configure las reglas de redireccionamiento para volver a enrutar tráfico selectivo desde las máquinas virtuales de carga de trabajo administradas por NSX hacia la VSIP. Estas reglas se aplican al puerto de vínculo superior de la instancia de PCG.	Consulte Configurar las reglas de redireccionamiento .

Procedimiento

1 Crear la definición de servicio y el endpoint virtual correspondiente

Debe utilizar las API de NSX Manager para crear una definición de servicio y un endpoint virtual para el dispositivo de servicio en la nube pública.

2 Configurar una sesión de VPN de IPSec

Configure una sesión de VPN de IPSec entre PCG y el dispositivo de servicio.

3 Configurar BGP y la redistribución de rutas

Configure BGP entre PCG y el dispositivo de servicio a través del túnel VPN de IPSec.

4 Configurar las reglas de redireccionamiento

Es posible ajustar las reglas de redireccionamiento según los requisitos.

Crear la definición de servicio y el endpoint virtual correspondiente

Debe utilizar las API de NSX Manager para crear una definición de servicio y un endpoint virtual para el dispositivo de servicio en la nube pública.

Requisitos previos

Seleccione una dirección IP reservada /32 que se pueda utilizar como endpoint virtual para el dispositivo de servicio en la nube pública, por ejemplo, 100.100.100.100/32. Esto se conoce como IP virtual de servicio (Virtual Service IP, VSIP).

Nota Si implementó el dispositivo de servicio en un par de alta disponibilidad, no cree otra definición de servicio, pero utilice la misma VSIP cuando lo anuncie en PCG durante la configuración de BGP.

Procedimiento

- 1 Para crear una definición de servicio para el dispositivo de servicio, ejecute la siguiente llamada API con credenciales de NSX Manager para la autorización:

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

Ejemplo de solicitud:

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

Ejemplo de respuesta:

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
}
```

```

    "_protection": "REQUIRE_OVERRIDE",
    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 Para crear un endpoint virtual para el dispositivo de servicio, ejecute la siguiente llamada API con credenciales de NSX Manager para la autorización:

```

PATCH https://{NSX Manager-IP}/policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-
services/cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

Ejemplo de solicitud:

```

{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [
        "100.100.100.100"
      ],
      "prefix_length": 32
    }
  ],
  "service_names": [
    "Service_Appliance1"
  ]
}

```

Ejemplo de respuesta:

```

200 OK

```

Nota El valor de `display_name` en el paso 1 debe coincidir con el valor de `service_names` en el paso 2.

Pasos siguientes

[Configurar una sesión de VPN de IPSec](#)

Configurar una sesión de VPN de IPSec

Configure una sesión de VPN de IPSec entre PCG y el dispositivo de servicio.

Requisitos previos

- Se debe implementar una instancia de PCG o un par de HA de este en una VPC o una VNet de tránsito.
- Se debe configurar el dispositivo de servicio en la nube pública, preferiblemente en la VPC o la VNet de tránsito.

Procedimiento

- 1 Desplácese hasta **Redes > VPN**.
- 2 Agregue un **servicio VPN** de tipo IPSec y tenga en cuenta las siguientes opciones de configuración específicas para NSX Cloud. Consulte [Agregar un servicio de VPN de IPSec](#) para obtener otros detalles.

Opción	Descripción
Nombre	El nombre de este servicio VPN se utiliza para configurar el endpoint local y las sesiones de VPN de IPSec. Tome nota de esto.
Tipo de servicio	Confirme que este valor esté establecido en IPSec.
Puerta de enlace de nivel 0	Seleccione la puerta de enlace de nivel 0 creada automáticamente para la VPC o la VNet de tránsito. Su nombre contiene el identificador de VPC o VNet (por ejemplo, <code>c1oud-t0-vpc-6bcd2c13</code>).

- 3 Agregue un **endpoint local** para PCG. La dirección IP del endpoint local es el valor de la etiqueta `nsx:local_endpoint_ip` para la instancia de PCG implementada en la VPC o la VNet de tránsito. Inicie sesión en la VPC o la VNet de tránsito de este valor. Tenga en cuenta las siguientes opciones de configuración específicas para NSX Cloud y consulte [Agregar endpoints locales](#) para obtener otros detalles.

Opción	Descripción
Nombre	El nombre de endpoint local se utiliza para configurar las sesiones de VPN de IPSec. Tome nota de esto.
Servicio VPN	Seleccione el servicio VPN que agregó en el paso 2.
Dirección IP	Busque este valor. Para ello, inicie sesión en la consola de AWS o el portal de Microsoft Azure. Es el valor de la etiqueta <code>nsx:local_endpoint_ip</code> aplicada a la interfaz de vínculo superior de PCG.

- 4 Cree una **sesión de IPSec basada en rutas** entre PCG y el dispositivo de servicio en la nube pública (preferiblemente alojado en la VPC o la VNet de tránsito).

Opción	Descripción
Tipo	Confirme que este valor esté establecido en Basada en rutas .
Servicio VPN	Seleccione el servicio VPN que agregó en el paso 2.
Endpoint local	Seleccione el endpoint local que creó en el paso 3.
Dirección IP remota	Introduzca la dirección IP privada del dispositivo de servicio.
Nota Si es posible acceder al dispositivo de servicio mediante una dirección IP pública, asigne una dirección IP pública a la dirección IP de endpoint local (también conocida como IP secundaria) a la interfaz de vínculo superior de PCG.	

Opción	Descripción
Interfaz de túnel	<p>Esta subred debe coincidir con la subred del dispositivo de servicio para el túnel de VPN. Introduzca el valor de subred configurado en el dispositivo de servicio para el túnel de VPN o anote el valor introducido aquí y asegúrese de utilizar la misma subred al configurar el túnel de VPN en el dispositivo de servicio.</p> <p>Nota Configure BGP en esta interfaz de túnel. Consulte Configurar BGP y la redistribución de rutas.</p>
Identificador remoto	Introduzca la dirección IP privada de su dispositivo de servicio en la nube pública.
Perfil de IKE	La sesión de VPN de IPSec debe asociarse con un perfil de IKE. Si creó un perfil, selecciónelo en el menú desplegable. También puede utilizar el perfil predeterminado.

Pasos siguientes

[Configurar BGP y la redistribución de rutas](#)

Configurar BGP y la redistribución de rutas

Configure BGP entre PCG y el dispositivo de servicio a través del túnel VPN de IPSec.

Se configuran los vecinos BGP en la interfaz de túnel VPN de IPSec que estableció entre PCG y el dispositivo de servicio. Consulte [Configurar BGP](#) para obtener detalles.

Debe configurar BGP de forma similar en el dispositivo de servicio. Consulte la documentación específica de su servicio en la nube pública para obtener detalles.

A continuación, configure la redistribución de la siguiente manera:

- PCG anuncia su ruta predeterminada (0.0.0.0/0) al dispositivo de servicio.
- El dispositivo de servicio anuncia la VSIP a PCG. Se trata de la misma dirección IP que se utiliza al registrar el servicio. Consulte [Crear la definición de servicio y el endpoint virtual correspondiente](#).

Nota Si implementó el dispositivo de servicio en un par de alta disponibilidad, anuncie la misma VSIP desde ambos dispositivos de servicio.

Procedimiento

- 1 Desplácese hasta **Redes > Puertas de enlace de nivel 0**.
- 2 Seleccione la puerta de enlace de nivel 0 creada automáticamente para la VPC o la VNet de tránsito con un nombre como `cloud-t0-vpc-6bcd2c13` y haga clic en **Editar**.
- 3 Haga clic en el número o el icono junto a **Vecinos BGP** en la sección **BGP**.

4 Tenga en cuenta estas configuraciones:

Opción	Descripción
Dirección IP	Utilice la dirección IP configurada en la interfaz de túnel de dispositivo de servicio para la VPN entre PCG y el dispositivo de servicio.
Número de AS remoto	Este número debe coincidir con el número de AS del dispositivo de servicio en la nube pública.
Filtro de ruta	Establezca un filtro de salida para anunciar la ruta predeterminada (0.0.0.0/0) del PCG al dispositivo de servicio.

5 En la sección **Redistribución de rutas**, habilite las rutas estáticas en la puerta de enlace de nivel 0.

Establecer redistribución de rutas

Puerta de enlace de nivel 0 cloud-to-415... #Redistribución de rutas ⓘ

AGREGAR REDISTRIBUCIÓN DE RUTAS

Nombre	Redistribución de rutas	Mapa de ruta
<input type="text" value="Introducir nombre"/>	Establecer*	<input type="text" value="Seleccionar mapa de rutas"/>

Establecer redistribución de rutas ⓘ

Puerta de enlace de nivel 0 cloud-to-415... #Orígenes seleccionados ⓘ

Seleccionar orígenes a continuación

Subredes de nivel 0

☒ Rutas estáticas
 ☐ IP local de IPSec
 ☐ IP de TEP de EVPN
 ☐ Interfaces y segmentos conectados
 ☐ Subred de interfaz de servicio
 ☐ Subred de interfaz de bucle invertido

☐ IP de NAT
 ☐ IP del reenviador de DNS
 ☐ Subred de interfaz externa
 ☐ Segmento conectado

Pasos siguientes

[Configurar las reglas de redireccionamiento](#)

Configurar las reglas de redireccionamiento

Es posible ajustar las reglas de redireccionamiento según los requisitos.

Tras finalizar la configuración inicial, es posible crear y editar reglas de redireccionamiento según sea necesario para volver a enrutar distintos tipos de tráfico para las máquinas virtuales de carga de trabajo administradas por NSX mediante el dispositivo de servicio.

Requisitos previos

Es necesario completar la configuración de la inserción de servicios para poder crear reglas de redireccionamiento.

Procedimiento

- 1 Desplácese hasta **Seguridad > Firewall norte-sur > Introspección de red (N-S)**.
- 2 Haga clic en **Agregar directiva**.

Opción	Descripción
Nombre:	Proporcione un nombre descriptivo para la directiva, por ejemplo Inserción de servicios de norte a sur para máquinas virtuales de Azure .
Redireccionar a:	Seleccione el nombre del endpoint virtual que creó para este dispositivo de servicio al registrar el servicio. Consulte Crear la definición de servicio y el endpoint virtual correspondiente .
Se aplica a:	Seleccione la puerta de enlace de nivel 0 de la PCG.

- 3 Seleccione la nueva directiva y haga clic en **Agregar regla**. Tenga en cuenta los siguientes valores específicos de la inserción de servicios:

Opción	Descripción
Orígenes	Seleccione un grupo de subredes cuyo tráfico deba ser redirigido, por ejemplo, un grupo de máquinas virtuales de carga de trabajo administradas por NSX.
Destinos	Seleccione una lista de servicios o direcciones IP de destino, por ejemplo, Google , que desee enrutar a través del dispositivo de servicio.
Se aplica a	Seleccione el puerto de vínculo superior de las instancias de PCG activas y en espera.
Acción	Seleccione Redireccionar .

Habilitar NAT en máquinas virtuales administradas por NSX

NSX Cloud permite habilitar NAT en máquinas virtuales administradas por NSX.

Puede habilitar el tráfico de norte a sur en las máquinas virtuales administradas por NSX mediante etiquetas de nube pública.

En la máquina virtual administrada por NSX para la que desea habilitar NAT, aplique la siguiente etiqueta:

Tabla 22-14.

Clave	Valor
<code>nsx.publicip</code>	dirección IP pública de su nube pública , por ejemplo, 50.1.2.3

Nota La dirección IP pública que se proporciona aquí debe ser de libre uso y no debe estar asignada a una máquina virtual, incluida la máquina virtual de carga de trabajo para la que desea habilitar NAT. Si asigna una dirección IP pública que estaba previamente asociada con cualquier otra instancia o dirección IP privada, NAT no funcionará. En ese caso, anule la asignación de la dirección IP pública.

Después de aplicar esta etiqueta, la máquina virtual de carga de trabajo puede acceder a tráfico de Internet.

Habilitar el reenvío de syslog

NSX Cloud es compatible con el reenvío de syslog.

Puede habilitar el reenvío de syslog de paquetes de firewall distribuido (Distributed Firewall, DFW) en máquinas virtuales administradas. Consulte **Configurar registros remotos** en *Guía de solución de problemas de NSX-T Data Center* para obtener más detalles.

Haga lo siguiente:

Procedimiento

- 1 Inicie sesión en PCG mediante el host de accesos directos.
- 2 Escriba **nsxcli** para abrir la CLI de NSX-T Data Center.
- 3 Escriba los siguientes comandos para habilitar el reenvío de registros de DFW:

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <server-IP-address> proto udp level info
messageid FIREWALL-PKTLOG
```

Una vez establecido esto, los registros de paquetes de DFW de agente NSX están disponibles en `/var/log/syslog` en PCG.

