

Guía para solucionar problemas de NSX

Actualización 8

Modificado el 21 de febrero de 2020

VMware NSX Data Center for vSphere 6.3



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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 © 2010 - 2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

1	Guía para solucionar problemas de NSX	6
	Directrices generales para solucionar problemas	6
	Utilizar el panel de control de NSX	7
	Referencia rápida de línea de comandos de NSX	10
	Comprobación de estado de host de NSX	23
2	Solucionar problemas de la infraestructura de NSX	24
	Preparación del host	24
	Información sobre la arquitectura de preparación de host	30
	Flujo de trabajo de implementación de servicios para la preparación del host	34
	Flujo de trabajo de implementación de servicios de terceros	36
	Comprobar el estado del canal de comunicación	38
	El estado de la instalación es No está listo (Not Ready)	40
	El servicio no responde	40
	No se pueden implementar servicios porque no está disponible OVF/VIB	42
	Problema que la opción Resolver (Resolved) no soluciona	44
	Acerca de vSphere ESX Agent Manager (EAM)	45
	Resolución de problemas de NSX Manager	46
	Conectar NSX Manager a vCenter Server	48
	NSX Manager secundario permanece en modo de tránsito	51
	Errores al configurar el servicio de búsqueda SSO de NSX	52
	Preparación de la red lógica: transporte de VXLAN	54
	La NIC de VMkernel de VXLAN no está sincronizada	57
	Cambio de la directiva de creación de equipos de VXLAN y de la configuración de la MTU	57
	Grupo de puerto del conmutador lógico no sincronizado	60
3	Resolución de problemas de enrutamiento de NSX	61
	Comprender el enrutador lógico distribuido	62
	Flujo de paquete de DLR de alto nivel	63
	Proceso de resolución del ARP de DLR	65
	Comprender el enrutamiento proporcionado por la puerta de enlace de Edge	66
	Flujo de paquete ECMP	67
	Enrutamiento de NSX: requisitos previos y consideraciones	69
	Interfaces de usuario de ESG y DLR	72
	Interfaz de usuario de enrutamiento de NSX	72
	Interfaz de usuario de instancias de NSX Edge	73
	NSX Edge nuevo (DLR)	75
	Diferencias entre ESG y DLR	78

Operaciones habituales de la interfaz de usuario de ESG y DLR	79
Configuración del registro del sistema	79
Rutas estáticas	81
Redistribución de la ruta	81
Resolución de problemas de enrutamiento de NSX	82
CLI del enrutamiento de NSX	82
Resumen breve del enrutamiento	85
Comprobar el estado del DLR mediante una muestra de topología en red	86
DLR y los componentes del host relacionado que están visibles	94
Arquitectura del subsistema de enrutamiento distribuido	96
Componentes del subsistema de enrutamiento de NSX	100
CLI del plano de control del enrutamiento de NSX	103
Efectos y modos de errores del subsistema de enrutamiento de NSX	106
Registros NSX relevantes para el enrutamiento	110
Correcciones y escenarios de errores comunes	112
Obtener datos para solucionar problemas	113
4 Solucionar problemas de NSX Edge	117
Problemas en la colocación de paquetes del firewall	121
Problemas de conectividad en red de Edge	126
Problemas de comunicación de NSX Manager y Edge	128
Depuración de mensajería bus	128
Diagnóstico y recuperación de Edge	130
5 Solución de problemas del firewall	133
Acerca de Distributed Firewall	133
Comandos de la CLI para DFW	134
Resolución de problemas de distributed firewall	137
Firewall de identidad	143
6 Solucionar problemas del equilibrio de carga	147
Escenario: configurar un equilibrador de carga one-armed	147
Diagrama de flujo de solución de problemas del equilibrador de carga	153
Verificación de configuración del equilibrador de carga y solución de problemas a través de la interfaz de usuario	154
Resolución de problemas del equilibrador de carga a través de la CLI	165
Problemas frecuentes del equilibrador de carga	176
7 Resolución de problemas de redes privadas virtuales (VPN)	181
VPN de Capa 2	181
Problemas frecuentes relacionados con la configuración de la VPN de Capa 2	181
Opciones de VPN de Capa 2 para mitigar los bucles	184

Solución de problemas a través de la CLI	186
SSL VPN	188
El portal web SSL VPN no se abre	188
SSL VPN-Plus: errores de instalación	189
SSL VPN-Plus: problemas de comunicación	192
SSL VPN-Plus: problemas de autenticación	196
El cliente SSL VPN-Plus deja de responder	196
Análisis de registro básico	197
IPsec VPN	198
Negociación correcta (Fase 1 y Fase 2)	198
No coincide la directiva de Fase 1	199
No coincide la Fase 2	200
Falta de coincidencia con PFS	201
No coincide con PSK	202
Captura de paquetes para una negociación correcta	203
8 Resolución de problemas relacionados con NSX Controller	209
Comprender la arquitectura del clúster de controladores	209
Problemas de implementación de NSX Controller	212
Resolución de problemas de latencia del disco	217
Ver alertas de latencia del disco	217
Problemas de latencia de disco	218
Errores de clústeres de NSX Controller	220
Método 1: Eliminar el controlador dañado e implementar un nuevo controlador	222
Método 2: Volver a implementar el clúster de NSX Controller	225
Controlador fantasma	226
NSX Controller está desconectado	228
Problemas del agente de plano de control (netcpa)	229
9 Solucionar problemas de Guest Introspection	233
Arquitectura de Guest Introspection	233
Registros de Guest Introspection	234
Registros del módulo de GI de ESX (MUX)	235
Registros de Thin Agent de GI	238
Registros de SVM y de EPSecLib de GI	240
Recopilar información de trabajo y del entorno de Guest Introspection	243
Solucionar problemas de Thin Agent en Linux o Windows	244
Solucionar problemas del módulo GI de ESX (MUX)	247
Solucionar problemas de EPSecLib	248

Guía para solucionar problemas de NSX

1

En la *Guía para solucionar problemas de NSX* se describe cómo supervisar y solucionar los problemas del sistema VMware NSX® for vSphere® mediante la interfaz de usuario de NSX Manager, vSphere Web Client y otros componentes de NSX si son necesarios.

Público objetivo

Este manual está destinado a quienes deseen utilizar NSX o solucionar los problemas relacionados en un entorno de VMware vCenter. La información de este manual está escrita para administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos. En este manual se da por sentado que está familiarizado con VMware vSphere, incluidos VMware ESXi, vCenter Server y vSphere Web Client.

Glosario de publicaciones técnicas de VMware

Publicaciones técnicas de VMware proporciona un glosario de términos que podrían resultarle desconocidos. Si desea ver las definiciones de los términos que se utilizan en la documentación técnica de VMware, acceda a la página <http://www.vmware.com/support/pubs>.

Este capítulo incluye los siguientes temas:

- [Directrices generales para solucionar problemas](#)

Directrices generales para solucionar problemas

En este tema se describen las directrices generales que puede seguir para solucionar cualquier problema de NSX for vSphere.

- 1 Acceda al [Utilizar el panel de control de NSX](#) (NSX Dashboard) y consulte si existen errores o advertencias referentes a un componente.
- 2 Acceda a la pestaña **Supervisar** (Monitor) del NSX Manager principal y consulte si existen eventos del sistema activados. Para obtener más información sobre los eventos del sistema y las alarmas, consulte *Eventos del sistema y de registro de NSX*.
- 3 Utilice la API GET `api/2.0/services/systemalarms` para consultar las alarmas del objeto NSX. Para obtener más información sobre la API, consulte la *Guía de NSX API*.
- 4 Solucione el problema como se describe en *Guía para solucionar problemas de NSX*.

- 5 Si el problema no se soluciona, descargue los registros de soporte técnico y póngase en contacto con el soporte de VMware. Consulte [cómo registrar una solicitud de soporte en My VMware](#). Para obtener más información sobre cómo descargar los registros, consulte *Eventos del sistema y de registro de NSX*.

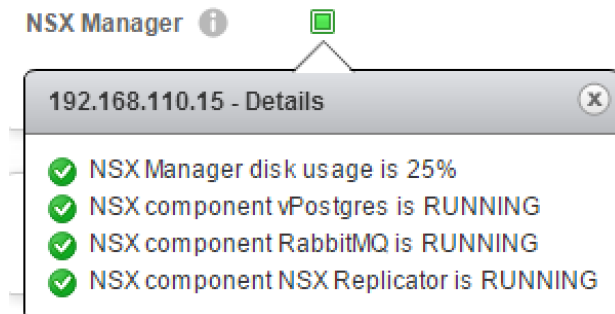
Utilizar el panel de control de NSX

El panel de control de NSX proporciona información sobre el estado general de los componentes de NSX en una vista centralizada. El panel de control de NSX simplifica la solución de problemas al mostrar el estado de diferentes componentes de NSX, como NSX Manager, los conmutadores lógicos, la preparación del host, la implementación del servicio, la copia de seguridad, así como las notificaciones de Edge.

- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Panel de control** (Dashboard). Se muestra la página Panel (Dashboard).
- 3 En un entorno Cross-vCenter NSX, seleccione NSX Manager con la función principal o el secundaria.

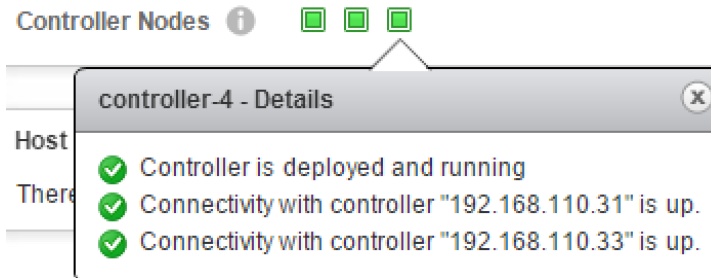
El panel de control proporciona la siguiente información:

- Infraestructura de NSX: se supervisa el estado de los componentes de NSX Manager para los siguientes servicios:
 - Servicio de base de datos (vPostgres).
 - Servicio de bus de mensajería (RabbitMQ).
 - Servicio de replicación: también supervisa los errores de replicación (si se habilita Cross-vCenter NSX).
 - Uso de disco de NSX Manager:
 - El color amarillo indica más del 80 % del disco utilizado.
 - El color rojo indica más del 90 % del disco utilizado.

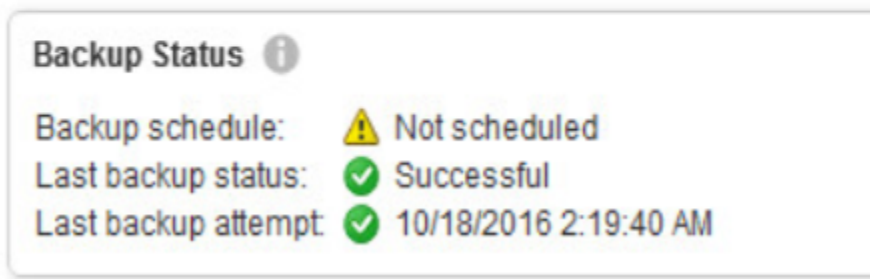
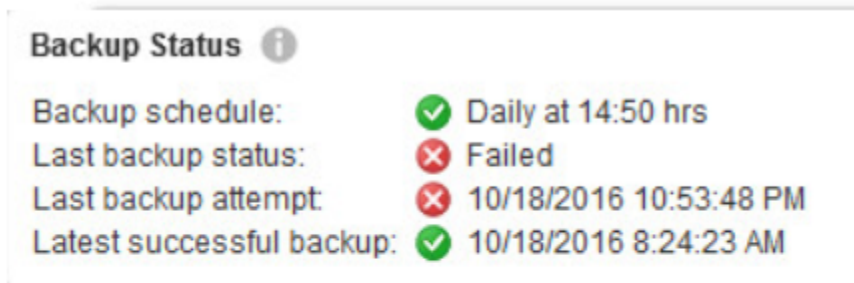


- Infraestructura de NSX: estado de NSX Controller:
 - Estado del nodo del controlador. activo/inactivo/en ejecución/implementando/eliminando/error/desconocido (up/down/running/deploying/removing/failed/unknown).

- Se muestra el estado de conectividad de los controladores en el mismo nivel. Si los controladores están inactivos y aparecen en rojo, los controladores en el mismo nivel aparecen en amarillo.
- Estado de la máquina virtual del controlador (apagada/eliminada) (powered off/deleted).
- Alertas de latencia del disco del controlador.



- Estado de la copia de seguridad de NSX Manager:
 - Programación de copia de seguridad (Backup schedule).
 - Estado de la última copia de seguridad (Last backup status): puede ser Error (Failed), Correcta (Successful) o No programada (Not scheduled) e incluye la fecha.
 - Último intento de copia de seguridad (Last backup attempt), con información sobre la fecha y la hora.
 - Última copia de seguridad correcta (Last successful backup), con información sobre la fecha y la hora.



- Infraestructura de NSX: se supervisa el estado de host para los siguientes servicios:
 - Relacionado con la implementación:
 - Número de clústeres que presentan un estado de error en la instalación.
 - Número de clústeres que necesitan actualizarse.
 - Número de clústeres en los que la instalación está en curso.
 - Número de clústeres no preparados.
 - Firewall:
 - Número de clústeres con el firewall deshabilitado.
 - Número de clústeres en los que el estado del firewall aparece en rojo o amarillo:
 - El color amarillo indica que el firewall distribuido está deshabilitado en algún clúster.
 - El color rojo indica que el firewall distribuido no pudo instalarse en algún host o clúster.
 - VXLAN:
 - Número de clústeres en los que VXLAN no se configuró.
 - Número de clústeres en los que el estado de VXLAN aparece en verde, amarillo o rojo:
 - El color verde indica que la función se configuró correctamente.
 - El color amarillo indica un estado ocupado cuando la configuración VXLAN está en curso.
 - El rojo (error) indica, por ejemplo, un estado en el que se produjo un error de creación de VTEP, que VTEP no encontró la dirección IP o que se le asignó la dirección IP *LinkLocal*.
- Infraestructura de NSX: estado de implementación de servicios
 - Errores de implementación: estado de instalación de los errores de implementación.
 - Estado de servicio: se aplica a todos los servicios con error.
- Infraestructura de NSX: notificaciones de NSX Edge

El panel de control de notificaciones de Edge destaca las alarmas activas de determinados servicios. Supervisa una lista de eventos críticos que se incluyen a continuación y realiza un seguimiento de estos hasta que el problema está sin resolver. Las alarmas se resuelven automáticamente cuando se informa del evento de recuperación, o bien Edge se actualiza, se vuelve a implementar o se fuerza su sincronización.

 - Equilibrador de carga (estado del servidor del equilibrador de carga de Edge):
 - El servidor backend del equilibrador de carga de Edge está inactivo.
 - Estado de advertencia del servidor backend del equilibrador de carga de Edge.
 - VPN (estado del canal de IPSec o del túnel de IPSec):
 - El canal de IPSec de Edge está inactivo.

- El túnel de IPSec de Edge está inactivo.
- Dispositivo (máquina virtual de Edge, puerta de enlace de Edge, sistema de archivos de Edge, NSX Manager y estados de informes de puerta de enlace de servicios de Edge):
 - Falta el pulso de la comprobación de estado de la puerta de enlace de servicios de Edge.
 - Se desconectó la máquina virtual de Edge.
 - Falta el pulso de la comprobación de estado de la máquina virtual de Edge.
 - El estado de NSX Edge no es correcto.
 - NSX Manager notifica que el estado de la puerta de enlace de servicios de Edge no es correcto.
 - La máquina virtual de Edge no aparece en el inventario de VC.
 - Se detectó una situación de cerebro dividido de alta disponibilidad.

Nota Las alarmas de VPN y del equilibrador de carga no se eliminan automáticamente al actualizar la configuración. Una vez que se soluciona el problema, debe eliminarlas manualmente con una API utilizando el comando `alarm-id`. A continuación se muestra un ejemplo de API que puede utilizar para borrar las alarmas. Para obtener más información, consulte la *Guía de NSX API*.

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

- Servicios de NSX: estado de publicación del firewall:
 - Número de hosts en los que el estado de publicación del firewall aparece con errores. El estado aparece en rojo cuando un host no se aplica de forma correcta la configuración del firewall distribuido publicado.
- Servicios de NSX: estado de la red lógica:
 - Número de conmutadores lógicos en los que aparece el estado Error (Error) o Advertencia (Warning).
 - Indica si el grupo de puertos virtuales distribuidos admitidos se elimina de vCenter Server.

Referencia rápida de línea de comandos de NSX

Puede utilizar la interfaz de línea de comandos (CLI) de NSX para solucionar problemas.

Tabla 1-1. Comprobar la instalación de NSX en el host ESXi: ejecutar comandos desde NSX Manager

Descripción	Comandos de NSX Manager	Notas
Lista de todos los clústeres para obtener sus ID.	<code>show cluster all</code>	Ver la información completa sobre el clúster
Lista de todos los hosts en el clúster para obtener los ID del host	<code>show cluster clusterID</code>	Ver la lista de los hosts en el clúster, los ID del host y el estado de preparación de la instalación del host
Lista de todas las máquinas virtuales de un host	<code>show host hostID</code>	Consultar información de un host en particular, las máquinas virtuales, los ID de las máquinas virtuales y el estado de energía

Tabla 1-2. Nombres de los VIB y los módulos instalados en los hosts para usarlos en los comandos

Versión de NSX	Versión de ESXi	VIB	Módulos
Cualquier versión 6.3.x	5.5	esx-vxlan y esx-vsip	vdl2, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.2 y anteriores	6.0 y posteriores	esx-vxlan y esx-vsip	vdl2, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.3 y posteriores	6.0 y posteriores	esx-nsxv	nsx-vdl2, nsx-vdrb, nsx-vsip, nsx-dvfilter-switch-security, nsx-core, nsx-bfd, nsx-traceflow

Tabla 1-3. Comprobar la instalación de NSX en el host ESXi: ejecutar comandos desde el host

Descripción	Comandos del host	Notas
Los VIB presentes dependen de las versiones de NSX y ESXi. Consulte la tabla <i>Nombres de los VIB y los módulos instalados en los hosts</i> (Names of VIBs and Modules Installed on Hosts) para obtener información sobre los módulos que se deben comprobar durante la instalación.	<code>esxcli software vib get -- vibName <name></code>	Comprueba la versión y la fecha de instalación <code>esxcli software vib list</code> muestra una lista de todos los VIB del sistema
Lista de todos los módulos del sistema cargados actualmente	<code>esxcli system module list</code>	Comando equivalente anterior: <code>vmkload_mod -l grep -E vdl2 vdrb vsip dvfilter-switch-security</code>

Tabla 1-3. Comprobar la instalación de NSX en el host ESXi: ejecutar comandos desde el host (continuación)

Descripción	Comandos del host	Notas
Los módulos presentes dependen de las versiones de NSX y ESXi. Consulte la tabla <i>Nombres de los VIB y los módulos instalados en los hosts</i> (Names of VIBs and Modules Installed on Hosts) para obtener información sobre los módulos que se deben comprobar durante la instalación.	<code>esxcli system module get -m <name></code>	Ejecute los comandos de cada módulo
Dos agentes del ámbito del usuario (UWA): agente de plano de control, agente de firewall	<code>/etc/init.d/vShield-Stateful-Firewall status</code> <code>/etc/init.d/netcpad status</code>	
Comprobar las conexiones de los UWA, puerto 1234 para las controladoras y 5671 para NSX Manager	<code>esxcli network ip connection list grep 1234</code> <code>esxcli network ip connection list grep 5671</code>	Conexión TCP del controlador Conexión TCP de bus de mensajería
Comprobar estado de EAM	vSphere Web Client, consulte Administración > vSphere ESX Agent Manager (Administration > vSphere ESX Agent Manager)	

Tabla 1-4. Comprobar la instalación de NSX en el host ESXi: comandos de la red de hosts

Descripción	Comandos de la red de hosts	Notas
Lista de los NIC/vmnic físicos	<code>esxcli network nic list</code>	Comprueba el tipo de NIC, el tipo de controlador, el estado del vínculo y la MTU
Detalles del NIC físico	<code>esxcli network nic get -n vmnic#</code>	Comprueba las versiones de la controladora y el firmware entre otros detalles
Lista de los NIC vmk con las direcciones IP, MAC y MTU, entre otras	<code>esxcli network ip interface ipv4 get</code>	Para asegurarse de que los VTEP se usan correctamente con las instancias
Detalles de cada NIC vmk, incluida la información vDS	<code>esxcli network ip interface list</code>	Para asegurarse de que los VTEP se usan correctamente con las instancias
Detalle de cada NIC vmk, incluida la información vDS para los vmks de VXLAN	<code>esxcli network ip interface list --netstack=vxlan</code>	Para asegurarse de que los VTEP se usan correctamente con las instancias
Buscar el nombre de VDS asociado al VTEP del host	<code>esxcli network vswitch dvs vmware vxlan list</code>	Para asegurarse de que los VTEP se usan correctamente con las instancias
Hacer ping de VXLAN a la pila TCP/IP dedicada	<code>ping ++netstack=vxlan -I vmk1 x.x.x.x</code>	Para solucionar los problemas de comunicación de VTEP: agregue la opción <code>-d -s 1572</code> para garantizar que la MTU de la red de transporte es adecuada para la VXLAN

Tabla 1-4. Comprobar la instalación de NSX en el host ESXi: comandos de la red de hosts (continuación)

Descripción	Comandos de la red de hosts	Notas
Ver la tabla de enrutamiento de VXLAN a la pila TCP/IP dedicada	<code>esxcli network ip route ipv4 list -N vxlan</code>	Soluciona los problemas de comunicación de VTEP
Ver la tabla de ARP de VXLAN a la pila TCP/IP dedicada	<code>esxcli network ip neighbor list -N vxlan</code>	Soluciona los problemas de comunicación de VTEP

Tabla 1-5. Comprobar la instalación de NSX en el host ESXi: archivos de registro del host

Descripción	Archivo de registro	Notas (Notes)
De NSX Manager	<code>show manager log follow</code>	Sigue los registros de NSX Manager Resulta útil para solucionar problemas en el momento
Cualquier registro relacionado con la instalación en un host	<code>/var/log/esxupdate.log</code>	
Problemas relacionados con el host	<code>/var/log/vmkernel.log</code>	
Informe de disponibilidad, alertas, mensajes y advertencia de VMkernel	<code>/var/log/vmksummary.log</code> <code>/var/log/vmkwarning.log</code>	
Se capturó el error de carga del módulo	<code>/var/log/syslog</code>	Error del controlador IXGBE Los errores de dependencia de los módulos de NSX son indicadores clave
En vCenter, ESX Agente Manager es responsable de las actualizaciones	En los registros de vCenter, <code>eam.log</code>	

Tabla 1-6. Comprobar los conmutadores lógicos: comandos ejecutados desde NSX Manager

Descripción	Comando de NSX Manager	Notas (Notes)
Lista de todos los conmutadores lógicos	<code>show logical-switch list all</code>	Lista de todos los conmutadores lógicos, las UUID que se usen en la API, la zona de transporte y vdnscope

Tabla 1-7. Conmutadores lógicos: comandos ejecutados desde NSX Controller

Descripción	Comandos de Controller	Notas (Notes)
Busca la controladora que es propietaria de VNI	<code>show control-cluster logical-switches vni 5000</code>	Tenga en cuenta la dirección IP de la controladora en la salida y su SSH
Buscar todos los hosts que están conectados a la controladora de este VNI	<code>show control-cluster logical-switch connection-table 5000</code>	La dirección IP de origen de la salida es la interfaz de administración del host y el número de puerto es el puerto de origen de la conexión TCP
Buscar todos los VTEP registrados en el host de este VNI	<code>show control-cluster logical-switches vtep-table 5002</code>	
Lista de direcciones MAC conocidas por las máquinas virtuales de este VNI	<code>show control-cluster logical-switches mac-table 5002</code>	Compruebe que la dirección MAC que está en el VTEP que realiza informes sobre ella