- 4 Para habilitar el reenvío de registros por máquina virtual, introduzca el siguiente comando:

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

Configurar una VPN en el modo forzado de NSX

Puede configurar una VPN mediante PCG que aparezcan como puertas de enlace de nivel 0 creadas automáticamente en la implementación de NSX-T Data Center local. Estas instrucciones son específicas para las máquinas virtuales de carga de trabajo administradas en el modo NSX Enforced Mode.

Use las PCG de la misma manera que utiliza las puertas de enlace de nivel 0 en NSX Manager para configurar la VPN siguiendo los pasos adicionales que se describen aquí. Puede crear túneles VPN entre PCG implementados en la misma nube pública o en nubes públicas diferentes, o con una puerta de enlace o enrutador local. Consulte [Capítulo 5 Red privada virtual \(VPN\)](#) para obtener más información sobre la compatibilidad de las VPN con NSX-T Data Center.

Requisitos previos

- Compruebe que tiene una o un par de HA de PCG implementadas en una VPC/VNet.
- Compruebe que el elemento remoto del mismo nivel sea compatible con la VPN basada en rutas y BGP.

Procedimiento

- 1 En la nube pública, busque el endpoint local asignado por NSX para la PCG y asigne una dirección IP pública si es necesario:
 - a Vaya a la instancia de PCG en la nube pública y desplácese hasta Etiquetas.
 - b Anote la dirección IP en el campo de valor de la etiqueta `nsx.local_endpoint_ip`.
 - c (opcional) Si el túnel VPN requiere una dirección IP pública, por ejemplo, si desea configurar una VPN a otra nube pública o a la implementación local de NSX-T Data Center:
 - 1 Desplácese hasta la interfaz de vínculo superior de la instancia de PCG.
 - 2 Asocie una dirección IP pública a la dirección IP `nsx.local_endpoint_ip` que anotó en el paso **b**.
 - d (opcional) Si tiene un par de HA de instancias de PCG, repita los pasos **a** y **b** y asocie una dirección IP pública, si es necesario, como se describe en el paso **c**.

- 2 En NSX Manager, habilite la VPN de IPSec para la PCG que aparece como una puerta de enlace de nivel 0 con el nombre `cloud-t0-vpc/vnet-<vpc/vnet-id>` y cree sesiones de IPSec de base de ruta entre este endpoint de la puerta de enlace de nivel 0 y la dirección IP remota del mismo nivel de VPN que desee. Consulte [Agregar un servicio de VPN de IPSec](#) para obtener otros detalles.

- a Vaya a **Redes > VPN > Servicios de VPN > Agregar servicio > IPSec**. Proporcione los siguientes detalles:

Opción	Descripción
Nombre	Introduzca un nombre descriptivo para el servicio de VPN, por ejemplo VPN_AWS-<ID-VPC> o VPN_AZURE-<ID-VNet> .
Puerta de enlace de nivel 0/nivel 1	Seleccione la puerta de enlace de nivel 0 para la PCG en la nube pública.

- b Vaya a **Redes > VPN > Endpoints locales > Agregar endpoint local**. Proporcione la siguiente información y consulte [Agregar endpoints locales](#) para obtener más información:

Nota Si tiene un par de HA de instancias de PCG, cree un endpoint local para cada instancia utilizando la dirección IP del endpoint local correspondiente asociada a ella en la nube pública.

Opción	Descripción
Nombre	Introduzca un nombre descriptivo para el endpoint local, por ejemplo LE-preferido-PCG-<ID-VPC> o LE-preferido-PCG-<ID-VNET> .
Servicio VPN	Seleccione el servicio de VPN para la puerta de enlace de nivel 0 de la PCG que creó en el paso 2a.
Dirección IP	Introduzca el valor de la dirección IP del endpoint local de la PCG que anotó en el paso 1b.

- c Vaya a **Redes > VPN > Sesiones de IPSec > Agregar sesión de IPSec > Basada en rutas**. Proporcione la siguiente información y consulte [Agregar una sesión de IPSec basada en rutas](#) para obtener más información:

Nota Si va a crear un túnel VPN entre varias PCG implementadas en una VPC, y varias PCG implementadas en una VNet, deberá crear un túnel entre cada endpoint local de PCG en la VPC y la dirección IP remota de la PCG en la VNet, y, a la inversa, desde la PCG de la VNet hasta la dirección IP remota de PCG en la VPC. Deberá crear un túnel separado para la PCG activa y en espera. Esto dará como resultado una malla completa de sesiones de IPSec entre las dos nubes públicas.

Opción	Descripción
Nombre	Introduzca un nombre descriptivo para la sesión de IPsec, por ejemplo, PCG1-<ID-VPC>-a-edge-remoto .
Servicio VPN	Seleccione el servicio VPN que creó en el paso 2a.
Endpoint local	Seleccione el endpoint local que creó en el paso 2b.

Opción	Descripción
Dirección IP remota	<p>Introduzca la dirección IP pública del elemento remoto del mismo nivel con el que va a crear el túnel VPN.</p> <p>Nota La IP remota puede ser una dirección IP privada si se puede acceder direcciones IP privadas, por ejemplo, mediante DirectConnect o ExpressRoute.</p>
Interfaz de túnel	<p>Introduzca la interfaz de túnel en formato CIDR. Se debe utilizar la misma subred para que el elemento remoto del mismo nivel establezca la sesión de IPSec.</p>

vm NSX-T

Inicio Redes Seguridad Inventario Planificar y solucionar problemas Sistema

DIRECTIVA ADMINISTRADOR

Información general de l...

Topología de red

Conectividad

Puertas de enlace de niv...

Puertas de enlace de niv...

Segmentos

Servicios de red

VPN

NAT

Paso 2a.

SERVICIOS VPN

AGREGAR SERVICIO

CONTRAER TODO

Filtrar por nombre, ruta y más

Nombre	Tipo de servicio	Puerta de enlace de nivel 0/nivel 1	Sesiones	Estado
<VPC-ID>-AWS_VPN	IPSec	cloud-to-vpc-073617880a9622d93	1	Correcto
Descripción		VPN service on AWS Transit VPC ID vpc-073617880a9622d93	Estado de administración	Habilitado
Nivel de registro de IKE		Información	Etiquetas	0
Sincronización de sesión		Habilitado		

vm NSX-T

Inicio Redes Seguridad Inventario Planificar y solucionar problemas Sistema

DIRECTIVA ADMINISTRADOR

Información general de l...

Topología de red

Conectividad

Puertas de enlace de niv...

Puertas de enlace de niv...

Segmentos

Servicios de red

VPN

NAT

Paso 2b.

ENDPOINTS LOCALES

AGREGAR ENDPOINT LOCAL

CONTRAER TODO

Filtrar por nombre, ruta y más

Nombre	Servicio VPN	Dirección IP	Certificado del sitio	Sesiones	Estado
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	No establecido	1	Correcto
Descripción		No establecido	Identificador local	10.99.3.35	
Certificados de CA de confianza		No establecido	Lista de revocación de certificados	No establecido	
Etiquetas		0			

vm NSX-T

Inicio Redes Seguridad Inventario Planificar y solucionar problemas Sistema

DIRECTIVA ADMINISTRADOR

Información general de l...

Topología de red

Conectividad

Puertas de enlace de niv...

Puertas de enlace de niv...

Segmentos

Servicios de red

VPN

NAT

Equilibrio de carga

Directivas de reenvío

Paso 2c.

SESIONES DE IPSEC

AGREGAR SESIÓN DE IPSEC

CONTRAER TODO

admin

Nombre	Tipo	Servicio VPN	Endpoint local	Dirección IP remota	Estado	Alarmas
<VPC-ID>-PCG-to-remote_edge	Basada en rutas	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	Inactivo	0
Descripción		No establecido	Estado de administración	Habilitado	VER ESTADÍSTICAS	
Suite de cumplimiento		Ninguno	Interfaz de túnel	192.168.50.10/24	DESCARGAR CONFIGURACIÓN	
Modo de autenticación		PSK	Identificador remoto	172.0.3.145		
Clave precompartida					
> Propiedades avanzadas						

ACTUALIZAR

1-1 de 1 Servicios VPN

- 3 Configure los vecinos BGP en la interfaz de túnel VPN de IPsec que estableció en el paso 2. Consulte [Configurar BGP](#) para obtener detalles.
 - a Desplácese hasta **Redes > Puertas de enlace de nivel 0**.
 - b Seleccione la puerta de enlace de nivel 0 creada automáticamente para la que creó la sesión de IPsec y haga clic en **Editar**.
 - c Haga clic en el número o el icono junto a **Vecinos BGP** en la sección **BGP** y proporcione los siguientes detalles:

Opción	Descripción
Dirección IP	Utilice la dirección IP de la VTI remota configurada en la interfaz de túnel en la sesión de IPsec para el elemento del mismo nivel de VPN.
Número de AS remoto	Este número debe coincidir con el número de AS del elemento remoto del mismo nivel.

Puerta de enlace de nivel 0

[AGREGAR PUERTA DE ENLACE](#)
EXPANDIR TODO
Filtrar

	Nombre de la puerta de enlace de nivel 0	Modo HA	Puertas de enlace de nivel 1 vinculadas	Segmentos vinculados
▼	BGP			
	AS local	1000	iBGP de SR interno	● Activado
	BGP	● Activado	ECMP	● Activado
	Reinicio estable	Solo aplicación auxiliar	Multipath Relax	● Activado
	Temporizador de reinicio estable	180 segundos	Temporizador obsoleto de reinicio estable	600 segundos
	Agregación de rutas	0	Vecinos BGP	1

Paso 3.

Vecinos BGP

Puerta de enlace de nivel 0 cloud-t0-415... #Vecinos 1

	Dirección IP	BFD	Número de AS remoto
⋮ ▼	192.168.50.11	Deshabilitado	1000
Direcciones de origen		No establecido	
Límite máximo de saltos		1	

- 4 Anuncie los prefijos que desea utilizar para la VPN mediante el perfil de redistribución. En Modo forzado de NSX , conecte las rutas habilitadas de nivel 1 en el perfil de redistribución.

Puerta de enlace de nivel 0

AGREGAR PUERTA DE ENLACE EXPANDIR TODO Filtrar por nombre, n

	Nombre de la puerta de enlace de nivel 0	Modo HA	Puertas de enlace de nivel 1 vinculadas	Segmentos vinculados	Estado
>	BGP				
>	REDISTRIBUCIÓN DE RUTAS				
	Redistribución de rutas	2	Paso 4.	Estado de redistribución de rutas	● Activado
>	VRP TORvf	Active Directory	0	0	● Corre

Redistribución de rutas

Puerta de enlace de nivel 0 cloud-t0-vpc... #Origenes seleccionados 1

Subredes de nivel 0

Subredes de nivel 1 anunciadas

- Interfaces y segmentos conectados
- Subred de interfaz de servicio
- Segmento conectado

Preguntas frecuentes

En esta sección se incluyen algunas preguntas frecuentes.

¿Cómo puedo verificar que los componentes de NSX Cloud están instalados y en ejecución?

- 1 Para comprobar que NSX Tools en la máquina virtual de carga de trabajo esté conectado a PCG, haga lo siguiente:
 - a Escriba el comando `nsxcli` para abrir la CLI de NSX.
 - b Escriba el siguiente comando para obtener el estado de conexión de la puerta de enlace, por ejemplo:

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

- 2 Las máquinas virtuales de carga de trabajo deben tener las etiquetas adecuadas para conectarse a la PCG:
 - a Inicie sesión en la consola de AWS o el portal de Microsoft Azure.

- b Compruebe la etiqueta `eth0` o la etiqueta de interfaz de la máquina virtual.

La clave `nsx.network` debe tener el valor `default`.

Las máquinas virtuales iniciadas con cloud-init se ponen en cuarentena y no permiten la instalación de herramientas de terceros. ¿Qué debo hacer?

Con la directiva de cuarentena habilitada, cuando se inician máquinas virtuales mediante scripts cloud-init con las siguientes especificaciones, las máquinas virtuales se ponen en cuarentena al iniciarse y no se pueden instalar en ellas aplicaciones o herramientas personalizadas:

- etiquetado con `nsx.network=default`
- servicios personalizados arrancados o instalados automáticamente cuando la máquina virtual está encendida

Solución:

Actualice el grupo de seguridad `default` (AWS) o `default-vnet-<vnet-ID>-sg` (Microsoft Azure) para agregar puertos entrantes y salientes según sea necesario para la instalación de aplicaciones personalizadas o de terceros.

Etiqueté mi máquina virtual correctamente e instale NSX Tools, pero la máquina virtual está en cuarentena. ¿Qué debo hacer?

Si se detecta este problema, intente lo siguiente:

- Compruebe si la etiqueta: `nsx.network` de NSX Cloud y su valor `default` están escritos correctamente. Se distinguen mayúsculas de minúsculas.
- Vuelva a sincronizar la cuenta de AWS o Microsoft Azure desde CSM:
 - Inicie sesión en CSM.
 - Vaya a **Nubes > AWS/Azure > Cuentas**.
 - Haga clic en **Acciones** en el mosaico de la cuenta de nube pública y haga clic en **Volver a sincronizar cuenta**.

¿Qué debo hacer si no tengo acceso a la máquina virtual de carga de trabajo?

Desde la nube pública (AWS o Microsoft Azure):

- 1 Asegúrese de que todos los puertos en la máquina virtual, incluidos los administrados por NSX Cloud, el firewall del sistema operativo (Microsoft Windows o IPTables) y NSX-T Data Center estén correctamente configurados para permitir tráfico.

Por ejemplo, para permitir ping en una máquina virtual, deberá configurarse correctamente lo siguiente:

- Grupo de seguridad en AWS o Microsoft Azure. Consulte [Detección de amenazas mediante la directiva de cuarentena de NSX Cloud](#) para obtener más información.
 - Reglas de DFW de NSX-T Data Center. Consulte [Estrategia de conectividad predeterminada para las máquinas virtuales de carga de trabajo administradas por NSX en Modo forzado de NSX](#) para obtener detalles.
 - Firewall de Windows o IPTables en Linux.
- 2 Intente resolver el problema iniciando sesión en la máquina virtual mediante SSH u otros métodos, por ejemplo, la consola serie en Microsoft Azure.
 - 3 Puede reiniciar la máquina virtual bloqueada.
 - 4 Si aún no puede acceder a la máquina virtual, asocie una NIC secundaria a la máquina virtual de carga de trabajo desde la que se pueda acceder a esa máquina virtual de carga de trabajo.

¿Necesito una PCG incluso en Modo forzado de nube nativa?

Sí.

¿Se puede cambiar la función de IAM para la PCG después de incorporar mi cuenta de nube pública en CSM?

Sí. Puede volver a ejecutar el script de NSX Cloud correspondiente a la nube pública para volver a generar la función de PCG. Edite la cuenta de nube pública en CSM con el nuevo nombre de función después de volver a generar la función de PCG. Cualquier nueva instancia de PCG implementada en su cuenta de nube pública utilizará la nueva función.

Tenga en cuenta que las instancias de PCG existentes seguirán utilizando la función de PCG anterior. Si desea actualizar la función de IAM para una instancia de PCG existente, vaya a la nube pública y cambie manualmente la función de esa instancia de PCG.

¿Puedo usar las licencias locales de NSX-T Data Center con NSX Cloud?

Sí, puede si su ELA tiene una cláusula al respecto.

VMware NSX® Intelligence™ ofrece una visualización de la postura de seguridad del entorno de NSX-T Data Center local. La visualización se basa en los flujos de tráfico de red agregados en un período de tiempo específico. NSX Intelligence también le ayuda a planificar la microsegmentación realizando recomendaciones basadas en análisis con la aplicación de directivas de seguridad.

Importante Debe disponer de una función de administrador empresarial para tener permiso para instalar, configurar y usar NSX Intelligence.

Antes de poder comenzar a usar las funciones de NSX Intelligence, debe instalar y configurar el dispositivo de NSX Intelligence. Consulte "Instalar y configurar el dispositivo de NSX Intelligence" en la *Guía de instalación de NSX-T Data Center*.

Este capítulo incluye los siguientes temas:

- [Introducción a NSX Intelligence](#)
- [Vistas y flujos de NSX Intelligence](#)
- [Trabajar con las recomendaciones de NSX Intelligence](#)
- [Copia de seguridad y restauración de NSX Intelligence](#)
- [Resolución de problemas de NSX Intelligence](#)

Introducción a NSX Intelligence

Para comenzar a usar las funciones de NSX Intelligence, familiarícese con la interfaz gráfica de usuario de NSX Intelligence.

Después de instalar y configurar el dispositivo de NSX Intelligence, las funciones de NSX Intelligence se habilitarán en la pestaña **Planificar y solucionar problemas** de la interfaz de usuario de NSX Manager. En la sección **Detectar y planificar**, utilice **Detectar y realizar acción** para ver las entidades del centro de datos de NSX-T y las **Recomendaciones** con el fin de obtener recomendaciones para la planificación de microsegmentación.

Paseo por la página de inicio de NSX Intelligence

Para acceder a la página de inicio de NSX Intelligence, haga clic en **Planificar y solucionar problemas > Descubrir y realizar acción** en la interfaz de usuario de NSX Manager.

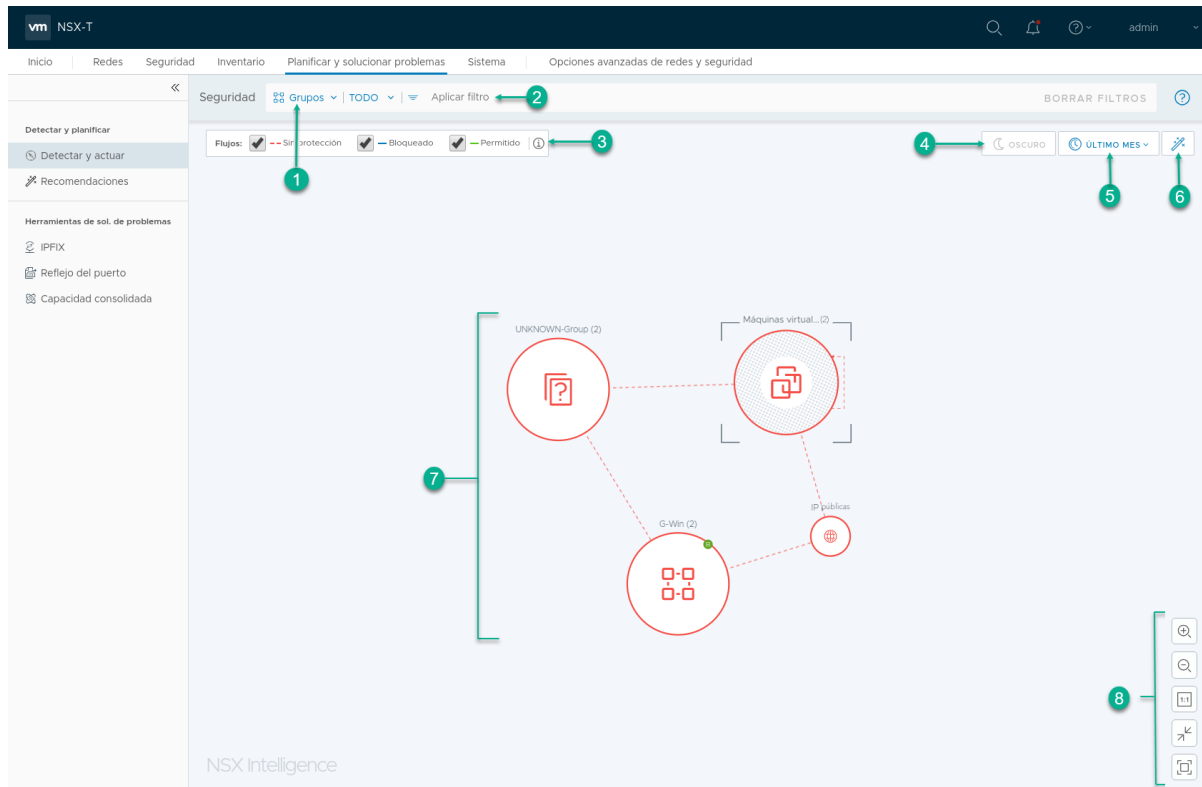
Después de instalar y configurar NSX Intelligence por primera vez, al hacer clic en **Descubrir y realizar acción**, es posible que se muestre el mensaje *No se encontraron datos y que es posible que necesite modificar los filtros*. Este mensaje se muestra porque NSX Intelligence aún no recibió los datos de tráfico de red para crear una visualización. Una vez que se reciban algunos datos de tráfico de red desde NSX Manager, NSX Intelligence podrá empezar a procesar algunas visualizaciones.

De forma predeterminada, al hacer clic en **Descubrir y realizar acción**, verá la visualización del estado de seguridad de todos los grupos de NSX-T Data Center que tenían flujos de tráfico sin protección entre sus máquinas virtuales durante las últimas 24 horas. Los flujos de tráfico de red sin protección son flujos entre máquinas virtuales que no tienen ninguna microsegmentación implementada. Si aún no hay ningún grupo definido, no se mostrarán grupos. Si hay máquinas virtuales, pero no pertenecen a ningún grupo, verá el siguiente icono del grupo Máquinas virtuales sin categorizar.





Si ya tiene grupos definidos y datos de tráfico capturado, es posible que se muestre una visualización similar a esta captura de pantalla. En la siguiente tabla se describen las secciones numeradas en la captura de pantalla.

Nota NSX Intelligence clasifica las direcciones IP que pertenecen a una de las siguientes notaciones CIDR como direcciones IP privadas: 192.168.0.0/16, 172.16.0.0/12 y 10.0.0.0/8. Cualquier dirección IP que no pertenezca a ninguna de estas notaciones CIDR se clasificará como una dirección IP pública. Si la dirección IP de la máquina virtual no se encuentra en una de estas notaciones CIDR, puede agregar la notación CIDR mediante la API de `PATCH /api/v1/intelligence/host-config` en la *Guía de la API de NSX-T Data Center*.