Tabla 1-7. Conmutadores lógicos: comandos ejecutados desde NSX Controller (continuación)

Descripción	Comandos de Controller	Notas (Notes)
Lista sobre la caché de ARP completada por las actualizaciones de IP de las máquinas virtuales	<code>show control-cluster logical-switches arp-table 5002</code>	La caché de ARP caduca en 180 segundos
Para un par específico de host y controladora, busque qué host VNI se unió	<code>show control-cluster logical-switches joined-vnis <host_mgmt_ip></code>	

Tabla 1-8. Conmutadores lógicos: comandos ejecutados desde los hosts

Descripción	Comando de los hosts	Notas (Notes)
Comprobar si la VXLAN del host está sincronizada o no	<code>esxcli network vswitch dvs vmware vxlan get</code>	Muestra el puerto y el estado de sincronización utilizados para la encapsulación
Ver la máquina virtual asociada y el ID del puerto del conmutador local para las capturas de la ruta de datos	<code>net-stats -l</code>	Es una buena manera de obtener el vm switchport de una máquina virtual específica
Comprobar que el módulo kernel vdl2 de VXLAN está cargado	<code>esxcli system module get -m vdl2</code>	Muestra todos los detalles del módulo especificado Comprobar la versión
Comprobar que se instaló la versión correcta de VIB de VXLAN Consulte la tabla <i>Nombres de los VIB y los módulos instalados en los hosts</i> (Names of VIBs and Modules Installed on Hosts) para obtener información sobre los VIB que se deben comprobar durante la instalación.	<code>esxcli software vib get --vibName esx-vxlan</code> <code>esxcli software vib get --vibName esx-nsxv</code>	Muestra todos los detalles del VIB especificado Comprobar la versión y la fecha
Comprobar que el host conoce la existencia de otros hosts en el conmutador lógico	<code>esxcli network vswitch dvs vmware vxlan network vtep list --vxlan-id=5001 --vds-name=Compute_VDS</code>	Muestra la lista de todos los VTEP que este host sabe que sirven de host de vtep 5001
Comprobar que el plano de control está disponible y activo para un conmutador lógico	<code>esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS</code>	Asegura que la conexión de la controladora está disponible y el recuento de Port/Mac coincide con las máquinas virtuales del conmutador lógico de este host
Comprobar que el host conoce las direcciones MAC de todas las máquinas virtuales	<code>esxcli network vswitch dvs vmware vxlan network mac list --vds-name Compute_VDS --vxlan-id=5000</code>	Debe mostrar una lista de todos los MAC para las máquinas virtuales VNI 5000 de este host
Comprobar que el host tiene una entrada ARP local en la caché para las máquinas virtuales remotas	<code>esxcli network vswitch dvs vmware vxlan network arp list --vds-name Compute_VDS --vxlan-id=5000</code>	Comprobar que el host tiene una entrada ARP local en la caché para las máquinas virtuales remotas

Tabla 1-8. Conmutadores lógicos: comandos ejecutados desde los hosts (continuación)

Descripción	Comando de los hosts	Notas (Notes)
Comprobar que la máquina virtual está conectada al conmutador lógico y asignada a una VMKnic local También muestra a qué ID de vmknic está asignado un dvPort de máquina virtual	<code>esxcli network vswitch dvs vmware vxlan network port list --vds-name Compute_VDS --vxlan-id=5000</code>	El vdrport siempre aparecerá en la lista mientras el VNI esté conectado a un router
Ver el ID de vmknic y a qué puerto de conmutador y enlace de descarga está asignado	<code>esxcli network vswitch dvs vmware vxlan vmknic list --vds-name=DSwitch-Res01</code>	

Tabla 1-9. Comprobar conmutadores lógicos: archivos de registro

Descripción	Archivo de registro	Notas (Notes)
Los hosts siempre están conectados a las controladoras que residen en sus VNI	<code>/etc/vmware/netcpa/config-by-vsm.xml</code>	Este archivo siempre debe tener todas las controladoras del entorno en la lista. El archivo <code>config-by-vsm.xml</code> se crea a través del proceso <code>netcpa</code>
NSX Manager inserta el archivo <code>config-by-vsm.xml</code> a través de <code>vsfwd</code> Si el archivo <code>config-by-vsm.xml</code> no es correcto, revise el registro de <code>vsfwd</code>	<code>/var/log/vsfwd.log</code>	Analiza este archivo para buscar errores. Para reiniciar el proceso: <code>/etc/init.d/vShield-Stateful-Firewall stop start</code>
La conexión a la controladora se realiza mediante <code>netcpa</code>	<code>/var/log/netcpa.log</code>	Analiza este archivo para buscar errores.
Los registros del módulo de conmutación lógica están en <code>vmkernel.log</code>	<code>/var/log/vmkernel.log</code>	Comprueba los registros del módulo de conmutación lógica en <code>/var/log/vmkernel.log</code> "con prefijo de VXLAN":

Tabla 1-10. Comprobar la ruta lógica: comandos ejecutados desde NSX Manager

Descripción	Comandos de NSX Manager	Notas
Comandos para ESG	<code>show edge</code>	Los comandos de la CLI para la puerta de enlace de servicios de Edge (ESG) se inician con "show edge"
Comandos para las máquinas virtuales de control de DLR	<code>show edge</code>	Los comandos de CLI para la máquina virtual de control del enrutador lógico distribuido (DLR) se inician con "show edge"
Comandos para DLR	<code>show logical-router</code>	Los comandos de CLI para el enrutador lógico distribuido (DLR) se inician con <code>show logical-router</code>
Lista de todas las instancias de edge	<code>show edge all</code>	Lista de todas las instancias de edge compatibles con la CLI central
Lista de todos los detalles de implementación y servicios de una instancia de edge	<code>show edge edgeID</code>	Ver la información de la puerta de enlace de servicios de Edge

Tabla 1-10. Comprobar la ruta lógica: comandos ejecutados desde NSX Manager (continuación)

Descripción	Comandos de NSX Manager	Notas
Lista de las opciones de comando para las instancias de edge	<code>show edge edgeID ?</code>	Ver detalles como versión, registros, NAT, tabla de enrutamiento, firewall, configuración, interfaz y servicios
Ver los detalles del enrutamiento	<code>show edge edgeID ip ?</code>	Ver la información del enrutamiento, BGP, OSPF y otros detalles
Ver la tabla de enrutamiento	<code>show edge edgeID ip route</code>	Ver la tabla de enrutamiento de Edge
Ver el enrutamiento vecino	<code>show edge edgeID ip ospf neighbor</code>	Ver la relación del enrutamiento vecino
Ver la información de la conectividad de los enrutadores lógicos	<code>show logical-router host hostID connection</code>	Comprobar que el número de LIF conectadas es correcto, que se cumple la directiva de formación de equipos y se usa el vDS apropiado
Lista de todas las instancias de los enrutadores lógicos que se ejecutan en el host	<code>show logical-router host hostID dlr all</code>	Comprobar el número de LIF y rutas La IP de la controladora debe ser la misma en todos los hosts de un router lógico El plano de control debe aparecer activado (Control Plane Active) --breve da una respuesta compacta
Comprobar la tabla de enrutamiento del host	<code>show logical-router host hostID dlr dlrID route</code>	Esta es la tabla de enrutamiento integrada por la controladora en todos los hosts de la zona de transporte Debe ser la misma en todos los hosts Si no aparecen ciertas rutas en algunos hosts, pruebe con el comando de sincronización desde la controladora mencionada anteriormente Las marcas E indican que las rutas se conocen a través de ECMP
Comprobar los LIF para un DLR en el host	<code>show logical-router host hostID dlr dlrID interface (all intName) verbose</code>	La información de LIF se integra en los hosts desde las controladoras Este comando permite asegurar que el host conoce todas los LIF que debe conocer

Tabla 1-11. Comprobar la ruta lógica: comandos ejecutados desde NSX Controller

Descripción	Comandos de NSX Controller	Notas (Notes)
Buscar todas las instancias del router lógico	<code>show control-cluster logical-routers instance all</code>	Debe mostrar una lista de la instancia del router lógico y todos los hosts de la zona de transporte que deben tener aplicada la instancia del router lógico Además, muestra la controladora que trabaja en ese router lógico
Consultar los detalles de todos los enrutadores lógicos	<code>show control-cluster logical-routers instance 0x570d4555</code>	La columna IP muestra la dirección IP de vmk0 de todos los hosts en los que existe este DLR
Ver todas las interfaces CONECTADAS al router lógico	<code>show control-cluster logical-routers interface-summary 0x570d4555</code>	La columna IP muestra la dirección IP de vmk0 de todos los hosts en los que existe este DLR
Consultar todas las rutas que este router lógico conoce	<code>show control-cluster logical-routers routes 0x570d4555</code>	Tenga en cuenta que la columna IP muestra las direcciones IP de vmk0 de todos los hosts en los que existe este DLR
Muestra todas las conexiones de red establecidas, como la salida del estado de red	<code>show network connections of-type tcp</code>	Comprobar si el host en el que está solucionando el problema tiene una conexión netcpa establecida para la controladora
Sincronizar interfaces de la controladora al host	<code>sync control-cluster logical-routers interface-to-host <logical-router-id> <host-ip></code>	Es útil si la nueva interfaz se conectó al router lógico pero no se sincronizó con todos los hosts
Sincronizar las rutas de la controladora al host	<code>sync control-cluster logical-routers route-to-host <logical-router-id> <host-ip></code>	Es útil si faltan ciertas rutas en algunos hosts pero están disponibles en la mayoría de los hosts

Tabla 1-12. Comprobar la ruta lógica: comandos ejecutados desde Edge

Descripción	Comandos de Edge o de la máquina virtual de control del router lógico	Notas (Notes)
Ver la configuración	<code>show configuration <global bgp ospf ...></code>	
Ver las rutas conocidas	<code>show ip route</code>	Compruebe que las tablas de enrutamiento y de reenvío están sincronizadas
Ver la tabla de envío	<code>show ip forwarding</code>	Compruebe que las tablas de enrutamiento y de reenvío están sincronizadas

Tabla 1-12. Comprobar la ruta lógica: comandos ejecutados desde Edge (continuación)

Descripción	Comandos de Edge o de la máquina virtual de control del router lógico	Notas (Notes)
Ver las interfaces del enrutador lógico distribuido	<code>show interface</code>	<p>El primer NIC que se muestra en la salida es la interfaz del enrutador lógico distribuido</p> <p>La interfaz del enrutador lógico distribuido no es un vNIC real de dicha máquina virtual</p> <p>Todas las subredes conectadas al enrutador lógico distribuido son de tipo INTERNO</p>
Ver otras interfaces (administración)	<code>show interface</code>	<p>La interfaz de HA o de administración es un vNIC real de la máquina virtual de control del router lógico</p> <p>Si se habilitó HA sin especificar una dirección IP, se usa 169.254.x.x/ 30.</p> <p>Si en la interfaz de administración se proporciona una dirección IP, aparece aquí</p>
depurar el protocolo	<code>debug ip ospf</code> <code>debug ip bgp</code>	<p>Es útil para detectar problemas de configuración (como áreas OSPF que no coinciden, temporizadores y ASN erróneo)</p> <p>Nota: la salida solo se ve en la consola de Edge (no a través de la sesión SSH)</p>
Comandos OSPF	<code>show configuration ospf</code> <code>show ip ospf interface</code> <code>show ip ospf neighbor</code> <code>show ip route ospf</code> <code>show ip ospf database</code> <code>show tech-support</code> (y buscar las cadenas "EXCEPCIÓN" (EXCEPTION) y "PROBLEMA" (PROBLEM))	
Comandos BGP	<code>show configuration bgp</code> <code>show ip bgp neighbor</code> <code>show ip bgp</code> <code>show ip route bgp</code> <code>show ip forwarding</code> <code>show tech-support</code> (buscar las cadenas "EXCEPCIÓN" (EXCEPTION) y "PROBLEMA" (PROBLEM))	

Tabla 1-13. Comprobar rutas lógicas: archivos de registro desde los hosts

Descripción	Archivo de registro	Notas (Notes)
La información de la instancia del enrutador lógico distribuido llega a los hosts mediante envío push realizado por vsfwd y se guarda en formato XML	/etc/vmware/netcpa/config-by-vsm.xml	Si falta alguna instancia del enrutador lógico distribuido en el host, en primer lugar busque en este archivo para ver si la instancia está en la lista Si no, reinicie vsfwd Utilice también este archivo para asegurarse de que el host conoce todas las controladoras
NSX Manager realiza un envío push del archivo anterior a través vsfwd Si el archivo config-by-vsm.xml no es correcto, revise el registro de vsfwd	/var/log/vsfwd.log	Analiza este archivo para buscar errores. Para reiniciar el proceso: /etc/init.d/vShield-Stateful-Firewall stop start
La conexión a la controladora se realiza mediante netcpa	/var/log/netcpa.log	Analiza este archivo para buscar errores.
Los registros del módulo de conmutación lógica están en vmkernel.log	/var/log/vmkernel.log	Comprueba los registros del módulo de conmutación lógica en /var/log/vmkernel.log "con prefijo de vxlan":

Tabla 1-14. Depuración de controladoras: comandos ejecutados desde NSX Manager

Descripción	Comando (de NSX Manager)	Notas (Notes)
Lista de todas las controladoras con su estado	show controller list all	Muestra la lista de todas las controladoras y su estado de ejecución

Tabla 1-15. Depuración de las controladoras: comandos ejecutados desde NSX Controller

Descripción	Comandos (en Controller)	Notas (Notes)
Comprobar el estado del clúster de la controladora	show control-cluster status	Siempre debe mostrar "Unión completa" (Join complete) y "Conectado al clúster principal" (Connected to Cluster Majority)
Comprobar los estados para los mensajes y las conexiones oscilantes	show control-cluster core stats	El recuento caído no debe cambiar
Ver la actividad del nodo en relación a la unión del clúster inicial o tras el reinicio	show control-cluster history	Resulta perfecto para solucionar problemas sobre uniones de clústeres
Consultar la lista de los nodos del clúster	show control-cluster startup-nodes	Tenga en cuenta que la lista no debe tener SOLO los nodos del clúster activo Debe mostrar una lista de todas las controladoras implementadas actualmente Para utilizar esta lista, se inicia la controladora para que se conecte a otras controladoras del clúster
Muestra todas las conexiones de red establecidas, como la salida del estado de red	show network connections of-type tcp	Comprobar si el host en el que está solucionando el problema tiene una conexión netcpa establecida para la controladora

Tabla 1-15. Depuración de las controladoras: comandos ejecutados desde NSX Controller (continuación)

Descripción	Comandos (en Controller)	Notas (Notes)
Reiniciar el proceso de la controladora	<code>restart controller</code>	Solo reinicia el proceso de la controladora principal Realiza una reconexión forzada al clúster
Reiniciar el nodo de la controladora	<code>restart system</code>	Reinicia la máquina virtual de la controladora

Tabla 1-16. Depuración de la controladora: archivos de registro de NSX Controller

Descripción	Archivo de registro	Notas (Notes)
Ver los reinicios, las uniones recientes y el historial de la controladora entre otros	<code>show control-cluster history</code>	Gran herramienta para solucionar los problemas de las controladoras, especialmente sobre clústeres
Comprobar un disco ralentizado	<code>show log cloudnet/cloudnet_java-zookeeper<timestamp>.log filtered-by fsync</code>	Una forma fiable de comprobar discos ralentizados es buscar mensajes "fsync" en el registro cloudnet_java-zookeeper Si la sincronización tarda más de 1 segundo, ZooKeeper imprime este mensaje e indica que otro recurso más estaba utilizando ese disco en ese mismo momento.
Comprobar un disco ralentizado o que no funciona correctamente	<code>show log syslog filtered-by collectd</code>	Mensajes como "collectd" que se produce en una salida amplia suelen estar relacionados con discos ralentizados o que no funcionan correctamente
Comprobar el uso del espacio en disco	<code>show log syslog filtered-by freespace:</code>	Existe una tarea en segundo plano llamada "espacio libre" que limpia de forma periódica los registros antiguos y otros archivos del disco cuando el uso del espacio alcanza algún umbral. En algunos casos, si el disco es pequeño o se llena muy rápido, verá una gran cantidad de mensajes de espacio libre. Esto puede indicar que el disco está lleno
Buscar miembros del clúster actualmente activos	<code>show log syslog filtered-by Active cluster members</code>	Muestra el id del nodo para los miembros del clúster activos actualmente. Es posible que necesite buscar en registros del sistema antiguos ya que el mensaje no se imprime todo el tiempo.

Tabla 1-16. Depuración de la controladora: archivos de registro de NSX Controller (continuación)

Descripción	Archivo de registro	Notas (Notes)
Ver los registros de las controladoras centrales	<code>show log cloudnet/cloudnet_java-zookeeper.20150703-165223.3702.log</code>	Es posible que existan varios registros de zookeeper, busque en el último archivo con marca de tiempo Este archivo contiene información sobre la elección principal del clúster de la controladora así como otra información relacionada con la naturaleza distribuida de las controladoras
Ver los registros de las controladoras centrales	<code>show log cloudnet/cloudnet_nsx-controller.root.log.INFO.20150703-165223.3668</code>	Registros de funcionamiento de la controladora principal como la creación de LIF, el agente de escucha de la conexión en el puerto 1234 y el particionamiento

Tabla 1-17. Comprobar el firewall distribuido: comandos ejecutados desde NSX Manager

Descripción	Comandos de NSX Manager	Notas
Ver información de las máquinas virtuales	<code>show vm vmID</code>	Detalles como DC, clúster, host, nombre de la máquina virtual, vNIC y dvfilters instalados
Ver la información de un NIC virtual en particular	<code>show vnic icID</code>	Detalles como nombre de VNIC, dirección mac, pg y filtros aplicados
Ver la información completa sobre el clúster	<code>show dfw cluster all</code>	Nombre del clúster, su id, nombre de la base de datos y estado del firewall
Ver la información de un clúster concreto	<code>show dfw cluster clusterID</code>	Nombre del host, su id y el estado de instalación
Ver la información del host relacionado con dfw	<code>show dfw host hostID</code>	Nombre de la máquina virtual, su id y estado de energía
Ver detalles en un dvfilter	<code>show dfw host hostID filter filterID <option></code>	Lista de normas, estados, conjuntos de direcciones, etc. para cada VNIC
Ver la información de DFW de una máquina virtual	<code>show dfw vm vmID</code>	Ver los filtros, el ID de VNIC, el nombre, etc. de una máquina virtual
Ver los detalles de VNIC	<code>show dfw vnic vnicID</code>	Ver el filtro, el grupo de puertos, la dirección MAC, el ID y el nombre de VNIC
Lista de los filtros instalados por vNIC	<code>show dfw host hostID summarize-dvfilter</code>	Buscar la máquina virtual o vNIC que sea de interés y obtener el campo del nombre para usarlo como filtro en los comandos siguientes
Ver las reglas de un filtro o vNIC específico	<code>show dfw host hostID filter filterID rules</code> <code>show dfw vnic vnicID</code>	
Ver detalles de un conjunto de direcciones	<code>show dfw host hostID filter filterID addrsets</code>	Las reglas solo muestran conjuntos de direcciones, este comando se puede utilizar para ampliar una parte de un conjunto de direcciones

Tabla 1-17. Comprobar el firewall distribuido: comandos ejecutados desde NSX Manager (continuación)

Descripción	Comandos de NSX Manager	Notas
Detalles de Spoofguard para vNIC	show dfw host hostID filter filterID spoofguard	Comprobar si SpoofGuard está habilitado y cuál es la IP/MAC actual
Ver detalles de los registros de flujo	show dfw host hostID filter filterID flows	Si está habilitada la supervisión del flujo, el host envía información de flujo periódicamente a NSX Manager Utilice este comando para observar los flujos por vNIC
Ver las estadísticas de cada regla de un vNIC	show dfw host hostID filter filterID stats	Resulta útil para comprobar si las reglas se ejecutan correctamente

Tabla 1-18. Comprobar el firewall distribuido: comandos ejecutados desde los hosts

Descripción	Comandos del host	Notas
Muestra los VIB descargados en el host. Consulte la tabla <i>Nombres de los VIB y los módulos instalados en los hosts</i> (Names of VIBs and Modules Installed on Hosts) para obtener información sobre los VIB que se deben comprobar durante la instalación.	esxcli software vib list grep esx-vsip o esxcli software vib list grep esx-nsxv	Comprueba que se descargó la versión correcta de VIB
Detalles de los módulos del sistema cargados actualmente Consulte la tabla <i>Nombres de los VIB y los módulos instalados en los hosts</i> (Names of VIBs and Modules Installed on Hosts) para obtener información sobre los módulos que se deben comprobar durante la instalación.	esxcli system module get -m vsip o esxcli system module get -m nsx- vsip	Comprueba que el módulo estaba instalado o cargado
Lista de procesos	ps grep vsfwd	Ver si el proceso vsfwd se está ejecutando con varios subprocesos
Comando Daemon	/etc/init.d/vShield-Stateful- Firewall {start stop status restart}	Comprobar si el demonio está en ejecución y reiniciar si es necesario
Ver la conexión de la red	esxcli network ip connection list grep 5671	Comprobar si el host tiene conectividad TCP a NSX Manager

Tabla 1-19. Comprobar el firewall distribuido: archivos de registro de los hosts

Descripción	Registro	Notas (Notes)
Registro del proceso	/var/log/vsfwd.log	El registro demonio vsfwd, útil para procesos vsfwd, conectividad de NSX Manager y solucionar problemas de RabbitMQ
Archivo dedicado a registros de paquetes	/var/log/dfwpktlogs.log	Archivo de registro dedicado a registros de paquetes
Captura de paquetes en el dvfilter	pktpcap-uw --dvfilter nic-1413082-eth0-vmware-sfw.2 -- outfile test.pcap	

Comprobación de estado de host de NSX

Puede comprobar el estado de cada host ESXi desde la CLI central de NSX Manager.

El estado que se notifica puede ser crítico, bueno o malo.

Por ejemplo:

```
nsxmgr> show host host-30 health-status
status: HEALTHY

nsxmgr> show host host-29 health-status
UNHEALTHY, Standard Switch vSwitch1 has no uplinks.
UNHEALTHY, Storage volume datastore1 has no enough free spaces: 19.% free.
status: UNHEALTHY

nsxmgr> show host host-28 health-status
CRITICAL, VXLAN VDS vds-site-a VNI 200000 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 200003 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 5000 multicast addr is not synchronized with VSM: 0.0.0.0.
Status: CRITICAL
```

El comando de comprobación del host se puede invocar también a través de la API de NSX Manager

Solucionar problemas de la infraestructura de NSX

2

La preparación de NSX es un proceso que consta de 4 pasos.

- 1 Conecte NSX Manager a vCenter Server. Hay una relación de uno a uno entre NSX Manager y vCenter Server.
 - a Regístrese en vCenter Server.
- 2 Implemente los NSX Controller (solo se necesitan para los conmutadores lógicos, el enrutamiento distribuido o en el caso de VXLAN en modo de unidifusión o híbrido. Si solo utiliza el firewall distribuido (DFW), los controladores no son obligatorios).
- 3 Preparación del host: instala VIBs para VXLAN, DFW y DLR en todos los hosts del clúster. Configura la infraestructura de mensajes basada en Rabbit MQ. Habilita el firewall. Avisa a las controladoras de que los hosts están listos para NSX.
- 4 Configurar VXLAN y las opciones del grupo de direcciones IP: crea VMKNICs y un grupo de puertos de VTEP en todos los hosts del clúster. Durante este paso, puede establecer la MTU, la directiva de formación de equipos y el ID de VLAN de transporte.