Sección	Descripción
1	<p>El área de selección de la vista Seguridad es donde se selecciona el tipo de visualización de seguridad que se va a mostrar. Existen dos tipos de vistas de seguridad disponibles: Grupos y Máquinas virtuales. Al hacer clic en Descubrir y realizar acción, la vista de seguridad predeterminada que se muestra será la vista Grupos de los objetos de grupo de NSX-T Data Center que tuvieron un tráfico de flujo sin protección durante las últimas 24 horas.</p> <ul style="list-style-type: none"> ■ Para seleccionar la vista máquinas virtuales, haga clic en la flecha hacia abajo junto a Grupos y seleccione Máquinas virtuales. ■ Para seleccionar las máquinas virtuales o los grupos específicos que desea incluir en la vista, haga clic en la flecha hacia abajo situada junto a TODOS y seleccione los elementos de la lista. ■ Para borrar los filtros de selección, haga clic en BORRAR FILTROS en la parte superior derecha de la pantalla. Al hacer clic en BORRAR FILTROS en la vista máquinas virtuales, los filtros de selección se borrarán y se colocarán en la vista Grupos. <p>Consulte Trabajar con la vista Grupos y Trabajar con la vista Máquinas virtuales para obtener más información sobre cómo trabajar con los dos tipos de vista.</p>
2	<p>Con Aplicar filtro puede ajustar los criterios utilizados para la visualización. En la lista desplegable, puede seleccionar los criterios que se utilizarán para la visualización. Puede seleccionar los miembros de la máquina virtual, etiquetas, tipos de flujo, la IP de origen, la IP de destino y el nombre o identificador de la regla. Para definir y aplicar más filtros, haga clic de nuevo en Aplicar filtro.</p>



Sección	Descripción
3	<p>En la sección Flujos puede seleccionar qué tipo de flujo de tráfico desea incluir en la visualización durante el período de tiempo seleccionado. En esta sección también se muestran los colores utilizados en la visualización de los tipos de flujo.</p> <ul style="list-style-type: none"> ■ Línea discontinua roja para los flujos Sin protección ■ Línea sólida azul para flujos Bloqueados ■ Línea sólida verde para los flujos Permitidos <p>De forma predeterminada, se selecciona el tipo de flujo de tráfico Sin protección para la visualización de NSX Intelligence actual. Consulte Trabajar con los flujos de tráfico para obtener más información.</p>
4	<p>La sección del modo de visualización define el tema que se utilizará para la visualización. De forma predeterminada, se utiliza el tema claro.</p> <ul style="list-style-type: none"> ■ Para usar el modo de tema oscuro, haga clic en el icono OSCURO. Puede utilizar el tema oscuro solo cuando esté viendo la visualización en modo de pantalla completa. ■ Para entrar en modo de pantalla completa, haga clic en  en la sección del control de visualización.
5	<p>En esta sección, seleccione el período de tiempo que se utilizará para determinar qué datos de flujo de red se usan para generar la visualización y recomendación deseadas. La selección determina los datos históricos que se utilizan en la vista Grupos o Máquinas virtuales. El período de tiempo va desde la hora actual hasta un determinado período de tiempo en el pasado.</p> <p>De forma predeterminada, se utiliza el intervalo de tiempo correspondiente a las últimas 24 horas. Para cambiar el período de tiempo seleccionado, haga clic en el período de tiempo seleccionado actualmente y seleccione Última hora, Últimas 12 horas, Últimas 24 horas, Última semana o Último mes.</p>
6	<p>Al hacer clic en el icono de la varita mágica Recomendación , el cuadro de diálogo Recomendaciones mostrará el resumen del inventario correspondiente a la vista actual. Si está en la vista Máquinas virtuales, puede generar una recomendación de NSX Intelligence haciendo clic en Iniciar nueva recomendación. Consulte Trabajar con las recomendaciones de NSX Intelligence.</p>
7	<p>Esta sección es la visualización del estado de seguridad de los grupos o las máquinas virtuales en su NSX-T Data Center local. También incluye la visualización de los flujos de tráfico de red que se produjeron durante el período de tiempo seleccionado. En esta sección, puede colocar el cursor en un nodo específico o a una flecha de flujo para obtener detalles sobre esa entidad específica.</p> <p>Para obtener más información, consulte Familiarizarse con los elementos gráficos de NSX Intelligence y Vistas y flujos de NSX Intelligence.</p>
8	<p>Esta sección incluye los controles de visualización para acercar y alejar la imagen, aplicar la relación de aspecto 1:1, cambiar el tamaño para ajustarse a la vista, y entrar o salir del modo de pantalla completa. También puede utilizar las teclas de acceso rápido del teclado para administrar los controles de visualización. Para mostrar la ventana de ayuda de los métodos abreviados de teclado, presione Mayús +/.</p> <p>Para desplazarse hasta una visualización usada anteriormente, utilice el botón Atrás del explorador web. Cuando esté en modo de pantalla completa, haga clic en Atrás (en la parte superior izquierda de la pantalla) para realizar el mismo desplazamiento hacia atrás que con el botón.</p>

Familiarizarse con los elementos gráficos de NSX Intelligence

La interfaz de usuario de NSX Intelligence incluye varios elementos gráficos para ayudar a visualizar las entidades del centro de datos, los flujos de tráfico y ciertas actividades en el entorno de NSX-T Data Center.

La siguiente tabla muestra un glosario de elementos gráficos de NSX-T Data Center que se pueden ver en una visualización de NSX Intelligence.

Elemento gráfico	Descripción
	Este icono representa un grupo, que es una colección de máquinas virtuales en las que se pueden aplicar directivas de seguridad, incluidas las reglas de firewall de este a oeste. Consulte Trabajar con la vista Grupos .
	Este icono representa una máquina virtual que forma parte del entorno de NSX-T Data Center. Una máquina virtual puede pertenecer a más de un grupo. Consulte Trabajar con la vista Máquinas virtuales .
	Este icono representa las IP públicas en Internet. Si al menos una máquina virtual del entorno de NSX-T Data Center se comunicó con una IP pública durante el período de tiempo seleccionado, ese flujo de tráfico se incluirá en la visualización actual.
	Una dirección IP, como una dirección IP de unidifusión, difusión o multidifusión, que participó en las actividades de tráfico de red durante el período de tiempo seleccionado.
 Máquinas virtual... (4)	Este icono se usa para el grupo de máquinas virtuales que no pertenecen a un grupo.
	Una flecha representa un flujo de tráfico de red producido entre dos máquinas virtuales durante un período de tiempo seleccionado. Existen tres tipos diferentes de flechas: las rojas discontinuas para los flujos sin protección, las azules continuas para los flujos bloqueados y las verdes continuas para los flujos permitidos. Consulte Trabajar con los flujos de tráfico .
	El nodo seleccionado como el nodo actual enfocado aparece rodeado de un círculo discontinuo. Es el nodo anclado durante el modo de selección y en la vista que se está mostrando.
	Este icono aparece en el borde de un nodo de grupo si el grupo se agregó al inventario de NSX-T Data Center durante el período de tiempo seleccionado. Si NSX-T Data Center descubrió una máquina virtual durante el período de tiempo seleccionado, el icono aparecerá en el borde de ese nodo de máquina virtual.

Elemento gráfico	Descripción
	<p>Este icono aparece en el borde del nodo de grupo si el grupo se eliminó durante el período de tiempo seleccionado y no se eliminaron los miembros de la máquina virtual. En el borde de un nodo de máquina virtual, este icono indica que la máquina virtual se eliminó durante el período de tiempo seleccionado. Aunque se elimine una máquina virtual o un grupo, seguirá apareciendo en la visualización actual para mostrar una vista histórica que indique que la máquina virtual o el grupo se eliminaron durante el período seleccionado.</p>
	<p>Este icono aparece cada vez que vemos grupos y máquinas virtuales juntos. Por ejemplo, en una vista de grupos de análisis profundo o máquinas virtuales relacionadas de un grupo. El icono aparece en el borde de un nodo de máquina virtual en los siguientes casos.</p> <ul style="list-style-type: none"> ■ si la máquina virtual se movió fuera del grupo que se está viendo actualmente durante el período de tiempo seleccionado ■ si, en algún momento durante el período de tiempo seleccionado, la máquina virtual formó parte del grupo que se está viendo actualmente, pero ya no forma parte de ese grupo

Vistas y flujos de NSX Intelligence

La visualización de NSX Intelligence se compone de los grupos o las máquinas virtuales y los flujos de red que se produjeron con dichos grupos o máquinas virtuales durante el período de tiempo seleccionado.

Importante La visualización que se muestra para un período de tiempo específico representa todos los flujos y las actividades de red (como la adición, la eliminación o el movimiento de las máquinas virtuales y los grupos) que se produjeron en el centro de datos de NSX-T durante ese período de tiempo. Es posible que una máquina virtual aparezca más de una vez en la visualización. Por ejemplo, si una máquina virtual estaba conectada a un host ESXi que originalmente no estaba administrado, y el host se pasa a administrarse a través de VMware vCenter Server™ durante el período seleccionado, la máquina virtual aparecerá dos veces en la vista máquinas virtuales. De forma similar, si un host ESXi se desconecta de vCenter Server y se vuelve a agregar durante el mismo período de tiempo seleccionado, las máquinas virtuales asociadas al host aparecerán eliminadas y nuevas durante el período de tiempo seleccionado. En una vista Grupos, si una máquina virtual estaba en el grupo sin clasificar y se agregó un grupo durante el mismo período seleccionado, la máquina virtual aparecerá tanto en el grupo sin clasificar como en su nuevo grupo.

NSX Intelligence solo admite grupos con tipos de miembros de máquinas virtuales. Si tiene grupos con otros tipos de miembros, es posible que la vista Grupos muestre flujos correlacionados entre los grupos con tipos de miembros de máquinas virtuales en lugar de grupos reales en la regla de seguridad.

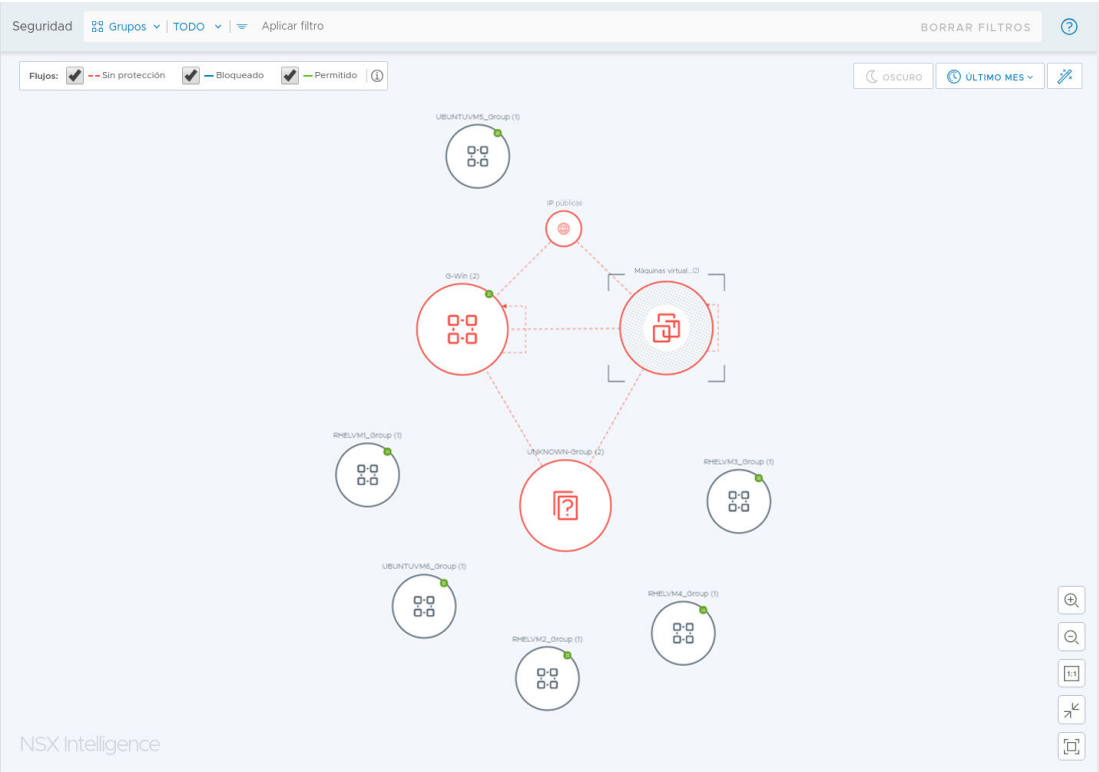
Consulte en esta sección más información sobre cómo trabajar con la vista Grupos, la vista Máquinas virtuales y los distintos flujos de tráfico.

Trabajar con la vista Grupos

La vista Grupos se muestra en la página de inicio de NSX Intelligence de forma predeterminada. Esta vista se filtra para mostrar todos los grupos que disponían de un flujo de tráfico no protegido durante las últimas 24 horas.

Nodos y flechas en la vista Grupos

Un nodo de una vista Grupos representa los objetos de NSX, como máquinas virtuales, conjuntos de direcciones IP, etc., en su entorno de NSX-T Data Center. En la siguiente captura de pantalla se muestra un ejemplo de una vista Grupos.



En la siguiente tabla se incluyen los tipos de nodos que se pueden ver en la vista Grupos.

Tipo de nodo de grupo	Icono	Descripción
Grupo normal		Un nodo de grupo normal en NSX Intelligence representa cualquier recopilación de objetos de NSX en el entorno NSX-T Data Center. En esta versión, esos objetos de NSX son solo máquinas virtuales y, por lo tanto, NSX Intelligence admite grupos normales solo con máquinas virtuales como miembros. Un objeto de NSX puede pertenecer a más de un grupo, por lo que una máquina virtual puede aparecer en más de un nodo de grupo.
Grupo sin categorizar		Un nodo de grupo sin categorizar representa una colección de máquinas virtuales que no pertenecen a ningún grupo.
Grupo desconocido		Un nodo de grupo desconocido representa un conjunto de objetos varios que no se encontraron en el inventario de NSX-T Data Center. Sin embargo, estos objetos se están comunicando con uno o varios objetos de NSX en el entorno de NSX-T Data Center.
Grupo de IP públicas		Un nodo de grupo de IP públicas representa una colección de direcciones IP públicas (IPv4 o IPv6) que se comunican con los objetos de NSX de NSX-T Data Center.

El tamaño de un nodo en la vista Grupos depende del número de objetos de NSX, como máquinas virtuales, que pertenezcan a ese grupo. Por ejemplo, cuanto más grande sea el nodo de un grupo, más máquinas virtuales pertenecen a ese grupo. El nombre del grupo y el número de máquinas virtuales que contiene se muestran sobre el nodo.

Las flechas entre los nodos de grupo representan los flujos de tráfico que se han producido entre las máquinas virtuales de esos nodos de grupo conectados durante el período seleccionado. Una flecha de autorreferencia en un nodo de grupo indica que al menos una máquina virtual se está comunicando con otra máquina virtual dentro del mismo grupo. Consulte [Trabajar con los flujos de tráfico](#) para obtener más información.

Un nodo con un borde rojo indica que se produjo al menos un flujo no protegido con una máquina virtual en el grupo, independientemente de cuántos flujos permitidos o bloqueados se detectaron durante el período de tiempo seleccionado. Un borde azul en un nodo significa que no se detectaron flujos de tráfico no protegidos, pero que sí se detectó al menos un flujo bloqueado, independientemente de cuántos flujos permitidos se detectaran durante el período de tiempo seleccionado. Un nodo con un borde verde indica que no se detectaron flujos sin protección ni bloqueados durante el período seleccionado, pero sí se detectó al menos un flujo permitido. Un nodo con un borde gris significa que no se detectó ningún flujo de tráfico para las máquinas virtuales pertenecientes a ese grupo durante el período de tiempo seleccionado.

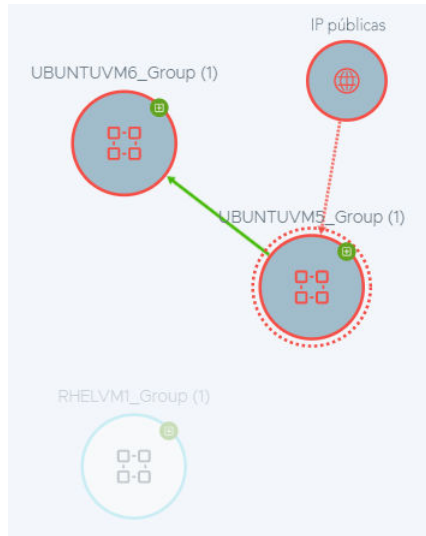
Si no ve la vista Grupos, haga clic en la flecha hacia abajo situada junto a **Máquinas virtuales** en el área de selección de la vista Seguridad y seleccione **Grupos**. En la lista desplegable de selección que se abre, puede seleccionar **Todos los grupos** o grupos específicos de la lista y, a continuación, hacer clic en **Aplicar**. Utilice el cuadro de texto **Buscar** para filtrar la lista de selección. Si sale de la lista desplegable sin seleccionar nada o si selecciona **Todos los grupos**, se aplicará la opción **Todos los grupos** a la vista Grupos.

Selección de nodos en la vista Grupos

Si coloca el cursor sobre un nodo de grupo, se mostrará información sobre ese grupo, como puede verse en el siguiente ejemplo del grupo G-Win. Se muestra también el número y los tipos de flujos detectados durante el período de tiempo seleccionado. Si el grupo se agregó durante el período de tiempo seleccionado, se mostrará también el icono Nueva etiqueta y los detalles de cuándo se creó el grupo.



Al hacer clic en el nodo de un grupo, se marcará la selección con un círculo discontinuo como un nodo de máquina virtual anclado. Los otros grupos que están conectados al nodo de grupo seleccionado también se harán más visibles en la vista. Los demás nodos se atenuarán. Por ejemplo, en la siguiente captura de pantalla, el nodo UBUNTUVM5_Group es el seleccionado, y también aparecen resaltados otros grupos que compartían un flujo de tráfico con UBUNTUVM5_Group durante el período de tiempo seleccionado. Los demás grupos que no se comunicaron con UBUNTUVM5_Group aparecerán atenuados en la vista.

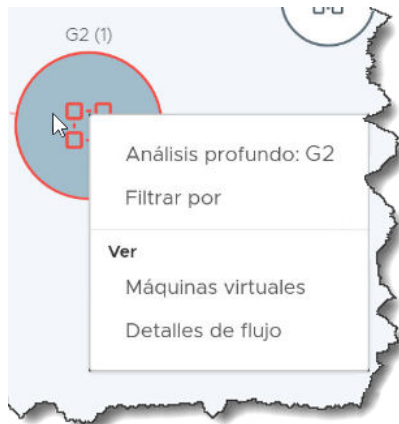


Para borrar la selección fija, haga clic en cualquier área vacía de la vista Grupos.

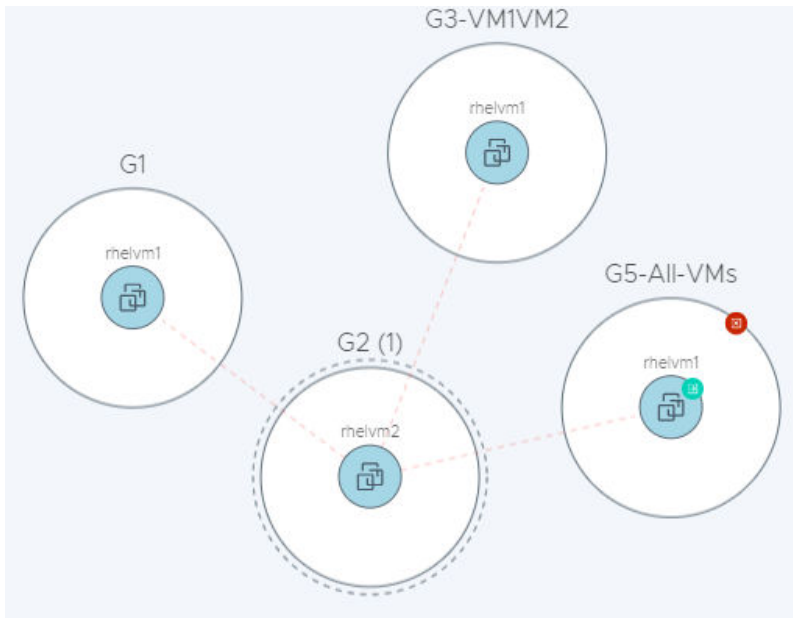
Si se aleja la vista Grupos y los detalles de los nodos ya no están visibles, coloque el cursor en cualquier parte visible de un nodo y se mostrarán los detalles.

Acciones disponibles en la vista Grupos

Al hacer clic con el botón secundario en el nodo de un grupo, como se muestra en la siguiente imagen, se muestra un menú contextual con las acciones disponibles.



- Al seleccionar **Análisis profundo:Nombre_grupo** se rodea el nodo del grupo seleccionado con un círculo discontinuo para marcarlo como el nodo de grupo anclado o el grupo actualmente en el foco. Las máquinas virtuales que pertenecen al grupo se muestran dentro del nodo del grupo. Todos los grupos que tuvieron flujos de tráfico con las máquinas virtuales en el grupo anclado durante el período de tiempo seleccionado también aparecerán en la vista Grupos. En el siguiente ejemplo, el grupo G2 es el grupo anclado y los otros grupos están en la vista porque las máquinas virtuales que contienen tenían flujos de tráfico con rhelvm2 en el grupo G2 durante el período de tiempo seleccionado.



- Al seleccionar **Filtrar por**, el grupo actual se agrega al filtro de visualización utilizado para la vista Grupos actual.
- Al seleccionar **Máquinas virtuales**, se muestra una tabla de todas las máquinas virtuales que pertenecían al grupo actual durante el período de tiempo seleccionado. En esa tabla puede ver los detalles de las máquinas virtuales que pertenecen al grupo seleccionado y otros grupos a los que pertenece también cada máquina virtual. Para agregar la máquina virtual al filtro de visualización actual, haga clic en el icono de filtro.
- Al seleccionar **Detalles de flujo**, se mostrará la tabla Detalles de flujo del grupo seleccionado actualmente, como se muestra en la siguiente captura de pantalla. En esta tabla se muestran los detalles de los flujos que han ocurrido y que están activos en las máquinas virtuales que pertenecen al grupo actual durante el período de tiempo seleccionado. Los detalles incluyen el tipo de flujo, los grupos de origen y de destino del flujo, la hora de inicio y finalización del flujo y los servicios que se utilizaron. Puede hacer clic en algunos de los detalles para obtener más información. Consulte [Trabajar con los flujos de tráfico](#) para obtener más información.