Para obtener más información sobre la instalación y la configuración de cada paso, consulte la *Guía de instalación de NSX* y la *Guía de administración de NSX*.

Este capítulo incluye los siguientes temas:

- [Preparación del host](#)
- [Resolución de problemas de NSX Manager](#)
- [Preparación de la red lógica: transporte de VXLAN](#)
- [Grupo de puerto del conmutador lógico no sincronizado](#)

Preparación del host

vSphere ESX Agent Manager implementa los paquetes de instalación de vSphere (VIB) en hosts ESXi.

Para la implementación en hosts, es necesario que el servidor DNS se configure en los hosts, vCenter Server y NSX Manager. Para la implementación no es necesario reiniciar ningún host ESXi, pero sí es necesario hacerlo para actualizar o eliminar los VIB.

Los VIB se alojan en NSX Manager y también están disponibles en un archivo ZIP.

Se puede acceder al archivo a través de la dirección `https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties`. El archivo ZIP para descargar varía en función de NSX o la versión de ESXi. Por ejemplo, en NSX 6.3.0, los hosts de vSphere 6.0 usan el archivo `https://<NSX-Manager-IP>/bin/vdn/vibs-6.3.0/6.0-númeroCompilación/vxlan.zip`.

```
# 5.5 VDN EAM Info
VDN_VIB_PATH.1=/bin/vdn/vibs-6.3.0/5.5-4744075/vxlan.zip
VDN_VIB_VERSION.1=4744075
VDN_HOST_PRODUCT_LINE.1=embeddedEsx
VDN_HOST_VERSION.1=5.5.*

# 6.0 VDN EAM Info
VDN_VIB_PATH.2=/bin/vdn/vibs-6.3.0/6.0-4744062/vxlan.zip
VDN_VIB_VERSION.2=4744062
VDN_HOST_PRODUCT_LINE.2=embeddedEsx
VDN_HOST_VERSION.2=6.0.*

# 6.5 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.3.0/6.5-4744074/vxlan.zip
VDN_VIB_VERSION.3=4744074
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.5.*

# Single Version associated with all the VIBs pointed by above VDN_VIB_PATH(s)
VDN_VIB_VERSION=6.3.0.4744320

# Legacy vib location. Used by code to discover available legacy vibs.
LEGACY_VDN_VIB_PATH_FS=/common/em/components/vdn/vibs/legacy/
LEGACY_VDN_VIB_PATH_WEB_ROOT=/bin/vdn/vibs/legacy/
```

Los VIB instalados en un host dependen de las versiones de NSX y ESXi:

Versión de ESXi	Versión de NSX	VIB instalados
5.5	Cualquier versión 6.3.x	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.2 o anterior	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.3 o posterior	<ul style="list-style-type: none"> ■ esx-nsxv

Puede consultar los VIB instalados usando el comando `esxcli software vib list`.

```
[root@esx-01a:~] esxcli software vib list | grep -e vsip -e vxlan
esx-vsip                6.0.0-0.0.XXXXXXX    VMware  VMwareCertified
2016-04-20
esx-vxlan                6.0.0-0.0.XXXXXXX    VMware  VMwareCertified
2016-04-20
```

O

```
esxcli software vib list | grep nsxv
esx-nsxv                6.0.0-0.0.XXXXXXX      VMware  VMwareCertified
2017-08-11
```

Problemas frecuentes durante la preparación del host

A continuación le mostramos los problemas más habituales que pueden aparecer durante la preparación de los hosts:

- Se produce un error en EAM al implementar los VIB.
 - Es posible que se deba a que el servidor DNS no está configurado correctamente en los hosts.
 - Es posible que se deba a que un firewall bloquea los puertos necesarios entre ESXi, NSX Manager y vCenter Server.

La mayoría de los problemas se resuelven haciendo clic en la opción **Resolver** (Resolve). Consulte [El estado de la instalación es No está listo \(Not Ready\)](#).

- Ya se instaló un VIB anterior de una versión más antigua. Para solucionar el problema, el usuario debe reiniciar los hosts.
- NSX Manager y vCenter Server experimentan problemas de comunicación. La pestaña **Preparación del host** (Host Preparation) del complemento de redes y seguridad no muestra todos los hosts correctamente:
 - Compruebe si vCenter Server puede enumerar todos los hosts y los clústeres.

Si el problema no se solucionó con la opción **Resolver** (Resolve), consulte [Problema que la opción Resolver \(Resolved\) no soluciona](#).

Resolución de problemas relacionados con la preparación del host (VIB)

- Compruebe el estado del canal de comunicación del host. Consulte [Comprobar el estado del canal de comunicación](#).
- Compruebe si hay errores en vSphere ESX Agent Manager.

Para ello, seleccione **Inicio de vCenter (vCenter home) > Administración (Administration) > Extensiones de vCenter Server (vCenter Server Extensions) > vSphere ESX Agent Manager**.

En vSphere ESX Agent Manager, compruebe el estado de las agencias con el prefijo "VCNS160". Si una agencia tiene un estado incorrecto, selecciónela y consulte sus problemas.

Agency	State	Status	Optimized Deployment
_VCNS_160_Management & Edge Cl...	Enabled	✓ Normal	✓
_VCNS_160_Compute Cluster A_VMwa...	Enabled	⚠ Alert	✓

Issues for the selected agencies

Trigger Time	Agency	Issue	Host	Agent VM
Thu Apr 28 12:03:12 GMT-0...	_VCNS_160_Compute Clu...	Agent VIB module is not installed	esx-01a.corp.local	

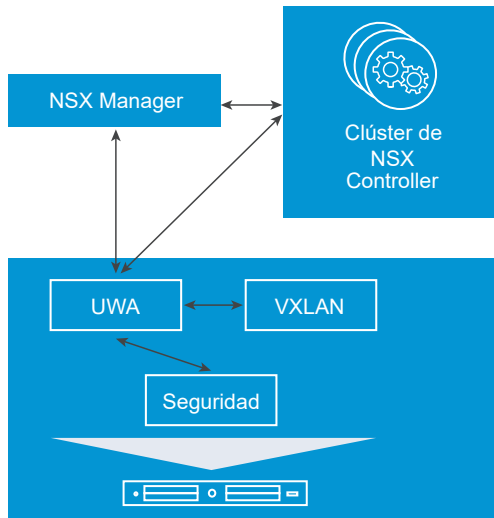
- En el host que presenta un problema, ejecute el comando `tail /var/log/esxupdate.log`.

```
2016-04-28T19:02:52Z esxupdate: downloader: DEBUG: Downloading https://vcsa-01a.corp.local/tmp/tmpKT0wjN...
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: An esxupdate error exception occurred
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: Traceback (most recent call last):
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/usr/sbin/esxupdate.py", line 106, in <module>
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     cmd.Run()
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/external/packages/vmware/esx5update/Cmdline.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/external/packages/vmware/esximage/Transaction.py", line 73, in DownloadMetadata
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: MetadataDownloadError: ('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-2161-fd3f37ad4c', None, "('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-2161-fd3f37ad4c', None, 'Temporary failure in name resolution')")
2016-04-28T19:03:12Z esxupdate: esxupdate: DEBUG: <<<
```

Resolución de problemas relacionados con la preparación del host (UWA)

NSX Manager configura dos agentes del ámbito del usuario en los hosts de un clúster:

- UWA de bus de mensajería (vsfwd)
- UWA del plano de control (netcpa)



En casos excepcionales, los VIB se instalan correctamente, pero por alguna razón uno o ambos agentes del ámbito del usuario no funcionan correctamente. Este error podría manifestarse de las siguientes formas:

- El firewall muestra un estado incorrecto.

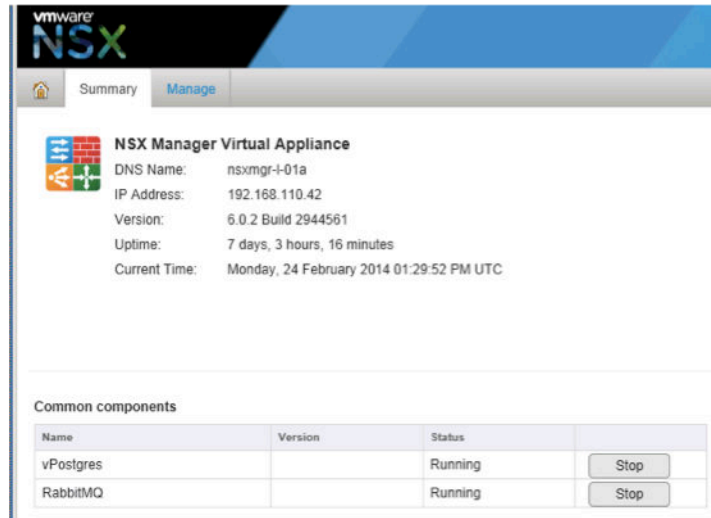
Cluster & Hosts	Installation Status	Firewall
▶ c-1	✓ 5.0 Uninstall	⚠ Error

- El plano de control entre los hipervisores y los controladores no está disponible. Compruebe los eventos del sistema de NSX Manager. Consulte *Eventos del sistema y de registro de NSX*.

Getting Started	Summary	Monitor	Manage
Audit Logs	System Events	Tasks	

Timestamp	Severity	Event Source	Code	Event Message
2/26/2014 10:56:38 AM	Critical	Host messaging infrastructure	391002	Messaging infrastructure down on host.
2/26/2014 10:51:56 AM	Critical	host-22	301502	Spoofguard configuration update number 139340752032...
2/26/2014 10:51:56 AM	Critical	host-20	301502	Spoofguard configuration update number 139340752032...

Si hay más de un host ESXi afectado, compruebe el estado del servicio de bus de mensajería en la pestaña **Resumen** (Summary) de la interfaz de usuario web del dispositivo de NSX Manager. Si RabbitMQ se detiene, reinícielo.



Si el servicio de bus de mensajería está activo en NSX Manager:

- Compruebe el estado del agente del ámbito del usuario del bus de mensajería en los hosts. Para ello, ejecute el comando `/etc/init.d/vShield-Stateful-Firewall status` en los hosts ESXi.

```
[root@esx-01a:~] /etc/init.d/vShield-Stateful-Firewall status
vShield-Stateful-Firewall is running
```

- Compruebe los registros del ámbito del usuario del bus de mensajería en `/var/log/vsfwd.log`.
- Ejecute el comando `esxcfg-advcfg -l | grep Rmq` en los hosts ESXi para mostrar todas las variables Rmq. Debe haber 16 variables Rmq.

```
[root@esx-01a:~] esxcfg-advcfg -l | grep Rmq
/UserVars/RmqIpAddress [String] : Connection info for RMQ Broker
/UserVars/RmqUsername [String] : RMQ Broker Username
/UserVars/RmqPassword [String] : RMQ Broker Password
/UserVars/RmqVHost [String] : RMQ Broker VHost
/UserVars/RmqVsmRequestQueue [String] : RMQ Broker VSM Request Queue
/UserVars/RmqPort [String] : RMQ Broker Port
/UserVars/RmqVsmExchange [String] : RMQ Broker VSM Exchange
/UserVars/RmqClientPeerName [String] : RMQ Broker Client Peer Name
/UserVars/RmqHostId [String] : RMQ Broker Client HostId
/UserVars/RmqHostVer [String] : RMQ Broker Client HostVer
/UserVars/RmqClientId [String] : RMQ Broker Client Id
/UserVars/RmqClientToken [String] : RMQ Broker Client Token
/UserVars/RmqClientRequestQueue [String] : RMQ Broker Client Request Queue
/UserVars/RmqClientResponseQueue [String] : RMQ Broker Client Response Queue
/UserVars/RmqClientExchange [String] : RMQ Broker Client Exchange
/UserVars/RmqSslCertSha1ThumbprintBase64 [String] : RMQ Broker Server Certificate base64 Encoded Sha1 Hash
```

- Ejecute el comando `esxcfg-advcfg -g /UserVars/RmqIpAddress` en los hosts ESXi. El resultado debe mostrar la dirección IP de NSX Manager.

```
[root@esx-01a:~] esxcfg-advcfg -g /UserVars/RmqIpAddress
Value of RmqIpAddress is 192.168.110.15
```

- Ejecute el comando `esxcli network ip connection list | grep 5671` en los hosts ESXi para buscar la conexión activa del bus de mensajería.

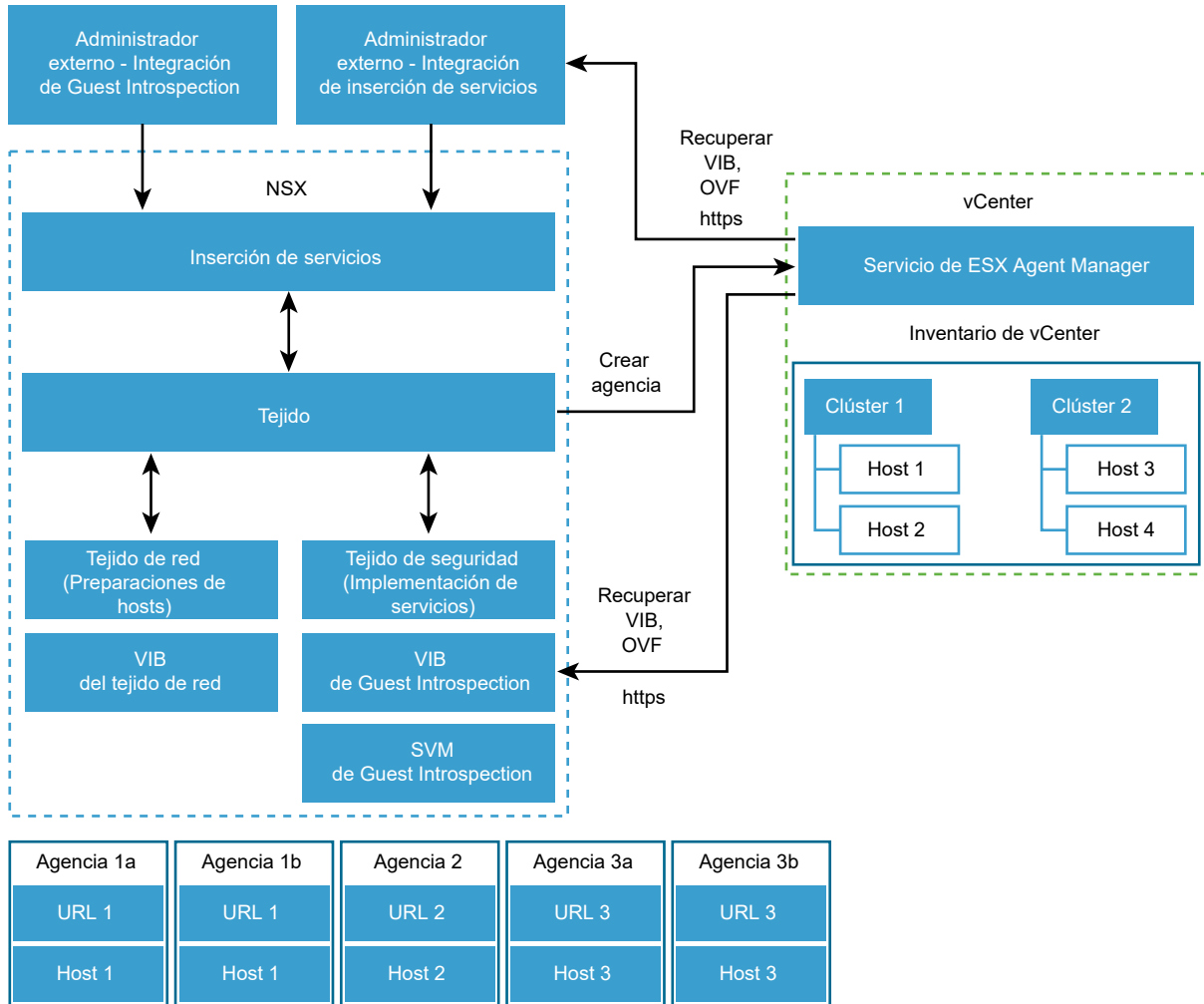
```
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp          0      0 192.168.110.51:29969      192.168.110.15:5671      ESTABLISHED
35505 newreno  vsfwd
tcp          0      0 192.168.110.51:29968      192.168.110.15:5671      ESTABLISHED
35505 newreno  vsfwd
```

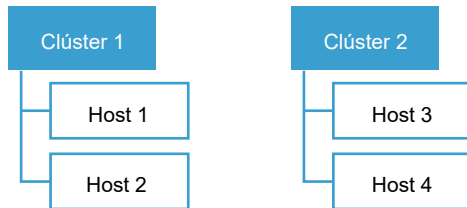
Para consultar los problemas relacionados con el agente del plano de control, consulte [Problemas del agente de plano de control \(netcpa\)](#).

Información sobre la arquitectura de preparación de host

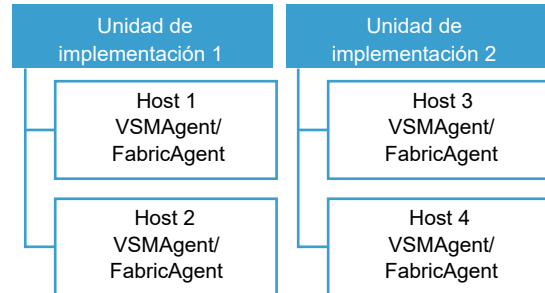
Este tema explica los fundamentos de la arquitectura de preparación de host.

- Para implementar el tejido de red, acceda a la pestaña **Preparación del host** (Host Preparation).
- Para implementar el tejido de seguridad, acceda a la pestaña **Implementación de servicios** (Service Deployment).

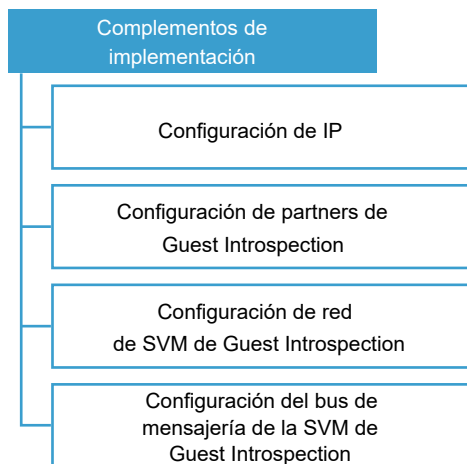




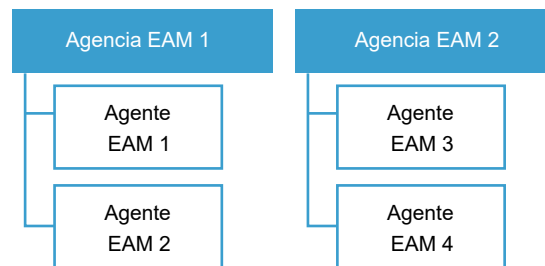
Objeto de NSX



Agente de tejido == VSM Agent



Objeto de vSphere ESXi Agent Manager (EAM)



Agencia 1	Agencia 2	Agencia 3
URL 1	URL 2	URL 3
Clúster 1	Clúster 2	Clúster 3

Agente 1	Agente 2	Agente 3
URL 1	URL 2	URL 3
Host 1	Host 2	Host 3

Los siguientes términos pueden ser útiles para comprender la arquitectura de preparación del host:

Tejido	<p>El tejido es una capa de software de NSX Manager que interactúa con ESX Agent Manager para instalar los servicios de tejidos de redes y seguridad en los hosts.</p>
Tejido de red	<p>Los servicios del tejido de red se implementan en un clúster. Entre los servicios de tejido de red se incluyen la preparación de host, VXLAN, el enrutamiento distribuido, el firewall distribuido y el bus de mensajería.</p>
Tejido de seguridad	<p>Los servicios del tejido de seguridad se implementan en un clúster. Los servicios del tejido de seguridad incluyen Guest Introspection y las soluciones de seguridad de los partners.</p>
Agente de tejido	<p>Un agente de tejido es una combinación de un servicio de tejido y un host en la base de datos de NSX Manager. Se crea una agente de tejido por host para un clúster en el que se implementa un servicio de tejido de redes o seguridad.</p> <p>También se conoce como agente VSM</p>
Unidad de implementación	<p>Una combinación de un servicio de tejido y un clúster en la base de datos de NSX Manager. Se debe crear una unidad de implementación para instalar los servicios de seguridad y de redes.</p>
Agente ESX Agent Manager	<p>Un agente ESX Agent Manager es una combinación de una especificación de servicio y un host de la base de datos de vCenter Server. Se asigna un agente ESX Agent Manager a un agente de tejido de NSX.</p>
Agencia ESX Agent Manager	<p>Una agencia ESX Agent Manager es una combinación de una especificación y un clúster en la base de datos de vCenter Server. La especificación describe agentes de ESX Agent Manager y VIB, OVF y las configuraciones (como la configuración de red y del almacén de datos) que administra.</p> <p>NSX Manager crea una agencia ESX Agent Manager para cada clúster que se preparó.</p> <p>Una agencia ESX Agent Manager se asigna a una unidad de implementación de NSX. La base de datos de NSX Manager de las unidades de implementación y la base de datos de vCenter ESX Agent Manager de las agencias ESX Agent Manager deben estar sincronizadas. En casos excepcionales, si las dos bases de datos no están sincronizadas, NSX activa eventos y alarmas para notificar la condición. NSX Manager crea una unidad de implementación en la base de datos para cada agencia ESX Agent Manager.</p>

NSX Manager crea una agencia ESX Agent Manager para cada clúster que se preparó. NSX Manager crea una unidad de implementación en la base de datos para cada agencia ESX Agent Manager. Una agencia ESX Agent Manager es igual a una unidad de implementación.

Puede consultar las agencias de las siguientes maneras:

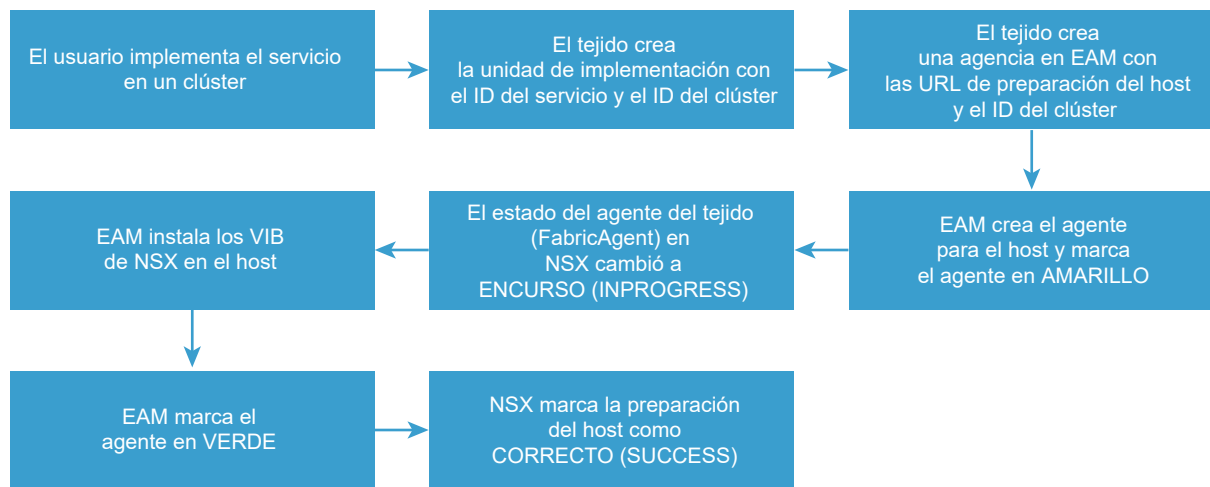
- Desde el MOB de EAM: <https://<nombredehost-VC/IP>/eam/mob/>.
- Desde vSphere Web Client:
 - Acceda a **vCenter Solutions Manager > vSphere ESX Agent Manager > Administrar (Manage)**.
 - En **Agencias de ESX** (ESX Agencies), puede consultar las agencias (una por clúster preparado para un host).

El ciclo de vida de una unidad de implementación está ligado al de la agencia y la eliminación de una agencia de ESX Agent Manager provoca la eliminación de la unidad de implementación correspondiente de NSX.

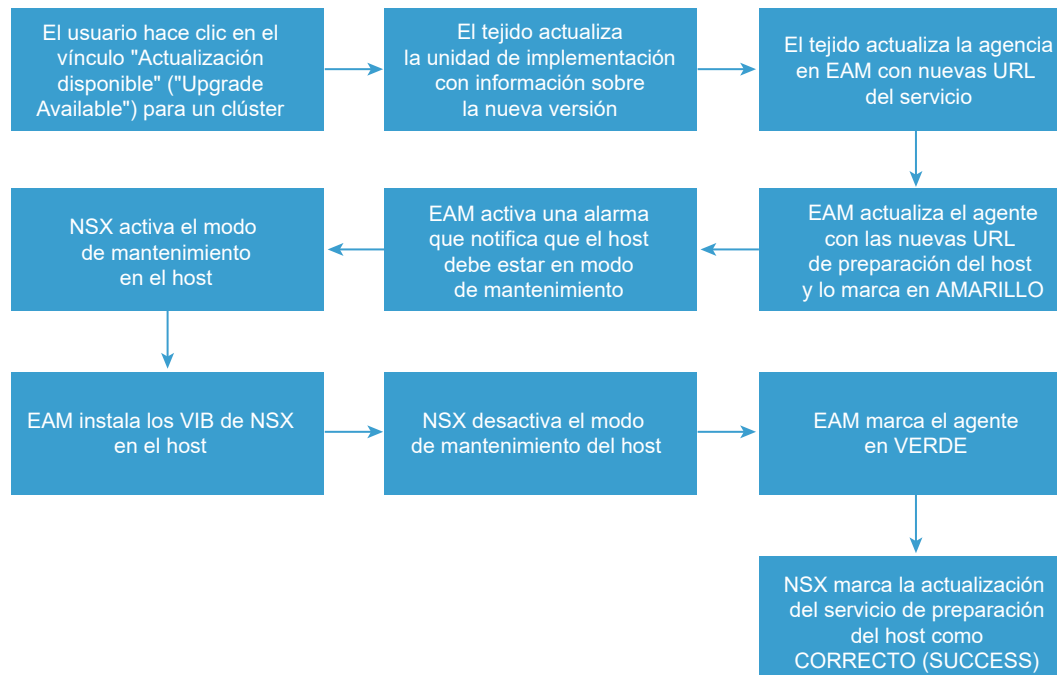
Flujo de trabajo de implementación de servicios para la preparación del host

En este tema se muestra el flujo de trabajo de implementación de servicios (instalación y actualización) para la preparación del host.

Flujo de trabajo de instalación



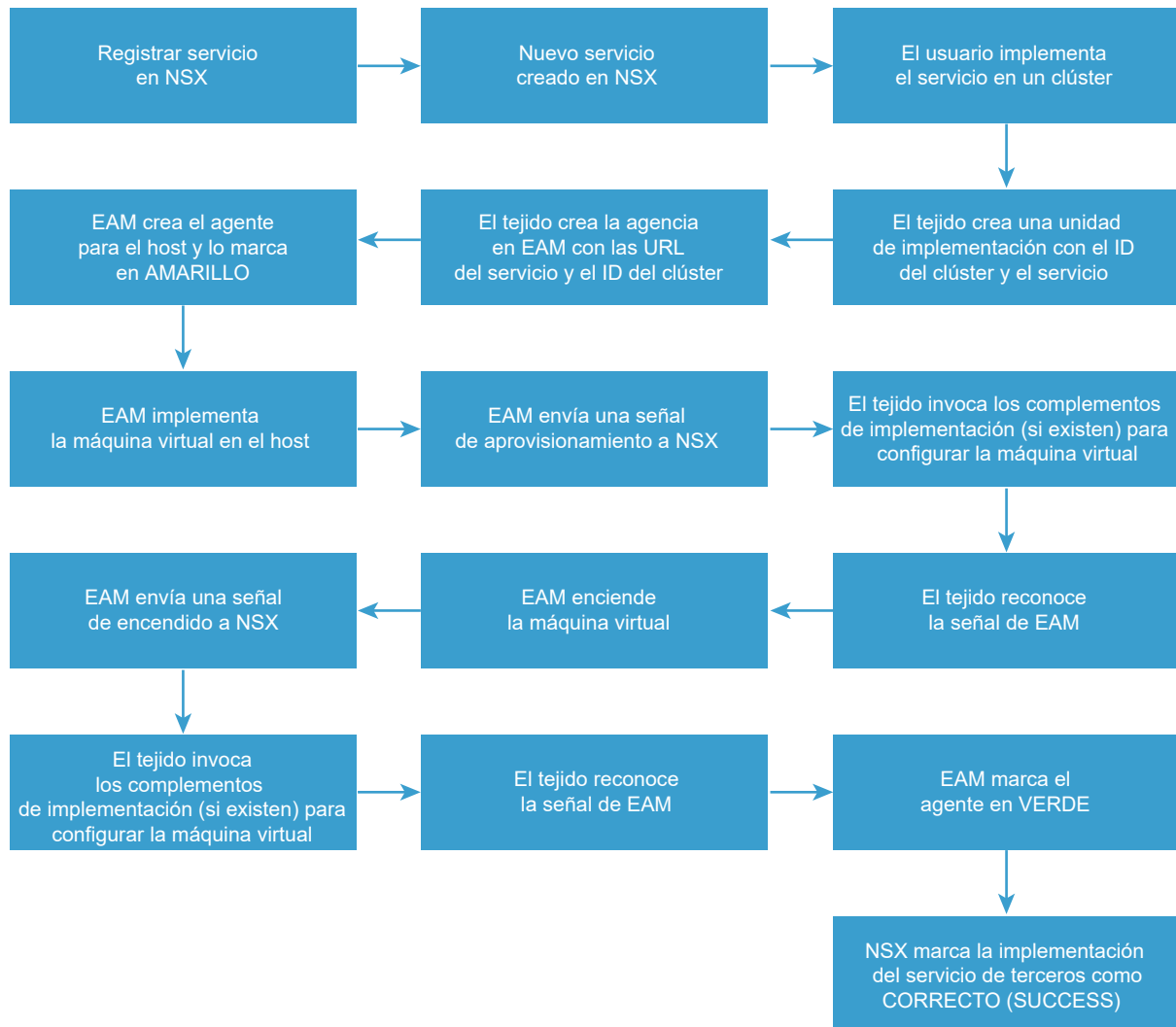
Flujo de trabajo de actualización



Flujo de trabajo de implementación de servicios de terceros

En este tema se muestra el flujo de trabajo de implementación de servicios (instalación y actualización) para servicios de terceros.

Flujo de trabajo de instalación




Flujo de trabajo de actualización



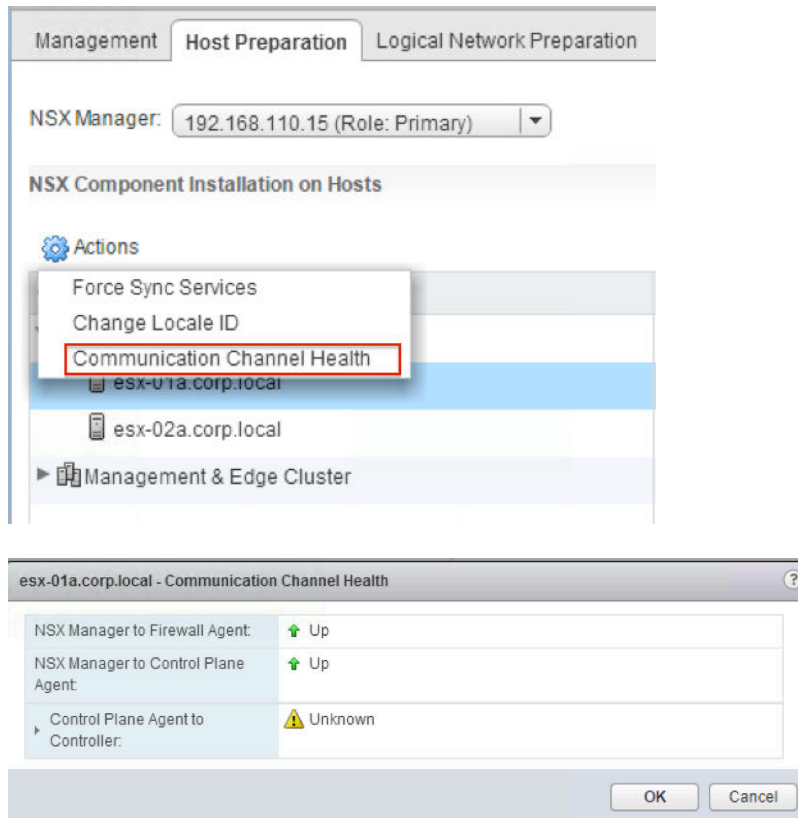
Comprobar el estado del canal de comunicación

Desde vSphere Web Client puede comprobar el estado de comunicación entre varios componentes.

Para comprobar el estado del canal de comunicación entre NSX Manager y el agente de firewall, entre NSX Manager y el agente de plano de control y entre el agente de plano de control y los controladores, realice los pasos siguientes:

- 1 En vSphere Web Client, desplácese a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)**.
- 2 Seleccione o expanda un clúster y seleccione un host. Haga clic en **Acciones (Actions)**  y seleccione **Estado de canal de comunicación (Communication Channel Health)**.

Se mostrará información sobre el estado del canal de comunicación.



Si cambia el estado de alguna de las tres conexiones de un host, se escribe un mensaje en el registro de NSX Manager. En el mensaje del registro, el estado de la conexión puede ser ACTIVA (UP), INACTIVA (DOWN) o NO_DISPONIBLE (NOT_AVAILABLE) (aparece como Desconocida (Unknown) en vSphere Web Client). Si el estado cambia de ACTIVA (UP) a INACTIVA (DOWN) o NO_DISPONIBLE, se genera un mensaje de advertencia. Por ejemplo:

```
2016-05-23 23:36:34.736 GMT+00:00 WARN TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1941, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: DOWN.
```

Si el estado cambia de INACTIVA (DOWN) o NO_DISPONIBLE a ACTIVA (UP) se generará un mensaje de información similar al mensaje de advertencia. Por ejemplo:

```
2016-05-23 23:55:12.736 GMT+00:00 INFO TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1938, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: UP.
```

Si el canal del plano de control sufre un error de comunicación, se genera un evento de sistema con una de las siguientes razones de error pormenorizadas:

- 1255601: Certificado del host incompleto (Incomplete Host Certificate)
- 1255602: Certificado del controlador incompleto (Incomplete Controller Certificate)
- 1255603: Error del protocolo de enlace SSL (SSL Handshake Failure)

- 1255604: Conexión rechazada (Connection Refused)
- 1255605: Tiempo de espera activo (Keep-alive Timeout)
- 1255606: Excepción de SSL (SSL Exception)
- 1255607: Mensaje incorrecto (Bad Message)
- 1255620: Error desconocido (Unknown Error)

Además, se envían mensajes de latidos desde NSX Manager a los hosts. Se activa una sincronización completa de la configuración si se pierde el latido entre NSX Manager y netcpa.

Para obtener más información sobre cómo descargar los registros, consulte la *Guía de administración de NSX*.

El estado de la instalación es No está listo (Not Ready)

Durante la preparación del host, es posible que el estado del clúster aparezca como No está listo (Not Ready).

Problema

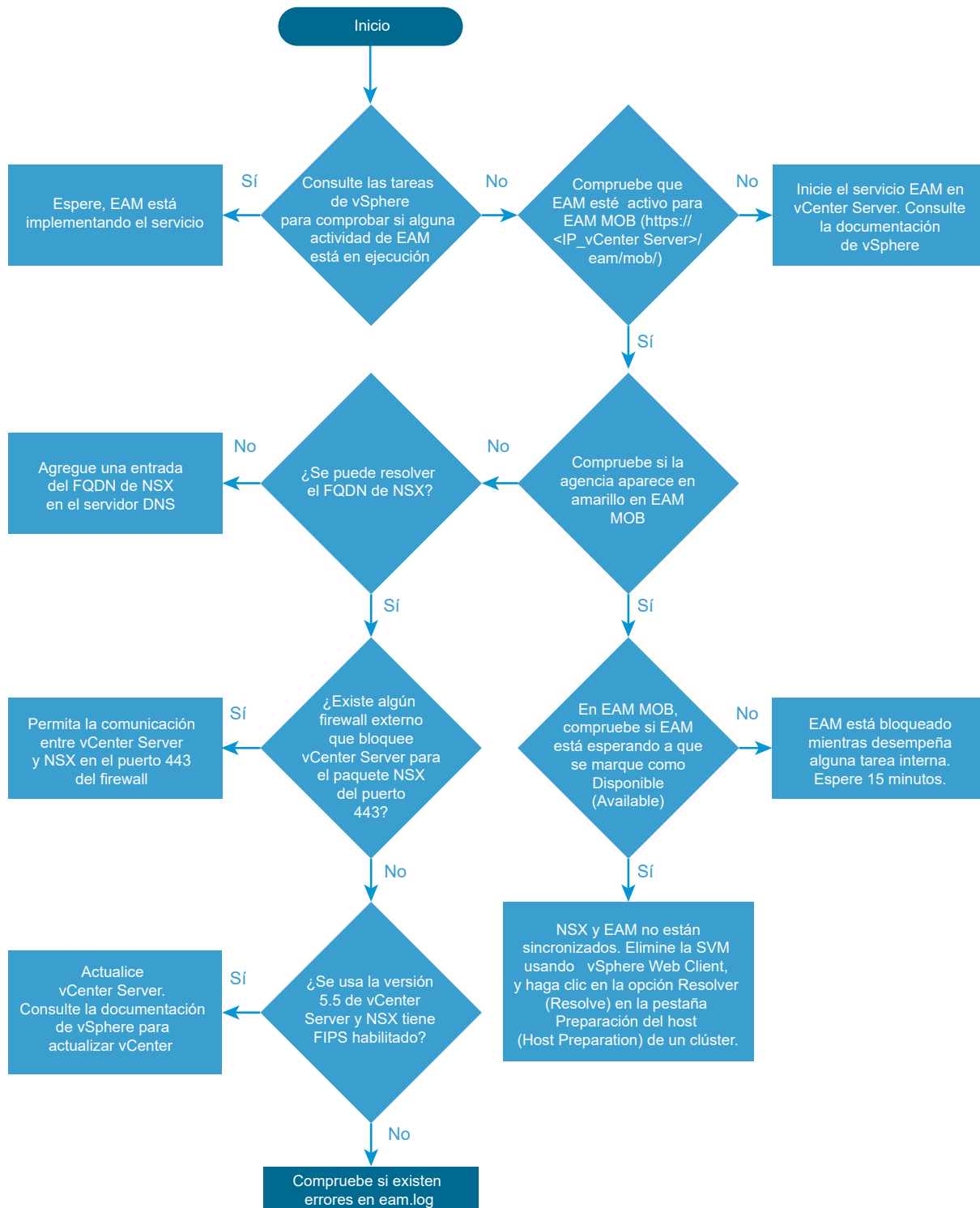
En la pestaña **Preparación del host** (Host Preparation) o en la pestaña **Implementación de servicios** (Service Deployment), el estado de la instalación aparece como No está listo (Not Ready).

Solución

- 1 Acceda a la pestaña **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)** o a la pestaña **Implementación de servicios** (Service Deployment).
- 2 En los clústeres y los hosts, haga clic en No está listo (Not Ready).
Aparece un mensaje de error.
- 3 Haga clic en la opción **Resolver** (Resolve).
Para consultar una lista de problemas resueltos por la opción **Resolver** (Resolve), consulte *Eventos del sistema y de registro de NSX*.
- 4 Si sigue apareciendo No está listo (Not Ready) y no se solucionó el error, consulte [Problema que la opción Resolver \(Resolved\) no soluciona](#).

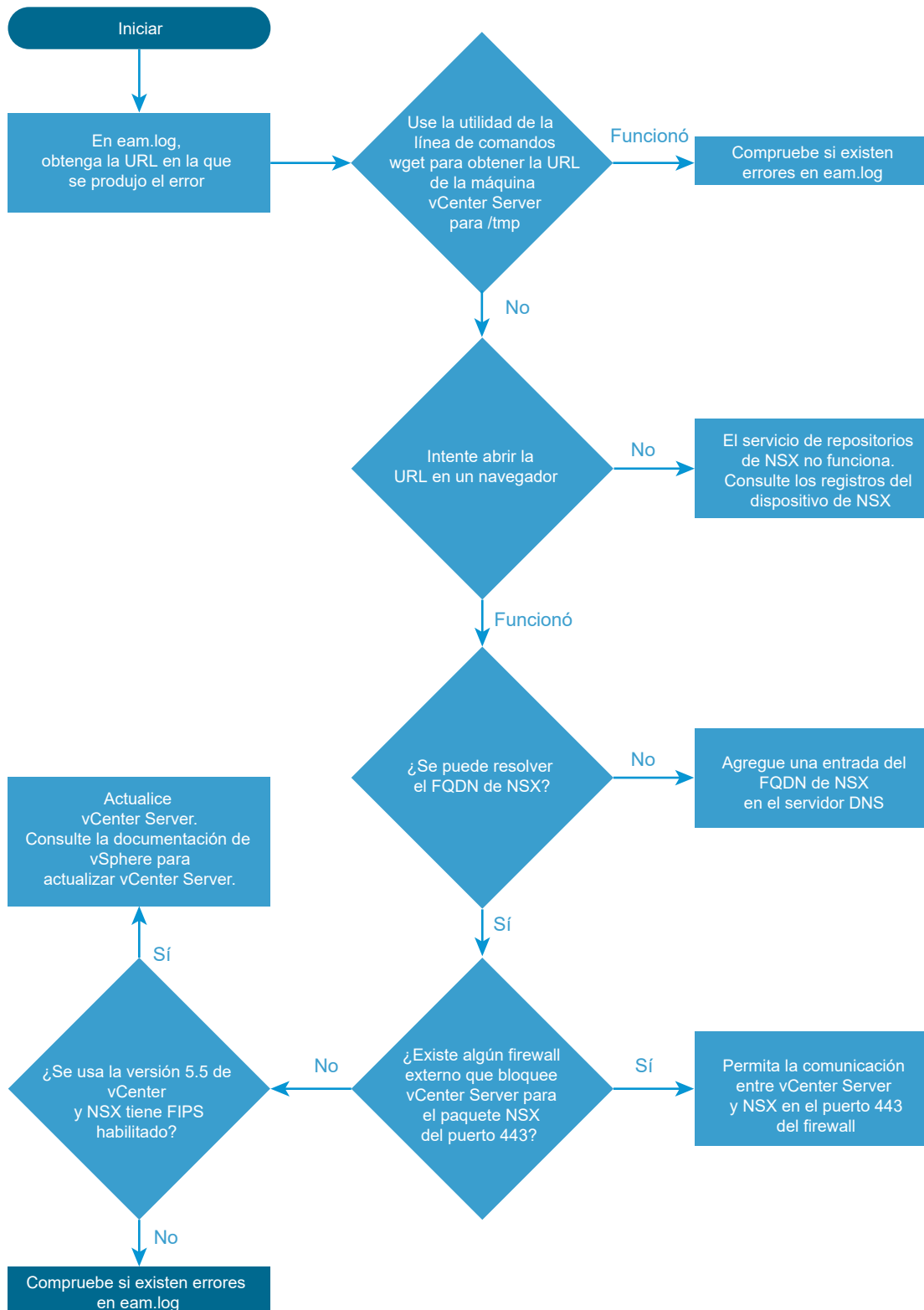
El servicio no responde

El diagrama de flujo ofrece información general del proceso de preparación del host de NSX y qué hacer cuando el servicio no responde o muestra un icono que gira durante mucho tiempo.



No se pueden implementar servicios porque no está disponible OVF/VIB

El diagrama de flujo indica qué hacer cuando no se puede realizar la implementación de servicios por el error OVF/VIB not accessible (OVF/VIB no accesible).



Problema que la opción Resolver (Resolved) no soluciona

En la pestaña **Redes y seguridad (Networking & Security) > Instalación (Installation) > Host Preparation** o en la pestaña **Implementación de servicios (Service Deployment)**, el estado de instalación aparece como No está listo (Not Ready) en los hosts y los clústeres. Al hacer clic en la opción **Resolver** (Resolve) no se soluciona el problema.

Problema

- Al hacer clic en el vínculo No está listo (Not Ready), aparece el error El módulo VIB de los agentes no está instalado en el host (VIB module for agent is not installed on the host).
- El host ESXi no puede acceder a los VIB desde vCenter Server.
- Al cambiar de vShield Endpoint a NSX Manager, es posible que el estado aparezca como Error (Failed).

Solución

- 1 Compruebe que el DNS esté configurado correctamente en vCenter Server, en los hosts ESXi y en NSX Manager. Asegúrese de que la resolución DNS directa e inversa de vCenter Server, los hosts ESXi, NSX Manager y vSphere Update Manager estén funcionando.
- 2 Para determinar si el problema está relacionado con DNS, consulte los registros de *esxupdate* y busque el mensaje "esxupdate: ERROR: MetadataDownloadError:IOError: <urlopen error [Errno -2] Name= or service not known" en el archivo *esxupdate.log*.

Este mensaje indica que el host ESXi no puede acceder al nombre de dominio completo (FQDN) de vCenter Server. Para obtener más información, consulte el [artículo 1008030 de la base de conocimientos de VMware sobre cómo comprobar la dirección IP administrada de VMware vCenter Server](#).
- 3 Compruebe que el protocolo de tiempo de redes (NTP) esté configurado correctamente. VMware recomienda configurar NTP. Para determinar si los problemas de falta de sincronización de NTP afectan al entorno, compruebe el archivo */etc/ntp.drift* en los paquetes de soporte técnico de NSX Manager con la versión 6.2.4 y versiones posteriores.
- 4 Compruebe que ningún firewall bloquee los puertos que NSX for vSphere 6.x necesita. Para obtener más información relacionada, consulte los siguientes artículos de la base de conocimientos:
 - [Requisitos del puerto de red para VMware NSX for vSphere \(2079386\)](#).
 - [Puertos TCP y UDP necesarios para acceder a VMware vCenter Server, host ESXi y ESX de VMware y otros componentes de red \(1012382\)](#).

Nota VMware vSphere 6.x admite las descargas de VIB mediante el puerto 443 (en lugar del puerto 80). Este puerto se abre y se cierra de forma dinámica. Los dispositivos intermedios entre los hosts ESXi y vCenter Server deben permitir que el tráfico use este puerto.