Detalles de flujo

Últimas 24 horas

Mostrando detalles de flujo de Máquinas virtuales sin categorizar

Flujos completados Flujos activos

Buscar

Origen	Grupo de origen	Destino	Grupo de destino	Servicios	Hora de finalización	Último flujo
ubuntu12.04.1-2G-LAMP	G5	ubuntu12.04-pace	UNCATEGORIZED	SSH... 2 más	6/11/19 8:05	Sin protección
ubuntu12.04.1-2G-LAMP	G1	ubuntu12.04-pace	UNCATEGORIZED	SSH... 2 más	6/11/19 8:05	Sin protección

Actualizar

1 - 2 of 2 Flujos

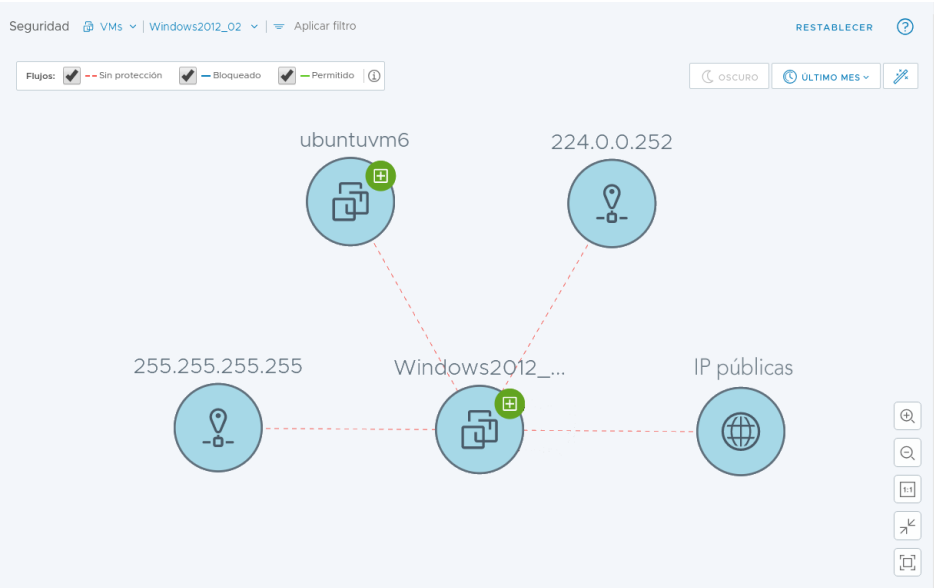
CERRAR

Trabajar con la vista Máquinas virtuales

Un nodo de la vista Máquinas virtuales representa una máquina virtual en su entorno local de NSX-T Data Center.

Nodos y flechas en la vista Máquinas virtuales

En la vista Máquinas virtuales, los límites de los grupos no están visibles. Cualquier nodo que se esté comunicando con una de las máquinas virtuales del entorno de NSX-T Data Center, pero que no se haya identificado como parte del inventario de NSX-T Data Center, también se incluirá en la vista Máquinas virtuales. A continuación, se muestra una vista Máquinas virtuales sencilla.



En la siguiente tabla se incluyen los tipos de nodos de máquinas virtuales que se pueden ver en la vista Máquinas virtuales.

Tipo de nodo de máquina virtual	Icono	Descripción
Máquina virtual normal		Un nodo de máquina virtual normal representa una máquina virtual que forma parte del entorno de NSX-T Data Center. Una máquina virtual puede pertenecer a más de un grupo.
IP pública		Un nodo de IP pública representa una dirección IP pública, ya sea IPv4 o IPv6, que se comunica con el entorno de NSX-T Data Center.
IP		Un nodo IP representa una dirección IP que participó en las actividades de tráfico de red durante el período de tiempo seleccionado. Una dirección IP puede ser una IP de unidifusión, difusión o multidifusión.

Si no ve la vista Máquinas virtuales, haga clic en la flecha hacia abajo situada junto a **Grupos** en el área de selección de la vista Seguridad y seleccione **Máquinas virtuales**. En la lista desplegable de selección que se abre, puede seleccionar **Todas las máquinas virtuales** o máquinas virtuales específicas de la lista y, a continuación, hacer clic en **Aplicar**. Utilice el cuadro de texto **Buscar** para filtrar la lista de selección. Si sale de la lista desplegable sin seleccionar nada o si selecciona **Todas las máquinas virtuales**, se aplicará la opción **Todas las máquinas virtuales** a la vista Máquinas virtuales.

Las flechas entre los nodos de máquinas virtuales representan los flujos de tráfico producidos entre las máquinas virtuales durante el período de tiempo seleccionado. Consulte [Trabajar con los flujos de tráfico](#) para obtener más información.

Selección de nodos en la vista Máquinas virtuales

Cuando se coloca el cursor sobre un nodo de máquinas virtuales, se muestra información sobre el nodo, como puede verse en el siguiente ejemplo. Se muestra también el número y los tipos de flujos a las máquinas virtuales detectados durante el período de tiempo seleccionado. Si el grupo se agregó durante el período de tiempo seleccionado, se mostrará también el icono Nueva etiqueta y los detalles de cuándo se agregó la máquina virtual.



Al hacer clic en el nodo de una máquina virtual, un círculo discontinuo marcará la selección como un nodo de máquina virtual anclado. Otros nodos de máquina virtual que tengan flujos de tráfico con ese nodo de máquina virtual anclado también se harán más prominentes en la vista Máquinas virtuales. Los demás nodos se atenúan para que sean menos visibles. Para borrar la selección fija, haga clic en cualquier área vacía de la vista Máquinas virtuales.

Si reduce el zoom de la vista Máquinas virtuales y los detalles de los nodos de máquina virtual ya no están visibles, coloque el cursor en cualquier parte visible del nodo de la máquina virtual y se mostrarán sus detalles.

Acciones disponibles en la vista Máquinas virtuales

Al hacer clic con el botón secundario en el nodo de una máquina virtual, como se muestra en la siguiente imagen, se muestra un menú contextual con las acciones disponibles.






Selección	Descripción
Filtrar por	La máquina virtual se agregará al filtro de visualización utilizado para la vista Máquinas virtuales actual.
Información de la máquina virtual	Se muestran los detalles de la máquina virtual durante el período de tiempo seleccionado.
Grupos relacionados	Tabla Grupos con información sobre los grupos a los que pertenecía la máquina virtual durante el período de tiempo seleccionado.
Detalles de flujo	<p>En esta tabla se muestran los detalles de los flujos que han ocurrido y que están activos en la máquina virtual durante el período de tiempo seleccionado. Entre los detalles, se incluyen los siguientes.</p> <ul style="list-style-type: none"> ■ tipo de flujo ■ grupos de origen y destino del flujo ■ hora de inicio y finalización del flujo ■ servicios que se utilizaron <p>Puede hacer clic en algunos de los detalles para obtener más información. Consulte Trabajar con los flujos de tráfico para obtener más información.</p>
Iniciar recomendación	Muestra el asistente Iniciar nuevas recomendaciones. Consulte Trabajar con las recomendaciones de NSX Intelligence para obtener información detallada.

Trabajar con los flujos de tráfico

Las flechas entre los nodos de grupo o de máquina virtual representan los flujos de tráfico de red producidos entre las máquinas virtuales durante el período de tiempo seleccionado.

Los flujos de tráfico de red se basan en las reglas de firewall distribuido (DFW) de capa 3 y en los flujos de tráfico que se produjeron durante el período de tiempo seleccionado. Todos los flujos de tráfico de red que coincidieron con una regla de DFW de capa 3 con estado que utilizaban IPv4 o IPv6 con protocolos TCP, UDP, GRE, ESP y SCTP se incluyen en los detalles de visualización y flujo. Los flujos TCP y UDP tienen detalles de nivel de IP y puerto y otros solo tienen detalles de nivel de IP.

Los flujos de tráfico se clasifican en los siguientes tipos.

Tipo de flujo	Gráfico	Descripción
Sin protección		Una flecha roja indica que el sistema detectó que el flujo de tráfico encontró una regla (Origen: Cualquiera Destino: Cualquiera Acción: Permitir, Rechazar o Anular) y que se requieren directivas de seguridad más detalladas. Esta regla puede ser la predeterminada o puede residir en cualquier parte del firewall distribuido de este a oeste.
Bloqueado		Una flecha azul indica que el sistema detectó que el flujo de tráfico cumplió una regla "Rechazar" o "Anular" más detallada que la que se menciona en la definición de flujo "Sin protección".
Permitido		Una flecha verde indica que el sistema detectó que el flujo de tráfico cumplió una regla "Permitir" más detallada que la que se menciona en la definición de flujos "Sin protección".

Para centrarse solo en objetos con ciertos tipos de flujos de tráfico, utilice el área de selección de la vista Seguridad para seleccionar el tipo de vista, y use el atributo de filtro "Tipo de flujo" para delimitar la selección.

Si anula la selección de un tipo de flujo, las líneas de flujo de ese tipo se ocultarán del gráfico. A menos que se apliquen filtros que excluyan determinados objetos, los objetos de grupo o de máquina virtual permanecerán visibles, independientemente de los tipos de flujo de tráfico que se hayan producido con esos objetos durante el período de tiempo seleccionado. Por ejemplo, si anula la selección del tipo de flujo "Permitido", todas las líneas de flujo permitidas se ocultarán en el gráfico. Sin embargo, se seguirán mostrando todos los objetos, incluso aquellos que solo tengan flujos de tráfico permitidos durante el período de tiempo seleccionado.

La dirección de las flechas de flujo indica el origen y el destino de cada flujo de tráfico detectado. En la vista Grupos, una flecha de autorreferencia en un nodo de grupo indica que al menos una máquina virtual se está comunicando con otra máquina virtual dentro del mismo grupo. En la vista Máquinas virtuales, una flecha de autorreferencia indica que un objeto de NSX de la máquina virtual se comunicó con otro objeto de NSX en la misma máquina virtual.

Cuando se coloca el cursor sobre una flecha de flujo, se muestra información sobre los flujos relacionados con el grupo o la máquina virtual, como se muestra en el siguiente ejemplo del grupo G2.



Al hacer clic en una flecha de flujo, se muestra el cuadro de diálogo Detalles de flujo. Muestra los detalles de los flujos activos y completados que se produjeron durante el período de tiempo seleccionado. Para obtener información más detallada sobre el origen, el destino, el tipo de servicio y el tipo de cada flujo, haga clic en los vínculos de la tabla para obtener más detalles.

Trabajar con las recomendaciones de NSX Intelligence

NSX Intelligence puede proporcionar recomendaciones de microsegmentación basadas en los patrones de flujos de tráfico que se han producido entre las máquinas virtuales de su entorno de NSX-T Data Center durante el periodo de tiempo seleccionado.

Información sobre las recomendaciones de NSX Intelligence

Las recomendaciones proporcionadas por NSX Intelligence incluyen directivas de seguridad, grupos de seguridad de directivas y servicios para las aplicaciones.

Las recomendaciones se basan en los patrones de flujo de tráfico de red entre cargas de trabajo de máquinas virtuales en hosts ESXi administrados por vCenter Server. Pueden ayudarle a aplicar una directiva de seguridad más dinámica al correlacionar los patrones de tráfico de comunicación que se produjeron dentro de su entorno de NSX-T Data Center.

Las recomendaciones de la directiva de seguridad son de la categoría Directivas de seguridad de firewall distribuido de este-oeste de aplicación. Las recomendaciones de los grupos de seguridad constan de una lista de máquinas virtuales que aparecen en los flujos de tráfico de red que se analizaron según el periodo de tiempo y el límite de la máquina virtual que especificó. Las recomendaciones de servicio son objetos de servicio utilizados en ciertos puertos por aplicaciones de las máquinas virtuales que especificó, pero estos servicios aún no están definidos en el inventario de NSX-T Data Center.

Existen varias formas de solicitar la recomendación, pero la más sencilla es usar la pestaña **Planificar y solucionar problemas > Recomendaciones** y hacer clic en **Iniciar nueva recomendación**. Debe especificar las máquinas virtuales que comprenden los límites de la aplicación y el intervalo de tiempo en el que se deben analizar los flujos de tráfico de red en dichas máquinas virtuales. Una vez que se haya completado el análisis de la recomendación, podrá consultarla de forma detallada y, si es necesario, modificarla antes de publicarla. Consulte [Generar una nueva recomendación de NSX Intelligence](#) para obtener más información.