- 5 Compruebe que la dirección IP administrada de vCenter Server esté configurada correctamente. Para obtener más información, consulte el [artículo 1008030 de la base de conocimientos de VMware sobre cómo comprobar la dirección IP administrada de VMware vCenter Server](#).

- 6 Compruebe que vSphere Update Manager esté funcionando correctamente. A partir de vCenter Server 6.0U3, los procedimientos de instalación y actualización de NSX dejan de utilizar vSphere Update Manager con ESX Agent Manager. VMware recomienda ejecutar al menos vCenter Server 6.0U3 o una versión posterior. Si no puede actualizar, asegúrese de que esté ejecutando el servicio vSphere Update Manager. Puede configurar la opción la opción de omisión de vSphere Update Manager, según el artículo [KB 2053782](#).
- 7 Si especifica puertos diferentes a los especificados al implementar vCenter Server, asegúrese de que el firewall del host ESXi no bloquee esos puertos.
- 8 Compruebe que el proceso *vpxd* de vCenter Server escucha el puerto TCP 8089. NSX Manager solo admite el puerto predeterminado 8089.

Acerca de vSphere ESX Agent Manager (EAM)

vSphere Agent Manager automatiza el proceso de implementación y administración de los servicios de redes y seguridad de NSX, mientras aumenta la función de un host ESXi para proporcionar los servicios adicionales que una solución de vSphere necesite.

Registros y servicios de ESX Agent Manager

Los registros de ESX Agent Manager se incluyen como parte del paquete de registros de vCenter.

- Windows—C:\ProgramData\VMware\vCenterServer\logs\eam\eam.log
- VCSA—/var/log/vmware/vpx/eam.log
- ESXi—/var/log/esxupdate.log

Supervisión de ESX Agent Manager

Importante Cambie la marca de *bypassVumEnabled* a **SÍ** (True) antes de comenzar la instalación de NSX y vuelva a cambiarla a **No** (False) tras la instalación. Consulte <https://kb.vmware.com/kb/2053782>.

Para comprobar el estado de ESX Agent Manager:

- 1 Acceda a vSphere Web Client.
- 2 Haga clic en **Administración > Extensiones de vCenter Server** (Administration > vCenter Server Extensions) y, a continuación, en vSphere ESX Agent Manager.
 - a Haga clic en la pestaña **Administrar** (Manage).

La pestaña **Administración** (Manage) muestra información sobre las agencias en ejecución, incluye una lista de los agentes de ESX huérfanos y registra información sobre los agentes de ESX que administra ESX Agent Manager.

Si desea obtener más información sobre los agentes y las agencias, consulte la documentación de vSphere.
 - b Haga clic en la pestaña **Supervisar** (Monitor).

La pestaña **Supervisar > eventos** (Monitor Events) muestra información sobre los eventos asociados con ESX Agent Manager.

Resolución de problemas de NSX Manager

Compruebe que todos los pasos que realiza para solucionar problemas, son adecuados en su entorno. Cada paso proporciona instrucciones para eliminar las posibles causas y realizar las acciones necesarias para corregirlas. Los pasos se ordenan en la secuencia más apropiada para aislar el problema e identificar la solución correcta. No se salte ningún paso.

Problema

- Errores al instalar VMware NSX Manager.
- Errores al actualizar VMware NSX Manager.
- Errores al iniciar sesión en VMware NSX Manager.
- Errores al acceder a VMware NSX Manager.

Solución

- 1 Revise las *notas de la versión de NSX* para comprobar si ya se ha resuelto el error.
- 2 Asegúrese de que se cumplen los requisitos mínimos del sistema cuando instale VMware NSX Manager.

Consulte la *Guía de instalación de NSX*.
- 3 Compruebe que todos los puertos necesarios están abiertos en NSX Manager.

Consulte la *Guía de instalación de NSX*.
- 4 Problemas de instalación:
 - Si se produce un error al configurar el servicio de búsqueda o vCenter Server, compruebe que los dispositivos Lookup Service y NSX Manager cuentan con sincronización de hora. Utilice las mismas configuraciones del servidor NTP tanto en NSX Manager como en Lookup Service. Asegúrese también de que DNS está configurado correctamente.
 - Compruebe que el archivo OVA se está instalando correctamente. Si un archivo OVA de NSX no se puede instalar, aparecerá una ventana de error en el cliente vSphere que indicará dónde se produjo el fallo. Compruebe y valide también las sumas de comprobación de MD5 del archivo OVA/OVF descargado.
 - Compruebe que la hora de los posibles hosts ESXi está sincronizada con NSX Manager.
 - VMware recomienda programar una copia de seguridad de los datos de NSX Manager inmediatamente después de instalar NSX Manager.
- 5 Problemas de actualización:
 - Antes de la actualización, compruebe la información de interoperabilidad más reciente en la página Matrices de interoperabilidad del producto (Product Interoperability Matrixes).

- VMware le recomienda que realice una copia de seguridad de su configuración actual y descargue los registros de soporte técnico antes de realizar la actualización.
- Es posible que sea necesario una resincronización forzada con el vCenter Server tras la actualización de NSX Manager. Para hacer esto, inicie sesión en la interfaz gráfica de usuario web de NSX Manager. Acceda a continuación a **Administrar registro de vCenter > Servicio de gestión de NSX > Editar** (Manage vCenter Registration > NSX Management Service > Edit) y vuelva a introducir la contraseña del usuario administrativo.

6 Problemas del rendimiento:

- Asegúrese de que se cumplan los requisitos mínimos de vCPU.
- Compruebe que la partición raíz (/) cuenta con el espacio adecuado. Puede comprobarlo si inicia sesión en el host ESXi y escribe este comando `df -h`.

Por ejemplo:

```
[root@esx-01a:~] df -h
Filesystem      Size  Used Available Use% Mounted on
NFS             111.4G  80.8G   30.5G    73% /vmfs/volumes/ds-site-a-nfs01
vfat            249.7M 172.2M   77.5M    69% /vmfs/volumes/68cb5875-d887b9c6-a805-65901f83f3d4
vfat            249.7M 167.7M   82.0M    67% /vmfs/volumes/fe84b77a-b2a8860f-38cf-168d5dfe66a5
vfat            285.8M 206.3M   79.6M    72% /vmfs/volumes/54de790f-05f8a633-2ad8-00505603302a
```

- Mediante el comando `esxtop`, compruebe qué procesos están utilizando gran cantidad de CPU y de memoria.
- Si NSX Manager encuentra algún error de memoria insuficiente en los registros, compruebe que existe el archivo `/common/dumps/java.hprof`. Si existe, cree una copia de este archivo e inclúyalo en el paquete de registro de soporte técnico de NSX (NSX Tech Support Log).
- Compruebe que no haya problemas de latencia del almacenamiento en el entorno.
- Intente migrar NSX Manager a otro host ESXi.

7 Problemas de conectividad:

- Si NSX Manager tiene problemas de conectividad tanto con vCenter Server como con el host ESXi, inicie sesión en la consola de la interfaz de línea (CLI) de NSX Manager, ejecute el comando `debug connection IP_of_ESXi_or_VC` y revise los resultados.
- Compruebe que se inició el servicio de administración de Virtual Center Web y que el navegador no está en estado de error.
- Si la interfaz de usuario (UI) web de NSX Manager no está actualizada, puede intentar resolver el problema si deshabilita y vuelve a habilitar los servicios web. Consulte <https://kb.vmware.com/kb/2126701>.
- Compruebe qué grupo de puertos y NIC de enlace de subida utiliza NSX Manager ejecutando el comando `esxtop` en el host ESXi. Para obtener más información, consulte <https://kb.vmware.com/kb/1003893>.

- Intente migrar NSX Manager a otro host ESXi.
- Compruebe la pestaña **Tareas y eventos** (Task and Event) del dispositivo de la máquina virtual de NSX Manager desde la pestaña **Supervisar** (Monitor) de vSphere Web Client.
- Si NSX Manager tiene problemas de conectividad con vCenter Server, intente migrar NSX Manager al mismo host ESXi en el que se ejecuta la máquina virtual de vCenter Server para eliminar posibles problemas de redes físicas subyacentes.

Tenga en cuenta que esto solo funciona si ambas máquinas virtuales están en el mismo grupo de puertos o la misma VLAN.

Conectar NSX Manager a vCenter Server

La conexión entre NSX Manager y vCenter Server permite a NSX Manager utilizar vSphere API para llevar a cabo funciones tales como implementar máquinas virtuales de servicios, preparar hosts y crear grupos de puertos de conmutadores lógicos. El proceso de conexión instala un complemento de cliente web para NSX en el servidor de clientes web.

Para que la configuración funcione, debe haber configurado los DNS y NTP en NSX Manager, vCenter Server y hosts ESXi. Si agregó hosts ESXi por nombre al inventario de vSphere, compruebe que los servidores DNS se configuraron en NSX Manager y que la resolución de nombres funciona. De lo contrario, NSX Manager no podrá resolver las direcciones IP. Debe especificar el servidor NTP para que la hora del servidor SSO y la hora de NSX Manager estén sincronizadas. En NSX Manager, el archivo drift de `/etc/ntp.drift` se incluye en el paquete de servicio técnico de NSX Manager.

La cuenta que utiliza para conectar NSX Manager a vCenter Server debe tener la función "Administrador" (Administrator) de vCenter. Esta función permite a NSX Manager registrarse con el servidor del servicio del token de seguridad. Cuando se utiliza la cuenta de un usuario concreto para conectar NSX Manager a vCenter, también se crea en NSX Manager una función "Administrador empresarial" (Enterprise Administrator) para dicho usuario.

Problemas frecuentes al conectar NSX Manager a vCenter Server

- El DNS no está correctamente configurado en NSX Manager, vCenter Server ni host ESXi.
- El NTP no está correctamente configurado en NSX Manager, vCenter Server ni host ESXi.
- Se utilizó una cuenta de usuario sin la función de administrador de vCenter para conectar NSX Manager a vCenter.
- Existen problemas de conectividad entre NSX Manager y vCenter Server.
- El usuario inicia sesión en vCenter con una cuenta que no tiene ninguna función en NSX Manager.

Debe iniciar sesión en vCenter inicialmente con la cuenta que utilizó para vincular NSX Manager a vCenter Server. A continuación podrá crear otros usuarios con funciones en NSX Manager mediante **Inicio > Redes y seguridad > Administradores de NSX > {Administrador de IP o NSX Manager} > Administrar > Usuarios** (Home > Networking & Security > NSX Managers > {IP of NSX Manager} > Manage > Users).

El primer inicio de sesión puede durar hasta 4 minutos mientras vCenter carga e implementa los paquetes de la interfaz de usuario de NSX.

Comprobar la conectividad entre NSX Manager y vCenter Server

- Inicie sesión en la consola de la CLI de NSX Manager.
- Para verificar la conectividad, consulte las tablas de enrutamiento y ARP.

```
nsxmgr# show arp
```

IP address	HW type	Flags	HW address	Mask	Device
192.168.110.31	0x1	0x2	00:50:56:ae:ab:01	*	mgmt
192.168.110.2	0x1	0x2	00:50:56:01:20:a5	*	mgmt
192.168.110.1	0x1	0x2	00:50:56:01:20:a5	*	mgmt
192.168.110.33	0x1	0x2	00:50:56:ae:4f:7c	*	mgmt
192.168.110.32	0x1	0x2	00:50:56:ae:50:bf	*	mgmt
192.168.110.10	0x1	0x2	00:50:56:03:19:4e	*	mgmt
192.168.110.51	0x1	0x2	00:50:56:03:30:2a	*	mgmt
192.168.110.22	0x1	0x2	00:50:56:01:21:f9	*	mgmt
192.168.110.55	0x1	0x2	00:50:56:01:23:21	*	mgmt
192.168.110.26	0x1	0x2	00:50:56:01:21:ef	*	mgmt
192.168.110.54	0x1	0x2	00:50:56:01:22:ef	*	mgmt
192.168.110.52	0x1	0x2	00:50:56:03:30:16	*	mgmt

```
nsxmgr# show ip route
Codes: K - kernel route, C - connected, S - static,
       > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt
```

- Busque errores en el registro de NSX Manager para indicar el motivo por el que no se conecta a vCenter Server. El comando para ver el registro es `show log manager follow`.

```
2014-02-26 12:53:23.815 GMT INFO VcEventsReaderThread DefaultRequestDirector:491 - I/O exception (org.apache.http.NoHttpResponseException: The target server failed to respond)
2014-02-26 12:53:23.815 GMT INFO VcEventsReaderThread DefaultRequestDirector:498 - Retrying request
2014-02-26 12:53:23.815 GMT WARN ViInventoryThread ViInventory:1482 - We received error from VC, probably lost connection
2014-02-26 12:53:23.817 GMT INFO VcEventsReaderThread VcEventsReader$VcEventsReaderThread:347 - Caught exception:com.vmware.vim.vimovm.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to https://vc-1-01a.corp.local refused
2014-02-26 12:53:23.821 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:348 - Caught exception during p
com.vmware.vim.vimovm.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to ht
```

- Ejecute el comando `debug connection IP_of_ESXi_or_VC` y examine el resultado.

Realizar una captura de paquetes en NSX Manager para ver las conexiones

Utilice el comando de paquetes de depuración: `debug packet [capture|display] interface interface filter`

El nombre de la interfaz en NSX Manager es `mgmt`.

La sintaxis del filtro sigue este formato: `"port_80_or_port_443"`

El comando solo se ejecuta en el modo con privilegios. Para habilitar este modo, ejecute el comando `enable` e introduzca la contraseña de administrador.

Ejemplo de captura de paquetes:

```
nsxmgr# en
nsxmgr# debug packet display interface mgmt port_80_or_port_443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on mgmt, link-type EN10MB (Ethernet), capture size 262144 bytes
23:40:25.321085 IP 192.168.210.15.54688 > 192.168.210.22.443: Flags [P.], seq 2645022162:2645022199,
ack 2668322748, win 244, options [nop,nop,TS val 1447550948 ecr 365097421], length 37
...
```

Comprobar la configuración de red en NSX Manager

El comando `show running-config` muestra la configuración básica de la interfaz de administración, el servidor NTP y las opciones de la ruta predeterminada.

```
nsxmgr# show running-config
Building configuration...

Current configuration:
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr
!
interface mgmt
 ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

Certificados de NSX Manager

NSX Manager admite dos formas de generar certificados.

- CSR generadas en NSX Manager: las funciones son limitadas debido a la CSR básica
- PKCS#12: recomendamos esta opción para producción

Hay un problema frecuente por el que CMS silenciosamente no puede realizar llamadas API.

Este problema se produce cuando el emisor del certificado es desconocido para el usuario que realiza la llamada porque es una autoridad de certificación con una raíz que no es de confianza o el certificado está autofirmado. Para solucionar el problema acceda al nombre de host o a la dirección IP de NSX Manager a través de un navegador y acepte el certificado.

NSX Manager secundario permanece en modo de tránsito

Utilice la solución que se indica a continuación si su NSX Manager secundario permanece en modo de tránsito, tal como se describe en el problema. Este problema se produce al restaurar la copia de seguridad en el NSX Manager principal cuando el NSX Manager secundario está en modo de tránsito.

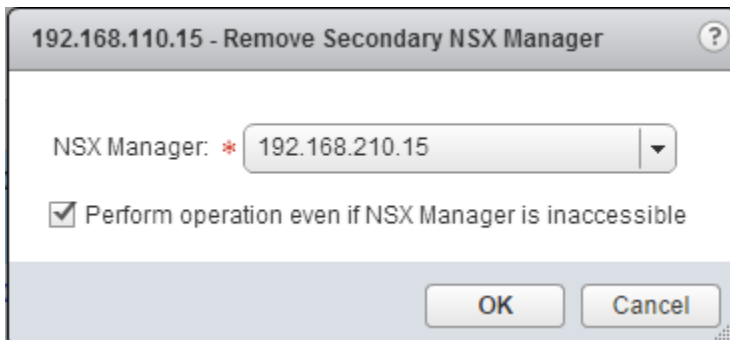
Problema

- 1 Tiene configurados NSX Manager principal y secundario.
- 2 Utiliza la copia de seguridad del NSX Manager principal.
- 3 Después, elimina el NSX Manager secundario. El NSX Manager secundario está en modo de tránsito.
- 4 Por algún motivo, restaura la copia de seguridad en el NSX Manager principal.
- 5 En la base de datos, se actualiza el NSX Manager en tránsito como **Secundario** (Secondary), pero se muestra en la interfaz de usuario como **Tránsito** (Transit) y se produce un error de sincronización.
- 6 Es posible que no pueda eliminar el NSX Manager secundario o utilizarlo de nuevo como secundario.
- 7 Al utilizarlo como NSX Manager en tránsito, aparece un mensaje de error que indica que ya existe el nodo de NSX Manager con esa dirección IP o ese nombre del host.
- 8 Al eliminar el NSX Manager en tránsito, se muestra un mensaje de error que indica que el nombre de usuario o la contraseña son incorrectos.

Solución

- 1 Inicie sesión en vCenter vinculado al NSX Manager primario con vSphere Web Client.
- 2 Acceda a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)** y seleccione la pestaña **Administración (Management)**.
- 3 Seleccione el NSX Manager secundario que quiera eliminar, haga clic en **Acciones (Actions)** y , a continuación, en **Eliminar NSX Manager secundario (Remove Secondary NSX Manager)**.

Se mostrará un cuadro de diálogo de confirmación.



- 4 Marque la casilla **Realizar operación aunque NSX Manager sea inaccesible** (Perform operation even if NSX Manager is inaccessible).

5 Haga clic en **Aceptar** (OK).

Se eliminará el NSX Manager secundario de la base de datos principal.

6 Agregue el NSX Manager secundario de nuevo.

Pasos siguientes

Para obtener más información sobre cómo agregar un NSX Manager secundario, consulte la *Guía de instalación de NSX*.

Errores al configurar el servicio de búsqueda SSO de NSX

Problema

- Errores al registrar NSX Manager en vCenter Server
- Error al configurar el servicio de búsqueda de SSO
- Pueden producirse los siguientes errores:

```
nested exception is java.net.UnknownHostException: vc.local( vc.corp.local )
```

```
NSX Management Service operation failed.( Initialization of Admin Registration Service  
Provider failed. Root Cause: Error occurred while registration of lookup service,  
com.vmware.vim.sso.admin.exception.InternalError: General failure.
```

```
com.vmware.vshield.vsm.security.service.impl.SamlTokenSSOAuthenticator : SSO is not  
configured or initialized properly so cannot authenticate user.
```

Solución

1 Problemas de conectividad:

- Si NSX Manager tiene problemas de conectividad tanto con vCenter Server como con el host ESXi, inicie sesión en la consola de la interfaz de línea (CLI) de NSX Manager, ejecute el siguiente comando: `debug connection IP_of_ESXi_or_VC` y revise los resultados.
- Haga ping desde NSX Manager a vCenter Server con la dirección IP y FQDN para comprobar el enrutamiento, la ruta estática o la ruta predeterminada de NSX Manager con este comando:

```
nsxmgr-l-01a# show ip route
```

Códigos:

K: ruta de kernel

C: conectado

S estático

>: ruta seleccionada

*: Ruta FIB

```
S>* 0.0.0.0/0 [1/0] via 192.168.110.2, mgmt
```

```
C>* 192.168.110.0/24 is directly connected, mgmt
```

2 Problema de DNS

Haga ping desde NSX Manager a vCenter Server con FQDN mediante este comando:

```
nsx-mgr> ping vc-l-01a.corp.local
```

Debería aparecer un resultado similar al siguiente ejemplo:

```
nsx-mgr> ping vc-l-01a.corp.local
PING vc-l-01a.corp.local (192.168.110.51): 56 data bytes
64 bytes from 192.168.110.51: icmp_seq=0 ttl=64 time=1.749 ms
64 bytes from 192.168.110.51: icmp_seq=1 ttl=64 time=2.111 ms
64 bytes from 192.168.110.51: icmp_seq=2 ttl=64 time=8.082 ms
64 bytes from 192.168.110.51: icmp_seq=3 ttl=64 time=2.010 ms
64 bytes from 192.168.110.51: icmp_seq=4 ttl=64 time=0.857 ms
```

Si no funciona, desplácese hasta **Administrar > Red > Servidores DNS** (Manage > Network > DNS Servers) en NSX Manager y asegúrese de que el DNS esté configurado correctamente.

3 Problema de Firewall

Si hay un firewall entre NSX Manager y vCenter Server, compruebe que permita SSL en TCP/443. Además, haga ping para comprobar la conectividad.

4 Compruebe que los siguientes puertos necesarios están abiertos en NSX Manager.

Tabla 2-1. Puertos abiertos de NSX Manager

Puerto	Necesario para
443/TCP	<p>Descargar el archivo OVA en el host ESXI para la implementación</p> <p>Usar las API de REST</p> <p>Usar la interfaz de usuario de NSX Manager</p>
80/TCP	<p>Iniciar la conexión con vSphere SDK</p> <p>Enviar mensajes entre NSX Manager y los módulos del host NSX</p>
1234/TCP	Comunicación entre NSX Controller y NSX Manager
5671	Rabbit MQ (tecnología de mensajería bus)
22/TCP	<p>Acceso de la consola (SSH) a la CLI</p> <p>Nota: Este puerto está cerrado de forma predeterminada</p>

5 Problemas de NTP

Compruebe que vCenter Server y NSX Manager tengan la hora sincronizada. Para lograrlo, utilice las mismas configuraciones del servidor NTP en NSX Manager y vCenter Server.

Para determinar la hora en NSX Manager, ejecute este comando desde la CLI:

```
nsxmgr-l-01a# show clock
```

```
Tue Nov 18 06:51:34 UTC 2014
```

Para determinar la hora en vCenter Server, ejecute este comando en la CLI:

```
vc-l-01a:~ # date
```

Debería aparecer un resultado similar al siguiente:

```
Tue Nov 18 06:51:31 UTC 2014
```

Nota: Después de configurar la hora, reinicie el dispositivo.

6 Problemas de permisos de usuario

Confirme que el usuario tenga privilegios de **administrador**.

Para registrarse en vCenter Server o en el servicio de búsqueda de SSO, debe tener derechos administrativos.

La cuenta predeterminada es `administrator` user: `administrator@vsphere.local`

7 Vuelva a conectarse a SSO introduciendo las credenciales.

Preparación de la red lógica: transporte de VXLAN

NSX prepara la instancia de vSphere Distributed Switch que seleccionó para VXLAN mediante la creación de un grupo de puertos virtuales distribuidos para las NIC de VMkernel de VTEP.

La directiva de formación de equipos, el método de equilibrio de carga, la MTU y el ID de VLAN de los VTEP se seleccionan durante la configuración de VXLAN. Los métodos de equilibrio de carga y formación de equipos deben coincidir con la configuración del DVS seleccionado para la VXLAN.

La MTU debe estar configurada a 1.600 como mínimo y puede ser inferior al valor ya configurado en el DVS.

El número de VTEP creados depende de la directiva de creación de equipos que esté seleccionada y la configuración de DVS.

Problemas habituales durante la preparación de VXLAN.

La preparación de VXLAN puede dar error por varias razones:

- El método seleccionado de creación de equipos para VXLAN no coincide con el que el DVS admite. Para revisar los métodos compatibles, consulte la *Guía de diseño de virtualización de redes de VMware NSX for vSphere* en <https://communities.vmware.com/docs/DOC-27683>.
- Se seleccionó un ID de VLAN incorrecto para los VTEP.
- Se seleccionó un DHCP para asignar direcciones IP de VTEP, pero no existe ningún servidor DHCP disponible.
- Falta una NIC de VMkernel. Resuelva el error como se describe en [La NIC de VMkernel de VXLAN no está sincronizada](#).

- Una NIC de VMkernel tiene una dirección IP incorrecta. Resuelva el error como se describe en <https://kb.vmware.com/kb/2137025>.
- Se seleccionó una configuración de la MTU incorrecta para los VTEP. Debe investigar si se produce un error de coincidencia de MTU, como se describe más adelante en este tema.
- Se seleccionó una puerta de enlace VXLAN incorrecta. Debe investigar si se produce un error al configurar la puerta de enlace de VXLAN, como se describe más adelante en este tema.

Números de puertos importantes

El puerto UDP de VXLAN se usa para la encapsulación de UDP. Antes de la versión 6.2.3 de NSX, el número de puerto VXLAN predeterminado era 8472. En la versión 6.2.3 de NSX, cambió a 4789 para las nuevas instalaciones. Por tanto, en NSX 6.2 y versiones posteriores que utilicen hardware VTEP debe utilizar el puerto 4789. Para obtener información sobre el cambio de configuración del puerto VXLAN, consulte "Cambiar el puerto VXLAN" (Change VXLAN port) en *Guía de administración de NSX*.

El estado del plano de control aparece como *deshabilitado* (disabled) si el host no tiene ninguna máquina virtual activa que necesite una conexión del controlador.

Use los comandos `show logical-switch` para ver los detalles de VXLAN en el host. Para obtener más información, consulte la *Referencia de la interfaz de línea de comandos de NSX*.

El comando `show logical-switch host hostID verbose` mostrará el estado del plano de control como *deshabilitado* (disabled) si el host no se rellenó con una máquina virtual que requiera una conexión al clúster del controlador para reenviar la información de la tabla.

```
Network count: 18
VXLAN network: 32003
Multicast IP: 0.0.0.0
Control plane: Disabled <<=====
MAC entry count: 0
ARP entry count: 0
Port count: 1
```

Error en la configuración de la puerta de enlace de VXLAN

Cuando configure VXLAN con un grupo IP estático en **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation) > Configurar VXLAN (Configure VXLAN)** y se produzca un error en la configuración para establecer una puerta de enlace de grupo de IP en VTEP, el estado de configuración de la VXLAN entra en estado de error (ROJO) en el clúster del host. El mensaje de error es "La puerta de enlace de la VXLAN no puede establecerse en el host" (VXLAN Gateway cannot be set on host) y el estado de error es "VXLAN_GATEWAY_SETUP_FAILURE".

En la llamada a REST API, GET `https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>`, el estado de la VXLAN es el siguiente:

```
<nwFabricFeatureStatus>
<featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

Solución alternativa: existen dos opciones para solucionar el error.

- Option 1: quite la configuración de la VXLAN del clúster del host, solucione la configuración de la puerta de enlace subyacente en el grupo de direcciones IP (asegúrese de que la puerta de enlace esté configurada correctamente y de que se pueda establecer una comunicación con ella) y, a continuación, vuelva a configurar la VXLAN del clúster del host.
- Option 2: realice los pasos siguientes..
 - a Solucione la configuración de la puerta de enlace subyacente en el grupo de direcciones IP; para ello, asegúrese de que la puerta de enlace esté configurada correctamente y de que se pueda establecer una comunicación con ella.
 - b Coloque el host (o los hosts) en modo de mantenimiento para asegurar que no haya tráfico de máquina virtual activo en el host.
 - c Elimine los VTEP de la VXLAN del host.
 - d Finalice el modo de mantenimiento del host. Al finalizar el modo de mantenimiento del host, se activa el proceso de creación de VTEP de la VXLAN en NSX Manager. NSX Manager intenta recrear los VTEP necesarios en el host.

Cómo investigar un error de coincidencia de MTU

- Ejecute el siguiente comando para comprobar si el valor configurado para la MTU es 1600 o superior:

```
ping ++netstack=vxlan -d -s 1572 -I <vmkx hostname_or_IP>
```

donde *vmkx* es el ID del puerto de VMkernel y *hostname_or_IP* es la dirección IP o nombre de host del puerto de VMkernel.

Esto permite comprobar la validez de todos los vínculos superiores. Si trabaja en un entorno de varios VTEP, puede validar todos los vínculos superiores ejecutando el comando ping de cada interfaz de origen o destino de VMkernel de VTEP que sea posible para validar todas las rutas.

- Compruebe la infraestructura física. Muchas veces, el problema se resuelve mediante un cambio de configuración de la infraestructura física.

- Determine si el problema se limita a un único conmutador lógico o si afecta también a otros.
Compruebe si el problema afecta a todos los conmutadores lógicos.

Para obtener más información sobre la comprobación de la MTU, consulte la sección "Comprobar el estado de funcionamiento de NSX" en la *Guía de actualización de NSX*.

La NIC de VMkernel de VXLAN no está sincronizada

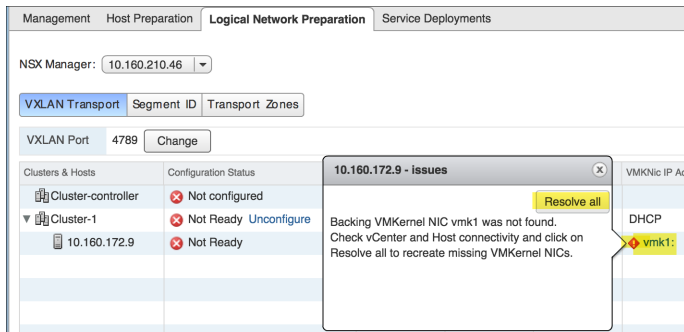
Cuando se elimina la NIC de VMkernel en el host, pero su información sigue disponible en NSX, NSX Manager muestra la NIC de VMkernel eliminada con un icono de **error**.

Requisitos previos

La NIC de VMkernel se eliminó en el host.

Procedimiento

- 1 En vSphere Web Client, acceda a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de red lógica (Logical Network Preparation)**.
- 2 En la pestaña **Transporte de VXLAN (VXLAN Transport)**, expanda el clúster y los hosts.



- 3 Haga clic en el icono **Error** para consultar la NIC de VMkernel que se eliminó en el host.
- 4 Haga clic en el botón **Resolver todo (Resolve All)** para volver a crear la NIC de VMkernel eliminada en el host.

Resultados

Se volverá a crear la NIC de VMkernel en el host.

Cambio de la directiva de creación de equipos de VXLAN y de la configuración de la MTU

La directiva de creación de equipos y la configuración de la MTU pueden cambiar en hosts y clústeres preparados, pero estos cambios solo se aplican al preparar nuevos hosts y clústeres para VXLAN. Los grupos de puertos virtuales existentes de VMkernel de VTEP solo se pueden cambiar preparando de nuevo los hosts manualmente. Puede cambiar la directiva de creación de equipos y la configuración de la MTU mediante la API.

Problema

Se seleccionó una configuración de la MTU incorrecta para los VTEP.

Solución

- 1 Recupere información sobre todos los conmutadores preparados de VXLAN que usen la API GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches`.

En los resultados de la API, localice el conmutador que desee modificar y anote su nombre. Por ejemplo, *dvs-35*.

- 2 A continuación, realice una consulta con la instancia de vSphere Distributed Switch que anotó antes.

Por ejemplo, la API GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35`.

Debería aparecer un resultado similar al siguiente ejemplo:

```
<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
  <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
  <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
  <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
  <revision>6</revision>
  <type>
    <typeName>VmwareDistributedVirtualSwitch</typeName>
  </type>
  < name>vds-site-a</name>
  <scope>
    <id>datacenter-21</id>
    <objectTypeName>Datacenter</objectTypeName>
    < name>Datacenter Site A</name>
  </scope>
  <clientHandle/>
  <extendedAttributes/>
  <isUniversal>false</isUniversal>
  <universalRevision>0</universalRevision>
</switch>
<mtu>1600</mtu>
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>false</promiscuousMode>
</vdsContext>
```

- 3 Puede modificar los parámetros como la directiva de creación de equipos y/o la MTU en un conmutador distribuido de vSphere usando la llamada de la API. En el siguiente ejemplo, se muestran el cambio de la directiva de creación de equipos de *dvs-35* de *FAILOVER_ORDER* a *LOADBALANCE_SRCMAC* y el cambio de la MTU de *1600* a *9000*.

- Para NSX: PUT `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches`

Debería aparecer un resultado similar al siguiente ejemplo:

```
<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
  <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
  <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
  <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
  <revision>6</revision>
  <type>
    <typeName>VmwareDistributedVirtualSwitch</typeName>
  </type>
  <name>vds-site-a</name>
  <scope>
    <id>datacenter-21</id>
    <objectTypeName>Datacenter</objectTypeName>
    <name>Datacenter Site A</name>
  </scope>
  <clientHandle/>
  <extendedAttributes/>
  <isUniversal>false</isUniversal>
  <universalRevision>0</universalRevision>
</switch>
<mtu>9000</mtu>
<teaming>LOADBALANCE_SRCMAC</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>false</promiscuousMode>
</vdsContext>
```

Nota A continuación, se incluye una lista de entradas válidas de la directiva de creación de equipos para el parámetro *<teaming>*:

- FAILOVER_ORDER
- ETHER_CHANNEL
- LACP_ACTIVE
- LACP_PASSIVE
- LOADBALANCE_LOADBASED
- LOADBALANCE_SRCID
- LOADBALANCE_SRCMAC LACP_V2

- 4 Utilice el comando GET para verificar que la sintaxis usada sea correcta y que el cambio esté activo para la instancia de vSphere Distributed Switch con el que esté trabajando. Por ejemplo, GET <https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35>.
- 5 Abra vSphere Web Client y confirme que se aplicaron los cambios de configuración.

Grupo de puerto del conmutador lógico no sincronizado

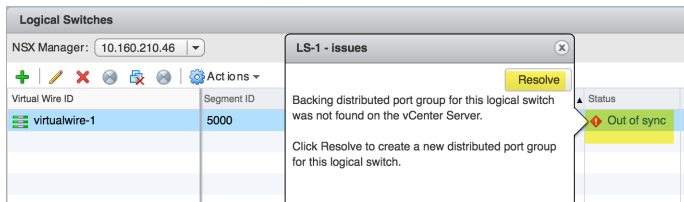
Si la copia de seguridad del grupo de puertos virtuales distribuidos (DVPG) del conmutador lógico se elimina de vCenter Server, la columna Estado (Status) de la página **Conmutadores lógicos** (Logical Switches) mostrará el estado **No sincronizado** (Out of sync).

Requisitos previos

El DVPG del conmutador lógico se eliminó de vCenter Server.

Procedimiento

- 1 En vSphere Web Client, acceda a **Inicio (Home) > Redes y seguridad (Networking & Security) > Conmutadores lógicos (Logical Switches)**.



- 2 En la columna Estado (Status), haga clic en el vínculo **No sincronizado** (Out of sync) para consultar los detalles de este estado.
- 3 Haga clic en el botón **Resolver** (Resolve) para solucionar el problema.

Resultados

Esto invoca a la API para recrear la copia de seguridad del DVPG.

Resolución de problemas de enrutamiento de NSX

3

NSX tiene dos tipos de subsistemas de enrutamiento optimizados para dos necesidades clave.

Los subsistemas de enrutamiento de NSX son los siguientes:

- El enrutamiento dentro del espacio lógico (también conocido como enrutamiento "este-oeste") que proporciona el enrutador lógico distribuido (DLR)
- El enrutamiento entre el espacio lógico y el físico (también conocido como enrutamiento "norte-sur") que proporcionan las puertas de enlace de servicios Edge (ESG)

Los dos subsistemas proporcionan opciones de escalado horizontal.

Puede escalar horizontalmente el enrutamiento este-oeste distribuido a través del DLR.

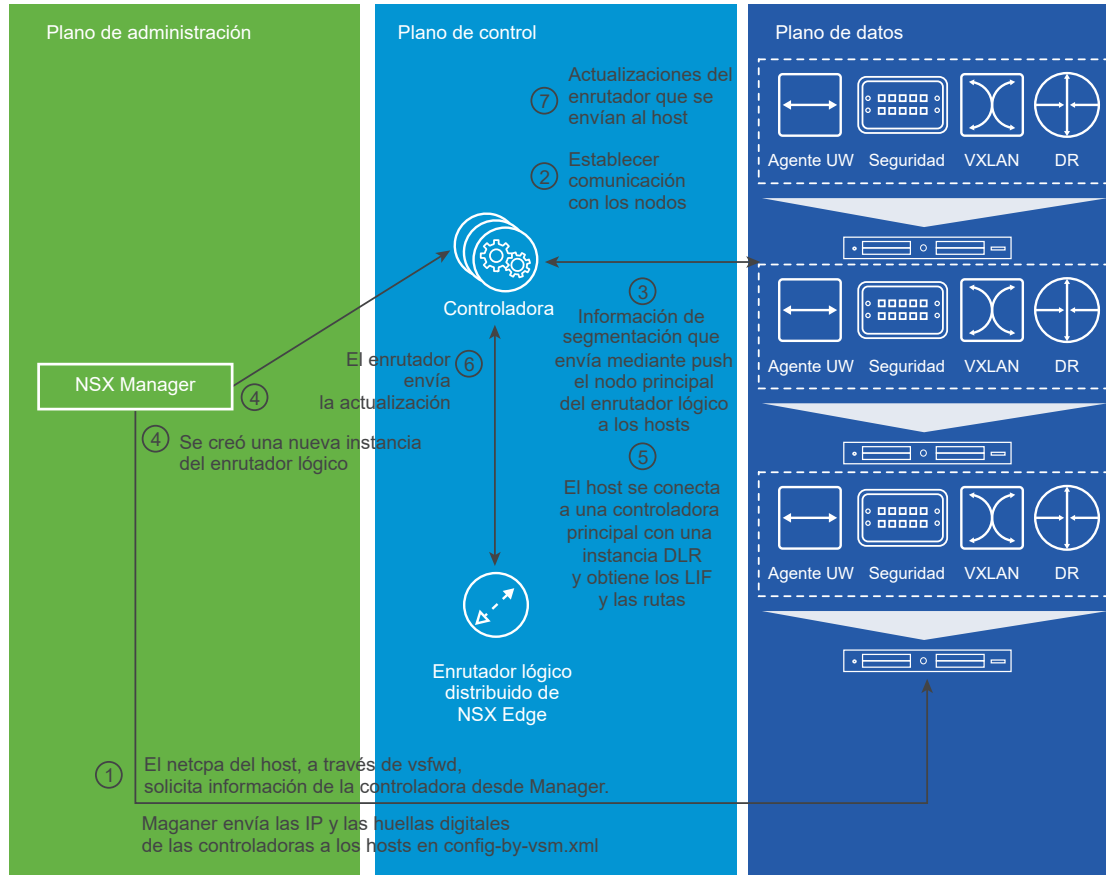
El DLR admite la ejecución de un solo protocolo de enrutamiento dinámico a la vez (OSPF o BGP), mientras que la ESG admite la ejecución de los dos protocolos de enrutamiento a la vez. Esto se debe a que el DLR se diseña para que sea un enrutador "stub" con una única ruta, lo que significa que no se necesitarán configuraciones de enrutamiento más avanzadas.

El DLR y la ESG admiten una combinación de rutas dinámicas y estáticas.

El DLR y la ESG admiten las rutas ECMP.

Ambos proporcionan separación del dominio de Capa 3, lo que significa que cada instancia de un enrutador lógico distribuido o una puerta de enlace de servicios Edge tienen su propia configuración de Capa 3, similar a un VRF de VPN de Capa 3.

Figura 3-1. Creación de un DLR.



Este capítulo incluye los siguientes temas:

- [Comprender el enrutador lógico distribuido](#)
- [Comprender el enrutamiento proporcionado por la puerta de enlace de Edge](#)
- [Flujo de paquete ECMP](#)
- [Enrutamiento de NSX: requisitos previos y consideraciones](#)
- [Interfaces de usuario de ESG y DLR](#)
- [NSX Edge nuevo \(DLR\)](#)
- [Operaciones habituales de la interfaz de usuario de ESG y DLR](#)
- [Resolución de problemas de enrutamiento de NSX](#)

Comprender el enrutador lógico distribuido

El DLR está optimizado para realizar reenvíos en el espacio lógico entre máquinas virtuales o en grupos de puertos de VXLAN respaldadas o VLAN respaldadas.

El DLR cuenta con las siguientes propiedades:

- Alto rendimiento, bajo consumo en el primer salto en ruta:

- Escalas lineales según el número de hosts
- Admite 8 tipos de ECMP en enlace de subida
- Hasta 1.000 instancias de DLR por host
- Hasta 999 interfaces lógicas (LIF) en cada DLR (8 x enlaces de subida + 991 internas) + 1 x de administración.
- Hasta 10.000 LIF por host distribuidas por todas las instancia de DLR (sin aplicar por parte de NSX Manager).

Tenga en cuenta las siguientes advertencias:

- No se puede conectar más de un DLR a cualquiera de las VLAN o VXLAN existentes.
- No se puede ejecutar más de un protocolo de enrutamiento en cada DLR.
- Si se utiliza OSPF, no se puede ejecutar en más de un enlace de subida de DLR.
- Para la ruta entre VXLAN y VLAN, la zona de transporte debe ocupar un único DVS.

El diseño del DLR a alto nivel es análogo al chasis del router modular de las formas siguientes:

- Los hosts ESXi son como tarjetas de línea:
 - Tienen puertos con estaciones conectadas por sus extremos (máquinas virtuales).
 - Es aquí donde se toman las decisiones de reenvío.
- La máquina virtual de control de DLR es como un motor de procesador de enrutamiento.
 - Ejecuta protocolos de enrutamiento dinámico para intercambiar información de enrutamiento con el resto de la red.
 - Calcula las tablas de reenvío para las "tarjetas de línea" basándose en la información de enrutamiento dinámico, las rutas estáticas y la configuración de interfaces.
 - Programa estas tablas de reenvío en las tarjetas de línea (a través del clúster de la controladora, para habilitar la escala y la resistencia).
- La red física que conecta los dos hosts ESXi es como un backplane:
 - Lleva los datos de VLAN o VXLAN encapsuladas entre las "tarjetas de línea".

Flujo de paquete de DLR de alto nivel

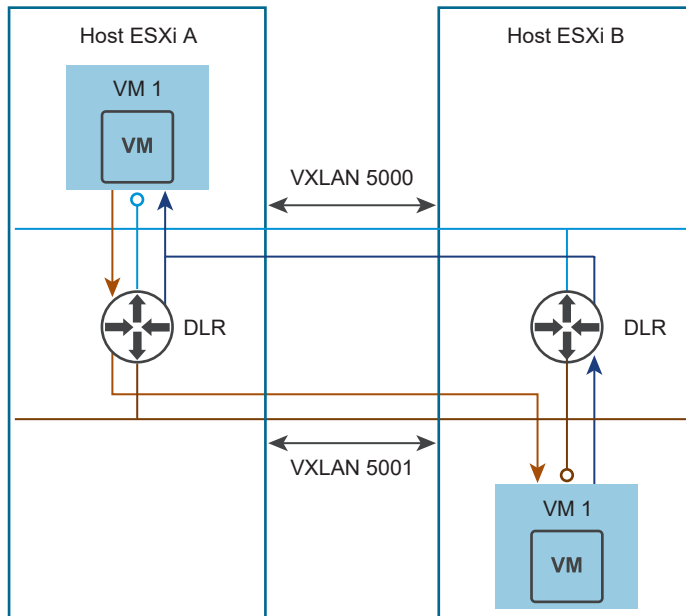
Cada host ESXi tiene su propia copia de todas las instancias de DLR configuradas. Cada instancia de DLR tiene su propia configuración única de tablas que contienen la información necesaria para reenviar paquetes. Esta información se sincroniza en todos los hosts cuando existe esta instancia de DLR. Las instancias de un DLR individual a través de distintos hosts contienen la misma información.

El enrutamiento siempre lo lleva a cabo una instancia de DLR en el mismo host en el que se ejecuta la máquina virtual de origen. Esto significa que cuando las máquinas virtuales de origen y de destino están en hosts distintos, la instancia de DLR que realiza los enrutamientos entre ellas capta los paquetes solo en una dirección: de la máquina virtual de origen a la de destino. El tráfico de retorno solo lo capta la instancia correspondiente del mismo DLR en el host de la máquina virtual de destino.

Tras el enrutamiento completo de DLR, el envío al destino final es responsabilidad de DVS a través de Capa2, VXLAN o VLAN si las máquinas virtuales de origen y de destino están en hosts diferentes o a través del DVS local si están en el mismo host.

Figura 3-2. Flujo de paquete de DLR de alto nivel muestra el flujo de datos entre dos máquinas virtuales diferentes, VM1 y VM2, que se ejecutan en diferentes hosts y que están conectadas a dos conmutadores lógicos distintos: VXLAN 5000 y VXLAN 5001.

Figura 3-2. Flujo de paquete de DLR de alto nivel



Flujo de paquetes (omitiendo la resolución ARP):

- 1 La VM1 envía un paquete a la VM2, que está asignada a la puerta de enlace de la VM1 para la subred de la VM2 (o a la que está asignada por defecto). Esta puerta de enlace es un LIF de VXLAN 5000 en DLR.
- 2 El DVS en el host ESXi A envía el paquete al DLR en ese host, donde se realizó la búsqueda, y el LIF de salida está determinado (en este caso: LIF de VXLAN 5001).
- 3 El paquete se envía entonces a ese LIF de destino, que básicamente devuelve el paquete al DVS pero con un conmutador lógico diferente (5001).
- 4 El DVS realiza envíos de Capa 2 de ese paquete al host de destino (host ESXi B), donde el DVS reenviará el paquete a la máquina virtual 2.

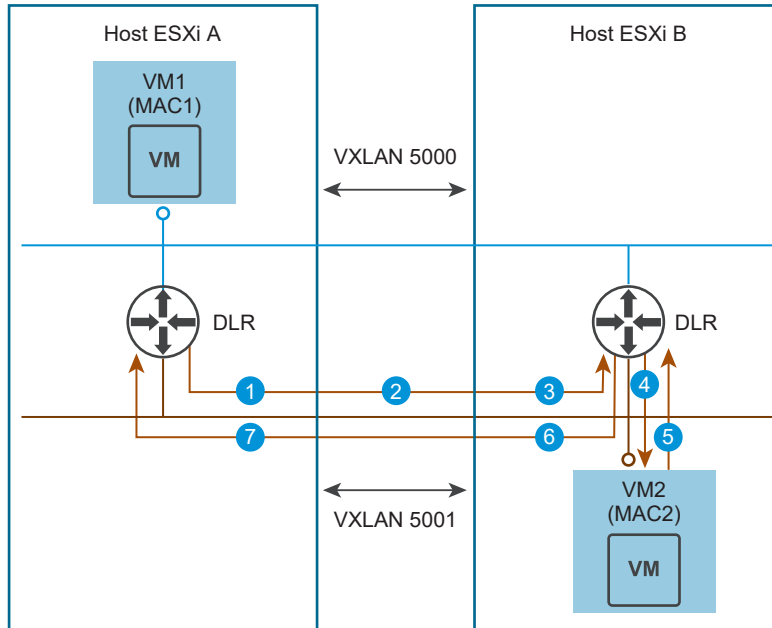
El tráfico de retorno continuará en el mismo orden, donde el tráfico desde la VM2 se reenvía a la instancia de DLR en el host ESXi B y, a continuación, se envía a través de Capa 2 a VXLAN 5000.