Generar una nueva recomendación de NSX Intelligence

La función Recomendaciones de NSX Intelligence proporciona recomendaciones para ayudarle a microsegmentar sus aplicaciones.

Generar una recomendación de NSX Intelligence implica recomendaciones de las directivas de seguridad, los grupos de seguridad de directivas y los servicios de la aplicación. Las recomendaciones se basan en el patrón de tráfico de comunicación entre las máquinas virtuales de su NSX-T Data Center. Existen varias formas de generar una recomendación con la interfaz de usuario de NSX Intelligence. A continuación se describen los tres métodos disponibles que se pueden utilizar.


Requisitos previos

Instale NSX Intelligence. Consulte "Instalar y configurar NSX Intelligence" en la *Guía de instalación de NSX-T Data Center*.

Procedimiento

- 1 En un navegador, inicie sesión con privilegios de administrador empresarial en una instancia de NSX Manager desde `https://<dirección-ip-nsx-manager>`.
- 2 Inicie la generación de una nueva recomendación.

Utilice esta tabla para elegir uno de los tres métodos disponibles.

Método	Pasos
Seleccione Planificar y solucionar problemas > Recomendaciones .	Haga clic en Iniciar nueva recomendación .
En la vista Máquinas virtuales, seleccione una máquina virtual y haga clic en ella con el botón secundario.	En el menú contextual, seleccione Iniciar nuevas recomendaciones .
Seleccione Planificar y solucionar problemas > Detectar y planificar .	<ol style="list-style-type: none"> 1 En el filtro Postura de seguridad, haga clic en la flecha abajo y seleccione Máquinas virtuales. 2 Seleccione las máquinas virtuales que comprenden el límite de la aplicación y haga clic en Aplicar. 3 Haga clic en el icono de la varita mágica  Recomendaciones. 4 En el cuadro de diálogo Recomendaciones, haga clic en Iniciar nueva recomendación.

- 3 En el asistente Iniciar nuevas recomendaciones, si lo desea puede cambiar el valor predeterminado de **Nombre de recomendación**.
- 4 Defina o modifique las máquinas virtuales que se utilizarán como límite para la recomendación de la directiva de seguridad.
 - a Haga clic en **Seleccionar máquinas virtuales** o en el número de **Máquinas virtuales seleccionadas**.
 - b En el cuadro de diálogo Seleccionar máquinas virtuales, marque las máquinas virtuales que desea utilizar como límite para el análisis y desmarque las que no desee incluir.

Puede seleccionar hasta 100 máquinas virtuales para usarlas como límite para la recomendación. También puede empezar a introducir el nombre en la barra de selección para filtrar las máquinas virtuales que desea seleccionar.
 - c Haga clic en **Guardar**.

El número de máquinas virtuales seleccionadas se indica en el cuadro de diálogo Detectar nueva recomendación.
- 5 Expandir la sección **Más opciones** para cambiar los valores predeterminados de **Descripción** e **Intervalo de tiempo** que se usan para el análisis de recomendaciones. El valor predeterminado de **Intervalo de tiempo** es Último mes, lo que significa que los flujos de tráfico de red que ocurrieron durante el último mes entre las máquinas virtuales seleccionadas se utilizarán durante el análisis de la recomendación.
- 6 Haga clic en **Iniciar detección**.

Las recomendaciones se procesan en serie. De media, puede tardar entre 3 y 4 minutos en finalizar cada recomendación, en función de si existen otras recomendaciones pendientes de su procesamiento. Si hay muchos flujos de tráfico entre las máquinas virtuales que se deben analizar, una recomendación puede tardar entre 10 y 15 minutos en generarse. Se puede realizar un seguimiento del estado desde la pestaña **Recomendaciones**. El estado pasa de Esperando a Analizando y, por último, a Listo para publicar. En la siguiente captura de pantalla se muestran los tres estados de las recomendaciones generadas.

Recomendaciones					
INICIAR NUEVA RECOMENDACIÓN		Filtrar por nombre, ruta o más			
	Nombre	Estado	Máquinas virtuales	Hora de creación	Última modificación
⋮ >	REC 20191107 10:09:19	No hay recomendaciones disponibles	6	7/11/19 2:09	7/11/19 2:09
⋮ >	REC 20191106 16:39:30	No hay recomendaciones disponibles	1	6/11/19 8:39	6/11/19 8:39
⋮ >	REC 20191106 16:15:53	No hay recomendaciones disponibles	1	6/11/19 8:16	6/11/19 8:16

Una vez publicada la recomendación, el estado cambiará a Publicado.

Pasos siguientes

Revise la recomendación generada y decida si desea publicarla. Consulte [Revisar y publicar una recomendación generada](#).

Revisar y publicar una recomendación generada

Una vez que la recomendación de NSX Intelligence generada alcance el estado Listo para publicar, podrá revisarla, modificarla si es necesario y decidir si desea publicarla.

Requisitos previos

Genere una nueva recomendación. Consulte [Generar una nueva recomendación de NSX Intelligence](#).

Procedimiento

- 1 En un navegador, inicie sesión con privilegios de administrador empresarial en una instancia de NSX Manager desde `https://<dirección-ip-nsx-manager>`.
- 2 Haga clic en **Planificar y solucionar problemas > Recomendaciones**.
- 3 Para limitar la lista de recomendaciones que se muestran, haga clic en **Filtrar por nombre, ruta o más** en la parte superior derecha de la pantalla y especifique los criterios de filtro que se utilizarán.
- 4 Si decide no utilizar la recomendación, haga clic en el icono de menú de tres puntos y seleccione **Eliminar**.
- 5 Para ver el resumen de una recomendación, haga clic en la punta de flecha junto al nombre de la recomendación para expandir la fila.

Puede ver el número de reglas generadas y el número de grupos afectados.

6 Revise y administre los detalles de la recomendación.

- a Haga clic en el nombre de la recomendación.

Se abrirá el asistente **Recomendaciones**, que tiene un aspecto similar a la siguiente imagen.

Recommendations

REC 20190719 15:59:02

Showing discovered recommendations. Review, Edit and Proceed with your selections to place the rules in the existing Firewall context.

Recommended FW Rules Recommended Groups Recommended Services

Category: Application Recommended Rules: 6 Recommended Groups: 3 Recommended Services: 0

Name	Sources	Destinations	Services	Profiles	Applied To	Action	
Policy-1 (REC 20190719 15:59:02)	(6)						
Rule-1 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	Win - RPC, DCOM, EP...	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-2 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBDS-Broadcast-V1	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-3 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCP-Server	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-4 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCPv6 Server	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-5 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBNS-Broadcast-V1	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-6 (REC 20190719 15:59:02)	Group-2 (REC 20190719 15:59:02)	Group-3 (REC 20190719 15:59:02)	SSH	None	Group-2 (REC 20190719 15:59:02)	Allow	<input checked="" type="checkbox"/>

1 of 1 Policy

CANCEL CONTINUE LATER NEXT

- b En la pestaña **Reglas de firewall recomendadas**, revise los detalles de la regla de Firewall. Para modificar cualquiera de los detalles, haga clic en el valor de la columna correspondiente y seleccione el icono Editar (lápiz).
- c Para definir cómo se deben gestionar los paquetes, seleccione **Permitir**, **Anular** o **Rechazar** en la columna **Acción**.
- d Use el botón situado a la derecha para habilitar o deshabilitar la regla. De forma predeterminada, la regla que se generó está configurada para habilitarse cuando se publique, como se muestra en la imagen del paso anterior.
- e Haga clic en **Grupos recomendados**.
- f Haga clic en el vínculo de la columna **Miembros** para revisar los detalles de las máquinas virtuales y las direcciones IP que se establecieron para la recomendación de grupo.
- g Haga clic en el icono de menú (tres puntos) situado junto al nombre del grupo y seleccione **Editar** para modificar la recomendación de grupo.
- h Haga clic en **Servicios recomendados** y revise los detalles.
- i Haga clic en el icono de menú (tres puntos) situado junto al nombre del servicio y seleccione **Editar** para modificar el nombre o la descripción. Antes de eliminar un servicio, asegúrese de que no lo utilice ninguna regla.
- j Haga clic en **Siguiente**.

- 7 En el panel **Colocar reglas en contexto de firewall**, puede cambiar el orden en el que se aplicará la recomendación de la regla con las reglas de firewall actuales. Arrastre la sección resaltada o haga clic en el icono de menú de tres puntos y seleccione **Mover la sección seleccionada arriba** o **Mover la sección seleccionada abajo**.
- 8 Haga clic en **Publicar**.
- 9 En el cuadro de diálogo **Publicar recomendaciones**, haga clic en **Sí**.
- 10 En la página de Resumen de la aplicación, compruebe que las directivas de seguridad se publicaron correctamente y haga clic en **Cerrar**.

La columna Estado de la recomendación cambiará a Publicado en la tabla de recomendaciones.

Resultados

Una vez que las recomendaciones de la directiva de seguridad se hayan publicado correctamente, estarán en modo de solo lectura en la pestaña **Planificar y solucionar problemas > Recomendaciones**. Para ver y administrar las recomendaciones de reglas publicadas, vaya a **Seguridad > Firewall distribuido**.

Importante Después de haber publicado las recomendaciones de la regla, la visualización continuará mostrando los flujos afectados entre las máquinas virtuales como flechas naranjas (flujos sin proteger) hasta que se generan nuevos flujos entre las máquinas virtuales afectadas. La visualización solo notifica los flujos de tráfico en función de la hora en la que se produjeron en el host, y no refleja el conjunto de reglas publicadas después de que se hayan producido dichos flujos de tráfico. Una vez que se publica el conjunto de reglas y se generan nuevos flujos de tráfico, los nuevos flujos se mostrarán como flechas verdes (flujos permitidos).

Copia de seguridad y restauración de NSX Intelligence

Si la configuración de NSX Intelligence actual deja de funcionar, o si desea restaurarla a un estado anterior, puede restaurar su configuración a partir de una copia de seguridad. El flujo de trabajo de copia de seguridad y restauración solo se admite si se usa la CLI de NSX Intelligence.

Cuando se hace una copia de seguridad, NSX Intelligence solo copia los archivos de configuración utilizados por todos los servicios que componen el dispositivo de NSX Intelligence. No se incluyen datos de visualización en la copia de seguridad.

Si se pierden o se dañan los datos en NSX Intelligence, también se perderán todos los datos de las recomendaciones y los flujos relacionados. Si se vuelve a instalar NSX Intelligence, se reiniciará la recopilación de datos de tráfico de red, y la visualización de los datos recopilados estará disponible a partir de ese punto en adelante.

Una vez finalizada la configuración de la copia de seguridad, podrá ejecutar manualmente el comando de copia de seguridad en el dispositivo de NSX Intelligence en cualquier momento. La copia de seguridad se cifra, se comprime y se almacena en el servidor remoto definido durante la configuración de la copia de seguridad. La fecha y la hora en las que se crea cada copia de seguridad se anexan al nombre del archivo para que cada uno sea único. Por ejemplo, `config-backup-2019-06-21T21_06_07UTC.tar.gz`.

Al restaurar una copia de seguridad de NSX Intelligence, se restaura el estado de configuración en el momento en el que se realizó la copia de seguridad. Debe restaurar la copia de seguridad en un dispositivo de NSX Intelligence que ejecute la misma versión que el dispositivo de NSX Intelligence desde el que se creó el archivo de copia de seguridad. Puede restaurar la copia de seguridad en un dispositivo de NSX Intelligence anterior o en un dispositivo de NSX Intelligence recién instalado, pero debe tener la misma versión que el dispositivo de NSX Intelligence del que se realizó la copia de seguridad.