Proceso de resolución del ARP de DLR

Antes de que el tráfico de la máquina virtual 1 llegue a la máquina virtual 2, el DLR debe conocer la dirección MAC de la máquina virtual 2. Una vez que conozca la dirección MAC de la máquina virtual 2, el DLR podrá crear los encabezados de Capa 2 correctos de los paquetes de salida.

El [Figura 3-3. Proceso de ARP de DLR](#) muestra el proceso de resolución del ARP de DLR.

Figura 3-3. Proceso de ARP de DLR



Para conocer la dirección MAC, el DLR sigue estos pasos:

- 1 La instancia de DLR del host A genera un paquete de solicitud de ARP con SRC MAC = vMAC y DST MAC = Broadcast. El módulo VXLAN del host A encuentra todos los VTEP en la VXLAN 5001 de salida y envía a cada uno una copia de esa trama de difusión.
- 2 Mientras la trama sale del host a través del proceso de encapsulación de VXLAN, el SRC MAC cambia de vMAC a pMAC A para que el retorno del tráfico pueda encontrar la instancia de DLR de origen en el host A. La trama ahora es SRC MAC = pMAC A y DST MAC = Broadcast.
- 3 Mientras se recibe y se deencapsula la trama en el host B, se examina y se garantiza que proceda de la dirección IP que coincide con la LIF de la instancia del DLR local en VXLAN 5001. Esto marca la trama como una solicitud para llevar a cabo la función de ARP del proxy. DST MAC cambia de Broadcast a vMAC para que la trama pueda llegar a la instancia del DLR local.
- 4 La instancia del DLR local del host B recibe la trama de solicitud de ARP (SRC MAC = pMAC A y DST MAC = vMAC) y ve su propia dirección IP de LIF solicitando esto. Guarda el SRC MAC y genera un nuevo paquete de solicitud de ARP con SRC MAC = vMAC y DST MAC = Broadcast. Esta trama se etiqueta como "DVS Local" para evitar que se congestione mediante dvUplin. El DVS envía la trama a la máquina virtual 2.

- 5 La máquina virtual 2 envía una respuesta de ARP, SRC MAC = MAC2, DST MAC = vMAC. El DVS la envía a la instancia de DLR local.
- 6 La instancia de DLR del host B sustituye a DST MAC con el pMAC A guardado desde el paso 4 y envía el paquete de vuelta al DVS para enviarlo de vuelta al host A.
- 7 Cuando la respuesta de ARP llega al host A, DST MAC cambia a vMAC y la trama de respuesta de ARP con SRC MAC = MAC2 y DST MAC = vMAC llega a la instancia de DLR del host A.

El proceso de resolución de ARP se completó y la instancia de DLR del host A ahora puede enviar tráfico a la máquina virtual 2.

Supresión de ARP en DLR

La supresión del protocolo de resolución de direcciones (ARP) es una técnica utilizada para reducir la cantidad de desbordamiento de difusión de ARP en segmentos de VXLAN individuales, es decir, entre máquinas virtuales conectadas al mismo conmutador lógico.

Cuando la máquina virtual 1 quiere conocer la dirección MAC de la máquina virtual 2, envía una solicitud ARP. Esta solicitud ARP es interceptada por el conmutador lógico y, si este ya tiene una entrada ARP para el destino, envía la respuesta ARP a la máquina virtual.

Si no es así, envía una consulta ARP a NSX Controller. Si el controlador conoce el enlace de IP a MAC de la máquina virtual, este responde con el enlace y el conmutador lógico envía la respuesta ARP. Si el controlador no tiene la entrada ARP, la solicitud ARP se vuelve a difundir en el conmutador lógico. NSX Controller obtiene la dirección MAC a través del módulo Switch Security, que consulta las solicitudes ARP y los paquetes DHCP.

La supresión de ARP se amplió para incluir también el enrutador lógico distribuido (DLR).

- Las solicitudes ARP del enrutador lógico distribuido se tratan igual que las solicitudes ARP de otras máquinas virtuales y son susceptibles de supresión. Cuando el enrutador lógico distribuido tiene que resolver la solicitud ARP de una IP de destino, el conmutador lógico suprime la solicitud ARP, evitando el desbordamiento cuando el controlador ya conoce el enlace de IP a MAC.
- Cuando se crea un LIF, el enrutador lógico distribuido agrega la entrada ARP de la IP del LIF al conmutador lógico, de forma que este también suprime las solicitudes ARP de la IP del LIF.

Comprender el enrutamiento proporcionado por la puerta de enlace de Edge

La puerta de enlace de Edge proporciona el segundo subsistema del enrutamiento de NSX.

La ESG es, básicamente, un router en una máquina virtual. Se envía en un factor de forma de dispositivo con cuatro tamaños con su ciclo de vida completo administrado por NSX Manager. La ESG se utiliza principalmente como un router perimétrico, en el que se implementa entre varios DLR y entre el mundo físico y la red virtual.

La ESG cuenta con las siguientes propiedades:

- Cada ESG puede tener hasta 10 interfaces vNIC o 200 subinterfaces en tronco.

- Cada ESG admite 8 tipos de ECMP para redundancia y la escalabilidad de rutas.

Flujo de paquete ECMP

Suponga que dos ESG se implementan para proporcionar a una instancia de DLR dos tipos de enlaces de subida ECMP con el entorno físico.

Figura 3-4. Flujo de paquetes de DLR y ESG de alto nivel con ECMP muestra el flujo de los paquetes ESG y DLR cuando el enrutamiento de múltiples rutas de igual costo (ECMP) está habilitado entre dos ESG y la infraestructura física.

La VM1 tiene por tanto acceso a un rendimiento bidireccional 2x si se compara con una implementación con ESG sencilla.

La VM1 está conectada a un conmutador lógico con VNI 5000.

El DLR tiene dos LIF: una interna en VNI 500 y un enlace de subida en VNI 500.

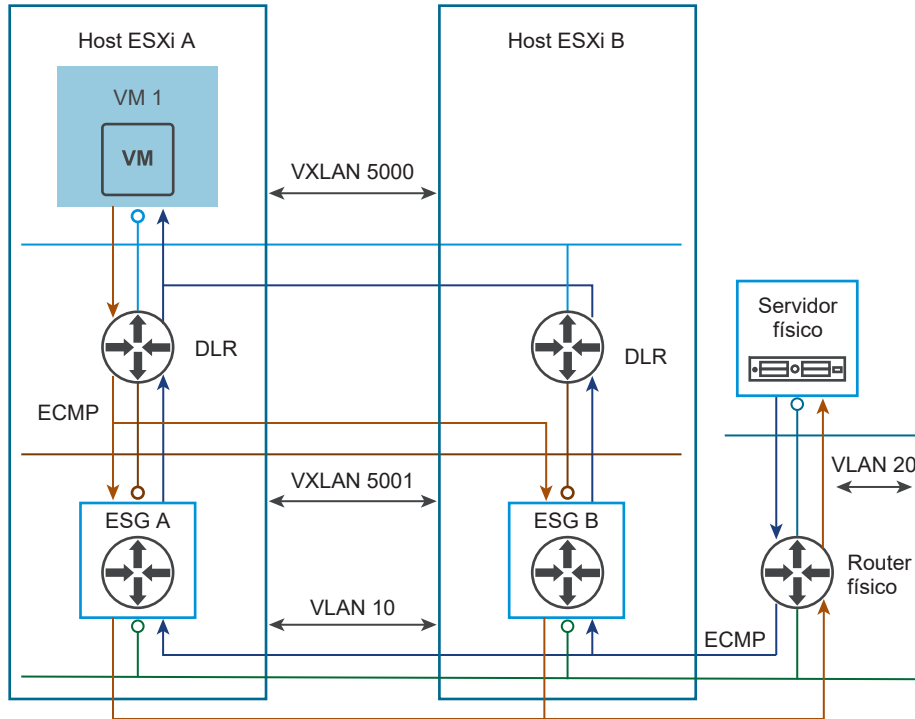
El DLR tiene habilitado el ECMP y recibe rutas de igual costo a través de la subred de la IP de VLAN 20 de un par de ESG: ESG A y ESG B a través de un protocolo de enrutamiento dinámico (BGP o OSPF).

Las dos ESG se conectan a un dvPortgroup respaldado por una VLAN asociada a la VLAN 10 donde también se conecta un router físico que proporciona conexión a la VLAN 20.

Las ESG reciben enrutadores externos para la VLAN 20 a través de un protocolo de enrutamiento dinámico desde el router físico.

El router físico en intercambio conoce la IP de la subred asociada con VXLAN 5000 desde ambas ESG y realiza equilibrio de carga de ECMP para el tráfico hacia las máquinas virtuales de dicha subred.

Figura 3-4. Flujo de paquetes de DLR y ESG de alto nivel con ECMP



El DLR puede recibir hasta ocho rutas de igual costo y tráfico de equilibrio a través de las rutas. El diagrama de la ESG A y la ESG B muestra dos rutas de igual costo.

Las ESG pueden realizar enrutamientos ECMP en toda la red física, asumiendo que existen múltiples enrutadores físicos. Para simplificarlo, el diagrama muestra un router físico único.

El EMCP no necesita estar configurado en las ESG hacia el DLR ya que todos los LIF de DLR son "locales" en el mismo host en el que se encuentra la ESG. No supone una ventaja adicional configurar varias interfaces de enlaces de subida en un DLR.

Si se necesita más ancho de banda Norte-Sur se pueden colocar varios ESG en distintos hosts ESXi para ampliar hasta 80 Gbps aproximadamente con 8 x ESG.

Flujo de paquete ECMP (sin incluir la resolución de ARP):

- 1 La VM1 envía un paquete al servidor físico, que se envía a la puerta de enlace de la IP de la VM1 (que es un LIF de DLR) en el host ESXi A.
- 2 El DLR realiza una búsqueda en ruta de la IP del servidor físico y encuentra que no está conectado directamente, pero que coinciden dos rutas ECMP recibidas desde la ESG A y la ESG B.
- 3 El DLR calcula un hash de ECMP, decide el próximo salto, que puede ser tanto ESG A como ESG B, y manda el paquete fuera del LIF de VXLAN 5001.
- 4 El DVS envía el paquete a la ESG seleccionada.
- 5 La ESG realiza la búsqueda de la ruta y encuentra que la subred del servidor físico es accesible a través de la dirección IP del router físico en la VLAN 10 que se conecta directamente a una de las interfaces de la ESG.

- 6 El paquete se envía a través del DVS, que lo pasa por la red física después de otorgarle la etiqueta 801.Q correcta con el ID 10 de VLAN.
- 7 El paquete viaja a través de la infraestructura de los conmutadores físicos para llegar al router físico, que realiza una búsqueda para encontrar si el servidor físico está conectado directamente a una interfaz en VLAN 20.
- 8 El router físico envía el paquete al servidor físico.

A la vuelta:

- 1 El servidor físico envía el paquete a la VM1, con el router físico como próximo salto.
- 2 El router físico realiza una búsqueda de la subred de la VM1 y observa dos rutas de igual costo en esa subred con los siguientes saltos, la interfaz VLAN 10 de la ESG A y ESG B respectivamente.
- 3 El router físico selecciona una de las rutas y envía el paquete a través de la ESG correspondiente.
- 4 La red física envía el paquete al host ESXi donde se encuentra la ESG y lo envía al DVS, que deencapsula el paquete y lo reenvía a la ESG en el dvPortgroup asociado a la VLAN 10.
- 5 La ESG realiza una búsqueda de la ruta y encuentra que se puede acceder a la subred de la VM1 a través de su interfaz asociada con VXLAN 5001, siendo el siguiente salto la dirección IP de la interfaz del enlace de subida de DLR.
- 6 La ESG envía el paquete a la instancia de DLR en el mismo host que la ESG.
- 7 El DLR realiza una búsqueda de la ruta para encontrar que la VM1 está disponible a través del LIF de su VXLAN 5000.
- 8 El DLR envía el paquete fuera del LIF de su VXLAN 5000 al DVS, que realiza el envío final.

Enrutamiento de NSX: requisitos previos y consideraciones

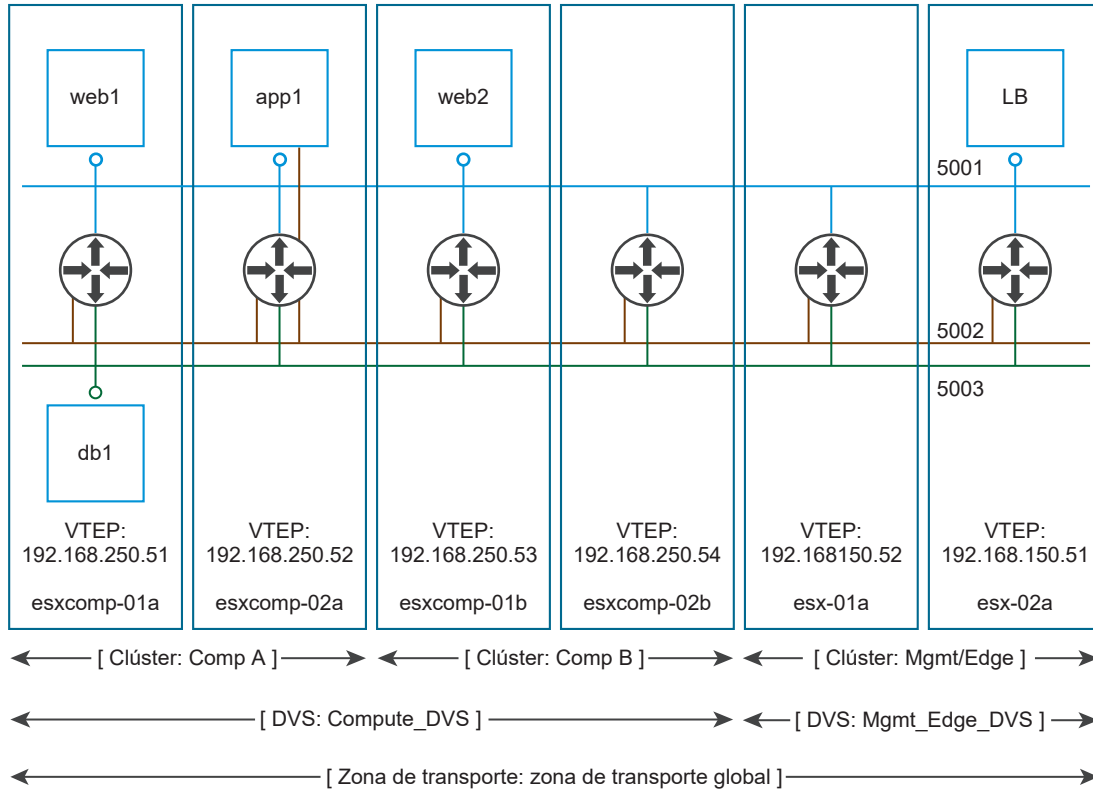
DLR y ESG se basan en el DVS para proporcionar servicios de reenvío de Capa 2 a dvPortgroups (ambos basados en VXLAN y VLAN) para que funcione la conectividad de extremo a extremo.

Esto significa que la Capa 2 que realiza servicios de reenvíos conectados a DLR o ESG debe estar configurada y operativa. En el proceso de instalación de NSX, "Preparación del host" (Host Preparation) y "Preparación de la red lógica" (Logical Network Preparation) proporcionan estos servicios.

Al crear zonas de transporte en configuraciones de DVS de varios clústeres, asegúrese de que todos los clústeres del DVS seleccionado estén incluidos en la zona de transporte. De esta forma se asegura de que el DLR esté disponible en todos los clústeres en los haya disponibles dvPortgroups de DVS.

Cuando una zona de transporte se alinea con el límite del DVS, la instancia de DLR se crea correctamente.

Figura 3-5. Zona de transporte correctamente alineada con el límite del DVS



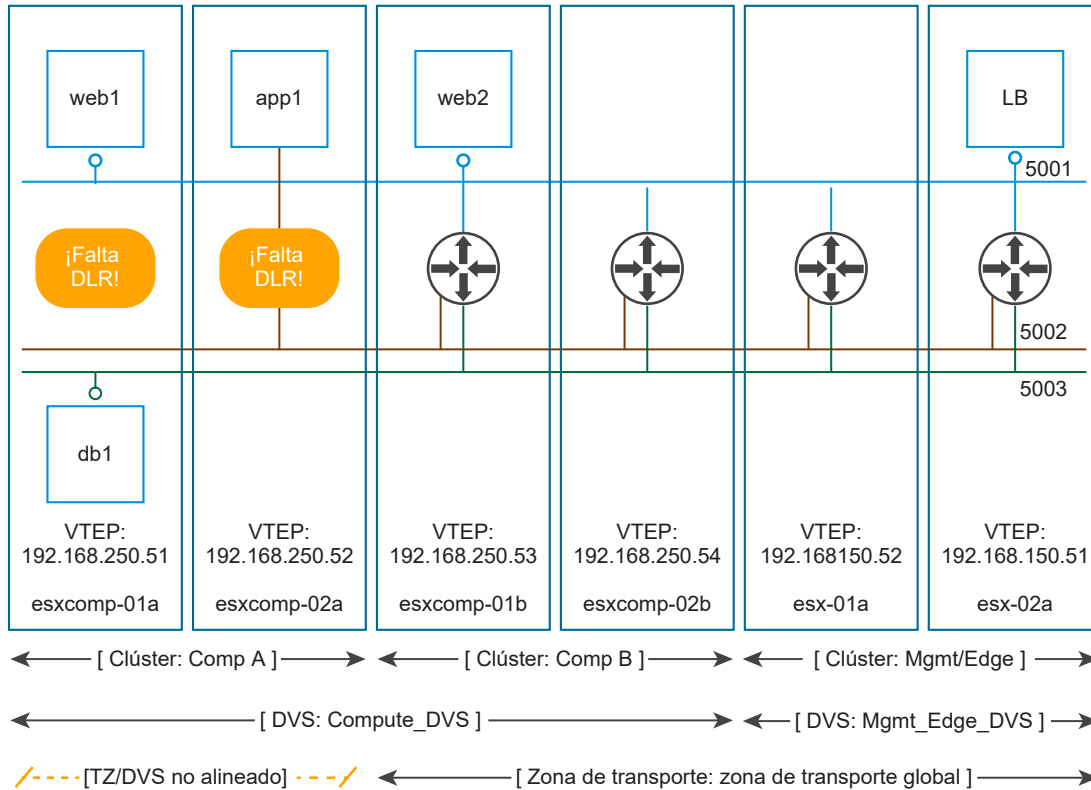
Si una zona de transporte no está alineada con el límite del DVS, el alcance de los conmutadores lógicos (5001, 5002 y 5003) y las instancias de DLR a las que están conectados quedan desasociados; esto hace que las máquinas virtuales del clúster Comp A no puedan acceder a los LIF del DLR.

En el diagrama anterior, el DVS "Compute_DVS" muestra dos clústeres: "Comp A" y "Comp B". La Zona de transporte global ("Global-Transport-Zone") incluye tanto "Comp A" como "Comp B".

Esto lleva a la correcta alineación entre el alcance de los conmutadores lógicos (5001, 5002 y 5003) y la instancia de DLR creada en todos los hosts de todos los clústeres en los que este conmutador lógico está presente.

Consulte a continuación una situación alternativa donde la zona de transporte no se configuró para incluir el clúster "Comp A":

Figura 3-6. Zona de transporte no alineada con el límite del DVS



En este caso, las máquinas virtuales que se estén ejecutando en el clúster "Comp A" tienen acceso total a todos los conmutadores lógicos. Esto se produce porque los conmutadores lógicos se representan a través de los dvPortgroups en los hosts y los dvPortgroups son construcciones basadas en el ancho de DVS. En nuestro entorno de ejemplo, "Compute DVS" muestra tanto "Comp A" como "Comp B".

Las instancias de DLR, sin embargo, se crean en estricta alineación con el alcance de la zona de transporte, lo que significa que ninguna instancia de DLR se creará en los hosts de "Comp A".

Como resultado, "web1" de la máquina virtual podrá alcanzar "LB" y "web2" de las máquinas virtuales porque están en el mismo conmutador lógico, pero "app1" y "db1" de las máquinas virtuales no podrán comunicarse con nada.

El DLR se basa en el clúster de la controladora para funcionar, mientras que la ESG no. Asegúrese de que el clúster de la controladora esté en funcionamiento y disponible antes de crear o modificar la configuración de DLR.

Si desea conectar el DLR a los dvPortgroups de VLAN, asegúrese de que todos los hosts ESXi que tengan el DLR configurado puedan comunicarse entre sí en UDP/6999 para que el proxy ARP basado en la VLAN del DLR funcione.

Consideraciones:

- Una instancia de DLR determinada no puede conectarse a los conmutadores lógicos que existen en zonas de transporte distintas. El objetivo de esto es garantizar que todas los conmutadores lógicos y DLR estén alineados.

- El DLR no se puede conectar a grupos de puertos respaldados en VLAN si dicho DLR está conectado a conmutadores lógicos que expanden más de un DVS. Como ya se ha mencionado, esto se realiza para asegurar la correcta alineación entre las instancias de DLR con conmutadores lógicos y los dvPortgroups a través de los hosts.
- Cuando seleccione la colocación de las máquinas virtuales de control de DLR, evite colocarla en el mismo host que uno o varios de sus ESG ascendentes mediante reglas antiafinidad de DRS si están en el mismo clúster. Esto reduce el impacto del fallo del host en los envíos de DLR.
- El OSPF se puede habilitar con un solo enlace de subida (pero admite varias adyacencias). Por otro lado, se puede habilitar BGP en varias interfaces de enlaces de subida cuando sea necesario.

Interfaces de usuario de ESG y DLR

Las interfaces de usuario de ESG y DLR proporcionan los indicadores del estado de funcionamiento del sistema.

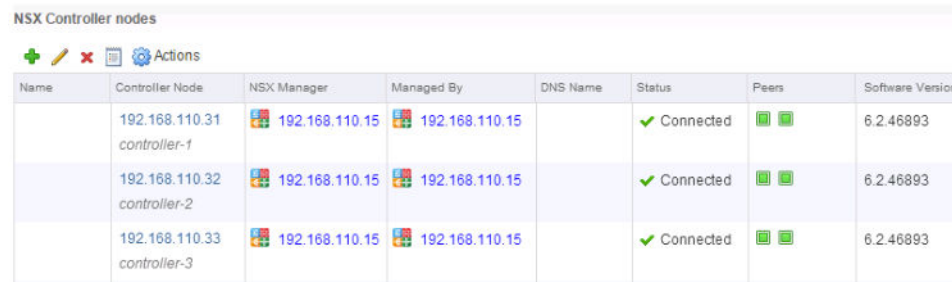
Interfaz de usuario de enrutamiento de NSX













La interfaz de usuario de vSphere Web Client contiene dos secciones principales que son relevantes para el enrutamiento de NSX.

Estas incluyen las dependencias de la infraestructura de plano de control y Capa 2 así como la configuración del subsistema de enrutamiento.

El enrutamiento distribuido de NSX requiere funciones que proporciona el clúster del controlador. La siguiente captura de pantalla muestra un clúster del controlador en buen estado.

NSX Controller nodes



Name	Controller Node	NSX Manager	Managed By	DNS Name	Status	Peers	Software Version
	192.168.110.31 controller-1	 192.168.110.15	 192.168.110.15		✓ Connected	 	6.2.46893
	192.168.110.32 controller-2	 192.168.110.15	 192.168.110.15		✓ Connected	 	6.2.46893
	192.168.110.33 controller-3	 192.168.110.15	 192.168.110.15		✓ Connected	 	6.2.46893

Tenga en cuenta:

- Hay tres controladores implementados.
- El estado de todas los controladores es "Conectado" (Connected).
- La versión de software de todas los controladores es la misma.
- El nodo de cada controlador tiene dos elementos del mismo nivel.