Configurar las copias de seguridad de NSX Intelligence

Debe configurar un servidor de archivos de copia de seguridad para poder realizar una copia de seguridad de la configuración de NSX Intelligence. Después de configurar un servidor de archivos de copia de seguridad, puede realizar una copia de seguridad de NSX Intelligence en cualquier momento.

Requisitos previos

- Compruebe que dispone de las credenciales de administrador para acceder a la CLI de NSX Intelligence.
- Asegúrese de que tiene el nombre de usuario y la contraseña del servidor remoto.
- Obtenga la ruta de archivo en la que se almacenarán los archivos de copia de seguridad en el servidor remoto.

Procedimiento

- 1 En el símbolo de la línea de comandos, inicie sesión con privilegios de administrador en el host de la CLI de NSX Intelligence.

```
$ ssh admin@dirección-ip-cli
admin@dirección-ip-cli's password:
```

- 2 Configure el servidor de archivos de copia de seguridad.

La sintaxis del comando es

```
set backup remote-host dirección_host_remoto remote-path ruta_carpeta_remota remote-
host-username usuario_host_remoto remote-host-password contraseña_host_remoto passphrase
frase_contraseña
```

donde *dirección_host_remoto* es la dirección IP del host remoto o la dirección FQDN del servidor de archivos de copia de seguridad, y la cuenta *usuario_host_remoto*

debe tener los privilegios necesarios para crear los archivos de copia de seguridad en *ruta_carpeta_remota*. Debe proporcionar un valor seguro para el parámetro *passphrase*. Este debe tener una longitud mínima de ocho caracteres e incluir al menos una letra mayúscula, una letra minúscula y un carácter especial. Por ejemplo,

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-
password MyRemotePassword passphrase MyPassPhra$e
```

3 Verifique la configuración.

```
get configuration
```

En el resultado, compruebe que la línea con `set backup` sea correcta. Si usamos el ejemplo anterior, el resultado debe incluir la siguiente línea.

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

Realizar una copia de seguridad de NSX Intelligence

Puede realizar una copia de seguridad de los archivos de configuración del dispositivo de NSX Intelligence mediante el comando de la CLI.

Requisitos previos

- Asegúrese de que tiene acceso de administrador a la CLI de NSX Intelligence.
- Configure un servidor de archivos de copia de seguridad. Consulte [Configurar las copias de seguridad de NSX Intelligence](#).

Procedimiento

- 1 Inicie sesión con privilegios de administrador en la CLI de NSX Intelligence.
- 2 Cree la copia de seguridad.

```
backup intelligence configuration
```

Si la copia de seguridad se realiza correctamente, verá un mensaje similar al siguiente.

```
Backup Complete. Archived at: dirección_IP_servidor_archivos_copia_de_seguridad:/root/
backup_archives/intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 Puede consultar el progreso de la copia de seguridad a través de otra sesión de la CLI.
 - a Inicie sesión en otra sesión de la CLI de NSX Intelligence.
 - b Introduzca el siguiente comando.

```
get log-file node-mgmt.log follow
```

Restaurar copias de seguridad de NSX Intelligence

Cuando se restaura una copia de seguridad, se restaura el estado de la configuración de NSX Intelligence en el momento en que se realizó la copia de seguridad. Puede restaurar una copia de seguridad de NSX Intelligence mediante el comando de la CLI.

Debe restaurar las copias de seguridad en una instalación del dispositivo de NSX Intelligence que tenga la misma versión que la copia de seguridad que va a restaurar. De forma predeterminada, el archivo de copia de seguridad restaurado es la copia de seguridad generada más recientemente. Si va a restaurar una copia de seguridad en un dispositivo de NSX Intelligence instalado recientemente, establezca el nombre del archivo antes de restaurar la copia de seguridad.

Requisitos previos

- Compruebe que tiene las credenciales de inicio de sesión de administrador y la información del host del servidor de archivos de copias de seguridad.
- Asegúrese de que tiene acceso de administrador a la CLI de NSX Intelligence.

Procedimiento

- 1 Inicie sesión con privilegios de administrador en el nuevo servidor de la CLI de NSX Intelligence.
- 2 Configure el servidor remoto en el que se encuentran las copias de seguridad.

La sintaxis del comando es

```
set restore remote-host dirección_IP_servidor_copia_de_seguridad remote-path
ruta_carpeta_remota remote-host-username usuario_host_remoto remote-host-password
contraseña_host_remoto passphrase frase_contraseña
```

donde *dirección_IP_servidor_copia_de_seguridad* es la dirección IP o FQDN del host remoto del servidor de archivos de copia de seguridad y la cuenta *usuario_host_remoto* debe tener los privilegios necesarios para acceder a los archivos de copia de seguridad en *ruta_carpeta_remota*. Por ejemplo,

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-
host-password MyRemotePassword passphrase MyPassPhra$e
```

- 3 Compruebe la configuración de la restauración.

```
get configuration
```

En el resultado, compruebe que la línea con `set restore` sea correcta. Si usamos el ejemplo anterior, el resultado debe incluir la siguiente línea.

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

- 4 Restaure la copia de seguridad con el siguiente comando.

```
restore intelligence configuration
```

Si la restauración se realiza correctamente, verá un mensaje similar al siguiente.

```
NSX Intelligence Restore Complete.
```

- 5 Puede ver el progreso de la restauración de la copia de seguridad mediante otra sesión de CLI.
 - a Inicie sesión en otra sesión de la CLI de NSX Intelligence.
 - b Introduzca el siguiente comando.

```
get log-file node-mgmt.log follow
```

Resolución de problemas de NSX Intelligence

Si el dispositivo de NSX Intelligence deja de responder, o si necesita más detalles sobre un mensaje de error que recibió al utilizar el dispositivo, puede ejecutar comandos específicos para obtener el estado de los servicios de NSX Intelligence.

También puede recopilar paquetes de soporte para ayudar al personal de soporte de VMware en los problemas de depuración que haya podido tener.

Comprobar el estado del dispositivo de NSX Intelligence

Si el dispositivo de NSX Intelligence deja de responder, compruebe el estado de los servicios de NSX Intelligence.

Problema

El dispositivo de NSX Intelligence dejó de responder o se recibió un mensaje de error indicando que el dispositivo no funciona según lo esperado.

Causa

Es posible que uno o varios de los servicios subyacentes de NSX Intelligence se hayan detenido o que no estén en buen estado.

Solución

- 1 Inicie sesión en el host de la CLI del dispositivo de NSX Intelligence utilizando una cuenta con la función Administrador empresarial.

2 Verifique el estado de los servicios de NSX Intelligence con el comando `get services`.

Si todos los servicios de NSX Intelligence funcionan correctamente, verá una salida similar a la del siguiente ejemplo.

```
my_nsx-intel> get services
Service name:      druid
Service state:     running
Coordinator health: good
Broker health:     good
Historical health: good
Overlord health:   good
MiddleManager health: good

Service name:      http
Service state:     running
Session timeout:   1800
Connection timeout: 30
Redirect host:     (not configured)
Client API rate limit: 100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:      kafka
Service state:     running
Service health:    good

Service name:      liagent
Service state:     stopped

Service name:      mgmt-plane-bus
Service state:     stopped

Service name:      node-mgmt
Service state:     running

Service name:      nsx-config
Service state:     running

Service name:      nsx-message-bus
Service state:     stopped

Service name:      nsx-upgrade-agent
Service state:     running

Service name:      ntp
Service state:     running
Start on boot:     True

Service name:      pace-server
Service state:     running

Service name:      postgres
Service state:     running
Service health:    good
```

```

Service name:           processing
Service state:          running

Service name:           snmp
Service state:          stopped
Start on boot:          False

Service name:           spark
Service state:          running
Service health:         good

Service name:           spark-job-scheduler
Service state:          running

Service name:           ssh
Service state:          running
Start on boot:          True

Service name:           syslog
Service state:          running

Service name:           ui-service
Service state:          running

Service name:           zookeeper
Service state:          running
Service health:         good

my_nsx-intel>

```

El estado de actividad un servicio puede ser En ejecución o Detenido. El estado de mantenimiento de un servicio puede ser Bueno o Degradado.

- 3 También puede consultar el archivo `syslog` y buscar la salida del script de comprobación de estado `pace-monitor.sh`, que registra el estado de los servicios de NSX Intelligence en este archivo.

Si todos los servicios están funcionando según lo esperado, se mostrará una salida similar a esta salida de muestra tras ejecutar el comando `get log-file syslog | find pace-monitor`.

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - - "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -   "href": "/"
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -   "rel":
"self"
<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - - "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - -   "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",

```

```

<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - - "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - - "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - - "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -
"druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -
"broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -
"coordinator": "good",
<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - - ],

```

```
<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - - "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED
- Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor
```

Si hay algún problema con uno de los servicios, es posible que se muestre la siguiente línea al ejecutar `get log-file syslog | grep pace-monitor`.

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

4 Si encuentra uno de los siguientes resultados, reinicie el servicio con el comando `restart service service-name`.

- Después de ejecutar el comando `get services`, uno de los servicios muestra `Service state: stopped` o `Service health: degraded`.
- Después de ejecutar el comando `get log-file syslog | grep pace-monitor`, la salida mostrará algo similar al mensaje `PACE health DEGRADED. Return code not HTTP OK..`

Por ejemplo, si el estado del servicio `postgres` es `Detenido`, o si es `En ejecución` pero con el estado de mantenimiento `Degradado`, ejecute el siguiente comando.

```
restart service postgres
```

Importante Debe usar el comando `restart service service-name` para reiniciar los servicios de NSX Intelligence. Si, en su lugar, decide utilizar los comandos `stop service service-name` y `start service service-name`, también tendrá que reiniciar manualmente cada uno de los servicios que dependan de *service-name*. La siguiente lista muestra el orden de dependencia en el que se deben reiniciar los servicios de NSX Intelligence.

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-server
```

Por ejemplo, si el servicio `nsx-config` se detiene y se inicia posteriormente con el comando `stop|start service service-name`, también deberá utilizar el comando `restart service service-name` para reiniciar los servicios `processing` y `pace-server`.

Asimismo, si utiliza el comando `restart service service-name` para reiniciar cualquier servicio incluido en la lista de orden de dependencia antes que el servicio `spark-job-scheduler`, también deberá reiniciar manualmente el servicio `spark-job-scheduler` con el comando `restart service spark-job-scheduler`. Si no lo hace, el estado del servicio `spark-job-scheduler` será incorrecto.

Recopilar paquetes de soporte de NSX Intelligence

Puede recopilar un paquete de soporte mediante la CLI de NSX Intelligence.

El contenido del archivo del paquete de soporte no incluye datos. Incluye archivos en los siguientes directorios.

- `/opt/vmware/*`
- `/var/log/*`
- `/etc/*`
- Estado del sistema con `journalctl` y `systemctl`

Requisitos previos

Asegúrese de que tiene acceso de Administrador empresarial a la CLI de NSX Intelligence.

Procedimiento

- 1 Inicie sesión en la CLI de NSX Intelligence utilizando una cuenta con privilegios de la función de Administrador empresarial.

2 Genere el paquete de soporte.

La sintaxis de comandos es la siguiente, en la que deberá indicar el valor de *nombre_archivo_soporte.tgz*.

```
get support-bundle file nombre_archivo_soporte.tgz
```

Por ejemplo,

```
get support-bundle file support_bundle123.tgz
```

Cuando se cree el archivo del paquete, recibirá mensajes similares a los siguientes ejemplos.

```
support_bundle123.tgz created, use the following command to transfer the file: copy
file support_bundle123.tgz url <url> After transferring support_bundle123.tgz, extract it
using:tar xvf support_bundle123.tgz
```

3 Verifique que el paquete de soporte existe con el siguiente comando.

```
get files
```

Se recibe un resultado similar al siguiente.

```
Directory of filestore:/
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```