Los módulos kernel del host del enrutamiento dinámico se instalan y se configuran como parte de la configuración de VXLAN en el host. Esto significa que el enrutamiento distribuido necesita que los hosts ESXi se preparen y que VXLAN se configure en ellos.

Clusters & Hosts	Installation Status	Firewall	VXLAN
▶ Compute Cluster A	✓ 6.2.3.3771501	✓ Enabled	✓ Configured
▶ Management & Edge Cluster	✓ 6.2.3.3771501	✓ Enabled	✓ Configured

Tenga en cuenta:

- El "Estado de instalación" (Installation Status) es verde.
- La red VXLAN está "Configurada" (Configured).

Comprueba que los componentes del transporte de VXLAN están configurados correctamente.

VXLAN Transport		Segment ID	Transport Zones				
Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKnic IP Addressing	Teaming Policy	VTEP
▼ Compute Cluster A	✓ Unconfigure	vds-site-a	0	1600	IP Pool	Fail Over	1
esx-02a.corp.local	✓ Ready				vmk3: 192.168.130.51		
esx-01a.corp.local	✓ Ready				vmk3: 192.168.130.52		
▼ Management & Edge	✓ Unconfigure	vds-mgt-edge	0	1600	IP Pool	Fail Over	1
esxmtg-02a.corp.l	✓ Ready				vmk3: 192.168.120.52		
esxmtg-01a.corp.l	✓ Ready				vmk3: 192.168.120.51		

Tenga en cuenta:

- El ID de VLAN debe ser correcto para el VLAN de transporte de VTEP. Tenga en cuenta que en la captura de pantalla anterior es "0". En la mayoría de las implementaciones este no sería el caso.
- MTU se configura para que sea 1600 o un número mayor. Compruebe que la MTU no se establezca en 9.000 con la expectativa de que la MTU de las máquinas virtuales se establezca también en 9.000. La MTU máxima de DVS es 9.000 y si las máquinas virtuales también se establecen en 9.000, no habrá espacio para los encabezados de VXLAN.
- Las VMKnics deben tener las direcciones correctas. Compruebe que no se establezcan en direcciones 169.254.x.x, indicando que los nodos no han podido obtener direcciones de DHCP.
- La directiva de formación de equipos debe ser consistente para todos los miembros del clúster del mismo DVS.
- El número de VTEP debe ser el mismo que el número de dvUplinks. Compruebe que las direcciones IP válidas o esperadas aparecen en la lista.

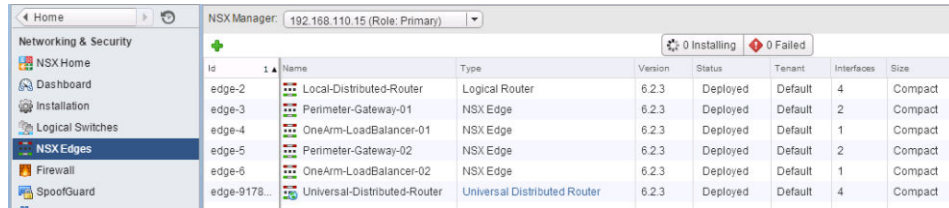
Las zonas de transporte deben estar correctamente alineadas con los límites de DVS para evitar que el DLR falte en varios clústeres.

Name	NSX vSwitch	Status
▶ Compute Cluster A	vds-site-a	✓ Normal
▶ Management & Edge ...	vds-mgt-edge	✓ Normal

Interfaz de usuario de instancias de NSX Edge

El subsistema de enrutamiento de NSX se configura y se administra en la sección "NSX Edges" de la interfaz de usuario.

Cuando se selecciona esta parte de la interfaz de usuario, aparece la vista que se indica a continuación.



Id	Name	Type	Version	Status	Tenant	Interfaces	Size
edge-2	Local-Distributed-Router	Logical Router	6.2.3	Deployed	Default	4	Compact
edge-3	Perimeter-Gateway-01	NSX Edge	6.2.3	Deployed	Default	2	Compact
edge-4	OneArm-LoadBalancer-01	NSX Edge	6.2.3	Deployed	Default	1	Compact
edge-5	Perimeter-Gateway-02	NSX Edge	6.2.3	Deployed	Default	2	Compact
edge-6	OneArm-LoadBalancer-02	NSX Edge	6.2.3	Deployed	Default	1	Compact
edge-9178...	Universal-Distributed-Router	Universal Distributed Router	6.2.3	Deployed	Default	4	Compact

Se muestran todos los DLR y las ESG implementados actualmente con la siguiente información para cada uno:

- El campo "Id" muestra el ID del dispositivo de Edge de DLR o ESG, que se puede utilizar para cualquier llamada API que haga referencia tanto a la ESG como al DLR.
- "Arrendatario" + "Id" forman el nombre de la instancia de DLR. Este nombre se ve y se utiliza en la CLI de NSX.
- "Tamaño" (Size) siempre es "Compacto" (Compact) para DLR así como el tamaño que seleccionó el operador de ESG.

Además de la información de la tabla, hay un menú contextual al que se puede acceder a través de botones o de acciones.

Tabla 3-1. Menú contextual de NSX Edge












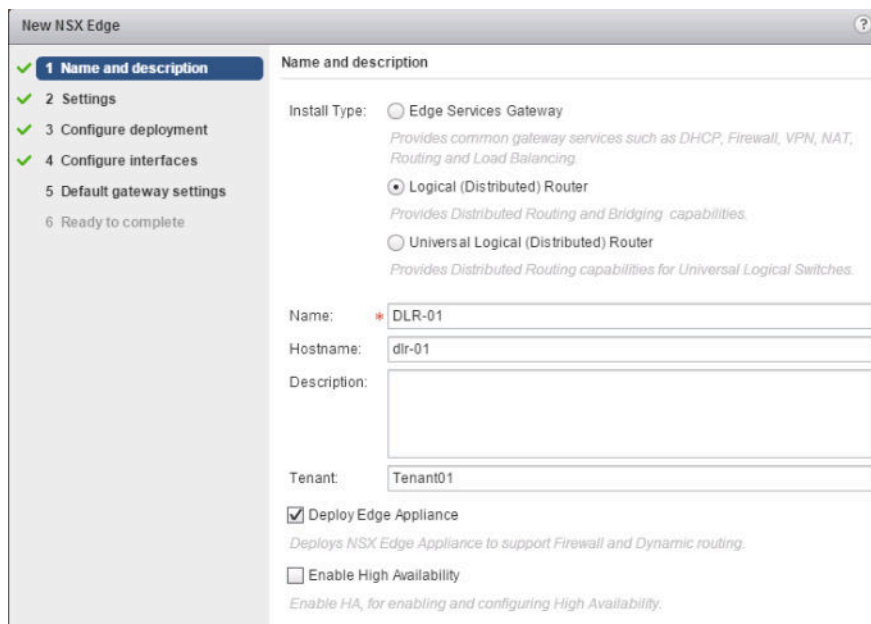
Icono	Acción
	La operación Forzar sincronización ("Force Sync") borra la configuración de la máquina virtual de control de DLR o de ESG y vuelve a introducir la configuración.
	La opción "Volver a implementar" (Redeploy) elimina la ESG o el DLR y crea una ESG o un DLR nuevos con la misma configuración. El ID existente se conserva.
	La opción "Cambiar configuración de reglas automáticas" (Change Auto Rule Configuration) se aplica a las reglas de firewall integradas de ESG, que se crean cuando los servicios están habilitados en la ESG (por ejemplo, un BGP que necesita TCP/179).
	La opción "Descargar registros de soporte técnico" (Download tech support logs) crea un paquete de registros de la máquina virtual de control de DLR o ESG. En el DLR, los registros de hosts no se incluyen en el paquete de soporte técnico y deben recogerse por separado.
	La opción "Cambiar tamaño de dispositivo" (Change appliance size) solo se aplica a las ESG. Esta opción volverá a realizar una implementación con un dispositivo nuevo (las direcciones MAC del vNIC cambiarán).
	La opción "Cambiar credenciales de CLI" (Change CLI credentials) permite al operador forzar la actualización de las credenciales de la CLI. Si la CLI no puede acceder a la máquina virtual de control de DLR o ESG después de iniciar sesión 5 veces de forma incorrecta, esta opción no anulará este bloqueo. Debe esperar 5 minutos o volver a implementar el DLR o la ESG para volver a iniciar sesión con las credenciales correctas.
	La opción "Cambiar nivel de registro" (Change Log Level) cambia el nivel de la información que se va a enviar al registro del sistema de ESG o DLR.
	La opción "Configurar depuración avanzada" (Configure Advanced Debugging) vuelve a implementar la ESG o el DLR con un volcado de memoria habilitado y un disco virtual adicional asociado para almacenar archivos de volcado de memoria.

Tabla 3-1. Menú contextual de NSX Edge (continuación)

Icono	Acción
	La opción "Implementar" (Deploy) está disponible cuando se crea una ESG sin implementarla. Esta opción simplemente realiza los pasos de implementación (implementa el OVF, configura interfaces e introduce la configuración en el dispositivo creado).
	Si la versión del DLR o la ESG es anterior a NSX Manager, la opción "Actualizar versión" (Upgrade Version) estará disponible.
	La opción "Filtro" (Filter) puede buscar los DLR o las ESG por nombre.

NSX Edge nuevo (DLR)

Cuando un operador crea un DLR nuevo, se utiliza el siguiente asistente para recoger la información necesaria.



New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete

Name and description

Install Type: ☐ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.
☒ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.
☐ Universal Logical (Distributed) Router
Provides Distributed Routing capabilities for Universal Logical Switches.

Name: * DLR-01
Hostname: dlr-01
Description:
Tenant: Tenant01

☒ Deploy Edge Appliance
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.
☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

En la pantalla "Nombre y descripción" (Name and Description) se recoge la siguiente información:

- El campo "Nombre" (Name) aparecerá en la interfaz de usuario de las distintas instancias de "NSX Edge".
- El campo "Nombre de host" (Hostname) se utilizará para establecer el nombre de DNS de la ESG o de la máquina virtual de control de DNR, que se puede ver en la sesión de la consola o de SSH, en los mensajes de registro del sistema y en la sección "Nombre de DNS" (DNS Name) de la página "Resumen" (Summary) de vCenter de la máquina virtual de DLR o ESG.
- El campo Descripción ("Description") se encuentra en la interfaz de usuario y muestra la lista de NSX Edges.
- El campo "Arrendatario" (Tenant) se utilizará para crear el nombre de la instancia de DLR que utiliza la CLI de NSX. Cloud Management Platform externa también puede utilizarla.

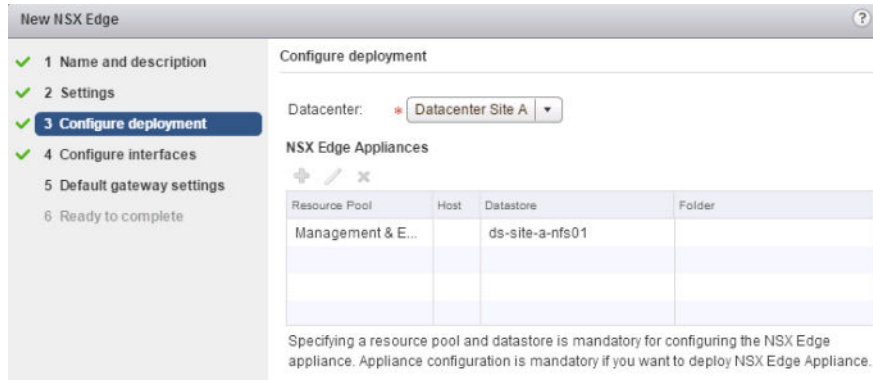
En la pantalla Configuración ("Settings"):

- El campo Nombre de usuario (User Name) y el campo Contraseña (Password) establecen las credenciales de la consola de la máquina virtual o la CLI para acceder a la máquina virtual de control de DLR. NSX no admite AAA en ESG o en máquinas virtuales de control de DLR. Esta cuenta tiene permisos totales para máquinas virtuales de control de ESG/DLR; sin embargo, la configuración de ESG/DLR no se puede cambiar a través de CLI/VMconsole.
- La opción "Habilitar acceso de SSH" (Enable SSH access) habilita el demonio de SSH en la máquina virtual de control de DLR para que se inicie.
 - Las reglas del firewall de la máquina virtual de control se deben ajustar para permitir el acceso de la red SSH.
 - El operador puede conectarse a la máquina virtual de control de DLR desde un host de la subred de la interfaz de administración de la máquina virtual de control o bien sin dicha restricción en "Dirección de protocolo" (Protocol Address) de OSPF o BGP si se configura una dirección de protocolo.

Nota No es posible tener conectividad de red entre la máquina virtual de control de DLR y una dirección IP que se encuentre en una subred configurada en cualquiera de las interfaces "internas" de ese DLR. Esto se produce porque la interfaz de salida de estas subredes en la máquina virtual de control de DLR apunta a la pseudointerfaz VDR, que no está conectada en este plano de datos.

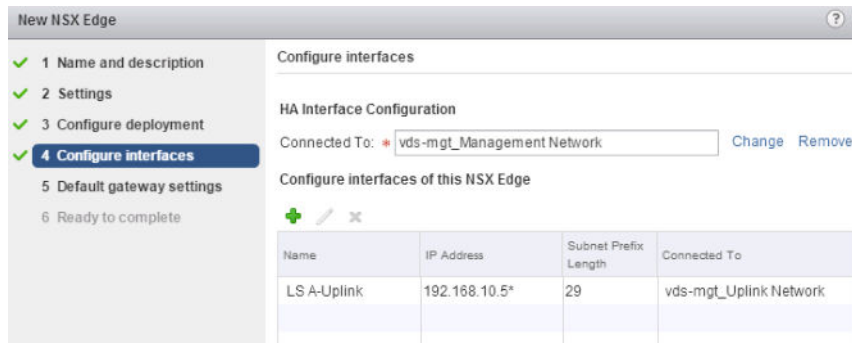
- La opción "Habilitar HA" (Enable HA) implementa la máquina virtual de control como un par HA activo o en espera.
- La opción "Registro de nivel de control de Edge" (Edge Control Level Logging) establece el nivel de registro del sistema en el dispositivo Edge.

En la pantalla "Configurar implementación" (Configure deployment):



- En el campo "Centro de datos" (Datacenter) se selecciona el centro de datos de vCenter en el que se implementará la máquina virtual de control.
- El campo "Dispositivos Edge NSX" (NSX Edge Appliances) hace referencia a la máquina virtual de control de DLR y permite definir exclusivamente uno (tal y como se muestra en la imagen).
 - Si se habilita HA, la instancia Edge en espera se implementará en el mismo clúster, host y almacén de datos. Se creará una regla de "máquinas virtuales distintas" de DRS para las máquinas virtuales de control de DLR activas o en espera.


En la pantalla "Configurar interfaces" (Configure Interfaces):



- Interfaz de HA ("HA Interface")
 - No se crea como una interfaz lógica de DLR compatible con el enrutamiento. Solo es un vNIC en la máquina virtual de control.
 - Esta interfaz no requiere una dirección IP porque NSX administra la configuración de DLR mediante VMCI.
 - Esta interfaz se utiliza para los latidos de HA si la casilla "Habilitar alta disponibilidad" (Enable High Availability) de DLR se marca en la pantalla "Nombre y descripción" (Name and description).
- "Interfaces de este NSX Edge" (Interfaces of this NSX Edge) hacen referencia a las interfaces lógicas de DLR (LIFs)
 - El DLR proporciona servicios de puertas de enlace de Capa 3 a las máquinas virtuales en el dvPortgroup del campo "Conectado a" (Connected To) o en el conmutador lógico con las direcciones IP de las subredes correspondientes.

- Los LIF de tipo "enlace de subida" se crean como vNICs en la máquina virtual de control, por lo que solo se admiten hasta ocho vNIC. Los últimos dos vNIC disponibles se asignan a la interfaz de HA y a un vNIC reservado.
- Se necesita un LIF de tipo "vínculo superior" para que el enrutamiento dinámico funcione en el DLR.
- Los LIF de tipo "interno" se crean como pseudo vNICs en la máquina virtual de control y es posible tener hasta 991 pseudo vNICs.

En la pantalla "Configuración de la puerta de enlace predeterminada" (Default gateway settings):



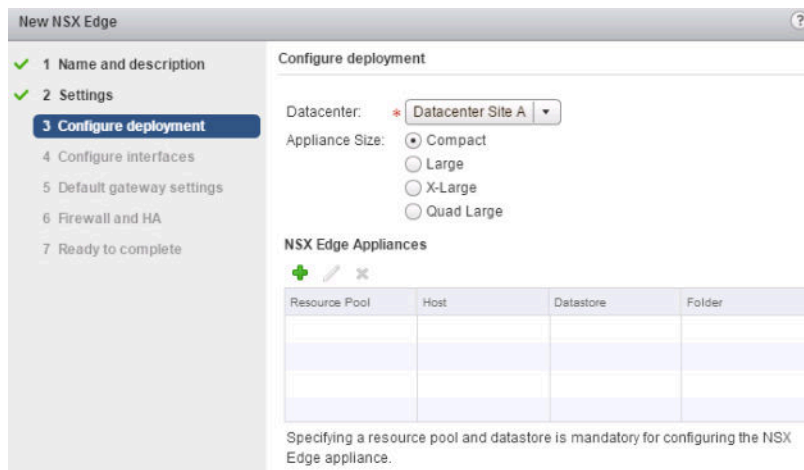
- Si selecciona la opción "Configurar puerta de enlace predeterminada" (Configure Default Gateway), se creará una ruta predeterminada estática en el DLR. Esta opción estará disponible si un LIF de tipo "vínculo superior" se crea en la pantalla anterior.
- Si se utiliza ECMP en el vínculo superior, le recomendamos que deje esta opción deshabilitada para evitar que se produzca una interrupción en el plano de datos si se produce un error en el salto siguiente.

Nota La flecha doble hacia la derecha situada en la esquina superior derecha le permite "suspender" el asistente en curso para que pueda reanudarlo más adelante.

Diferencias entre ESG y DLR

Comparado con DLR, existen algunas diferencias entre los asistentes cuando se implementa un ESG.

La primera es la ventana Configurar implementación (Configure deployment):



En un ESG, la ventana Configurar implementación (Configure deployment) permite seleccionar el tamaño de Edge. Si se utiliza un ESG solo para realizar el enrutamiento, el tamaño que suele ser apropiado en la mayoría de las situaciones es Grande ("Large"). Seleccionar un gran tamaño no proporciona más recursos de la CPU a los procesos de enrutamiento de ESG y tampoco supone un mayor rendimiento.

También es posible crear un ESG sin implementarlo, pero sigue necesitando la configuración de un dispositivo Edge.

Si Edge no está implementado, se puede implementar posteriormente a través de una llamada API o con la opción Implementar (Deploy) de la interfaz de usuario.

Si está seleccionado Edge HA, debe crear al menos una interfaz interna o devolverá un error silenciosamente en HA, llevando a una situación de "cerebro dividido".

La API y la interfaz de usuario de NSX permiten a un operador eliminar la interfaz "interna" que hace que HA falle silenciosamente.

Operaciones habituales de la interfaz de usuario de ESG y DLR

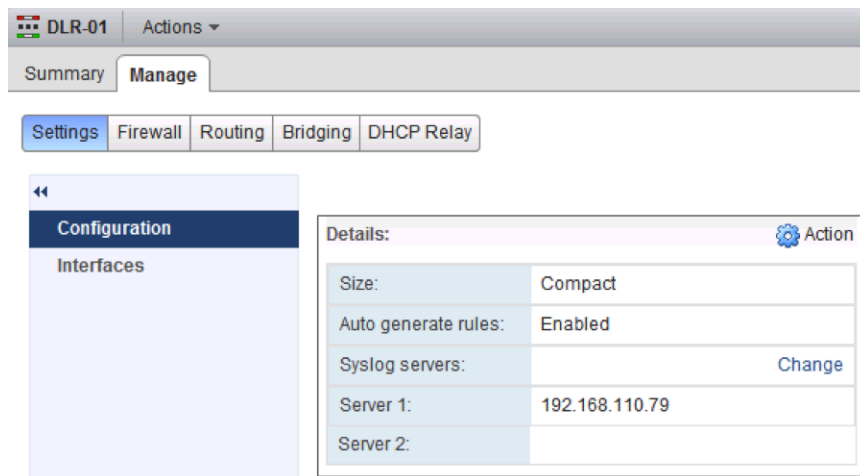
Además de su creación, existen varias operaciones de configuración que se ejecutan normalmente tras la implementación inicial.

Entre ellas se incluyen:

- Configuración del registro del sistema
- Administración de las rutas estáticas
- Configuración de los protocolos y la redistribución de las rutas

Configuración del registro del sistema

Configure la ESG o la máquina virtual de control de DLR para enviar entradas de registro a un servidor de registro del sistema remoto.



Notas:

- El servidor de registro del sistema debe estar configurado como una dirección IP ya que la ESG y la máquina virtual de control de DLR no están configurados con un solucionador DNS.
 - En el caso de la ESG, es posible "Habilitar el servicio DNS" (Enable DNS Service) (DNS proxy) que la propia ESG podrá utilizar para resolver los nombres de DNS, pero especificando de forma general el servidor de registro del sistema como una dirección IP en un método más efectivo con menos dependencias.
- No hay manera de especificar un puerto de registro del sistema en la interfaz de usuario (siempre es 514), pero sí el protocolo (UDP/TCP).
- Los mensajes de registro del sistema se originan desde la dirección IP en la interfaz de Edge que está seleccionada por la tabla de reenvíos de Edge como salida para la IP del servidor de registro del sistema.
 - Para el DLR, la dirección IP del servidor de registro del sistema no puede estar en ninguna subred configurada en cualquiera de las interfaces "internas" (Internal) de DLR. Esto se produce porque la interfaz de salida de estas subredes en la máquina virtual de control de DLR apunta a la pseudointerfaz "VDR", que no está conectada en este plano de datos.

Por defecto, el registro de la ruta ESG/DLR está deshabilitado. Si es necesario, habilítelo en la interfaz de usuario, para ello, haga clic en "Editar" (Edit) para "Configuración del enrutamiento dinámico" (Dynamic Routing Configuration).

The screenshot shows the NSX Manager interface for a DLR-01 object. The 'Manage' tab is active, and the 'Routing' sub-tab is selected. The 'Routing Configuration' section is expanded, showing the following settings:

- ECMP:** Disabled (with an 'Enable' button).
- Default Gateway:** A section with 'Edit' and 'Delete' buttons, containing fields for 'Interface', 'Gateway IP', 'MTU', and 'Description'.
- Dynamic Routing Configuration:** A section with an 'Edit' button, containing fields for 'Router ID', 'OSPF' (Disabled), 'BGP' (Disabled), 'Logging' (Disabled), and 'Log Level'.

También debe configurar el ID del router, que suele ser la dirección IP de la interfaz del enlace de subida.

Rutas estáticas

Las rutas estáticas deben tener configurado el siguiente salto en una dirección IP en una subred asociada a una de los LIF de DLR o de las interfaces de ESG. De lo contrario, la configuración falla.

Si no está seleccionada la interfaz (Interface), para configurarla automáticamente se conecta el siguiente salto a uno conectado directamente a las subredes.

Add Static Route ?

Network: * 10.10.10.0/24
*Network should be entered in CIDR format
 e.g. 192.169.1.0/24*

Next Hop: * 192.168.10.1

Interface: ⓘ

MTU: 1500

Description:

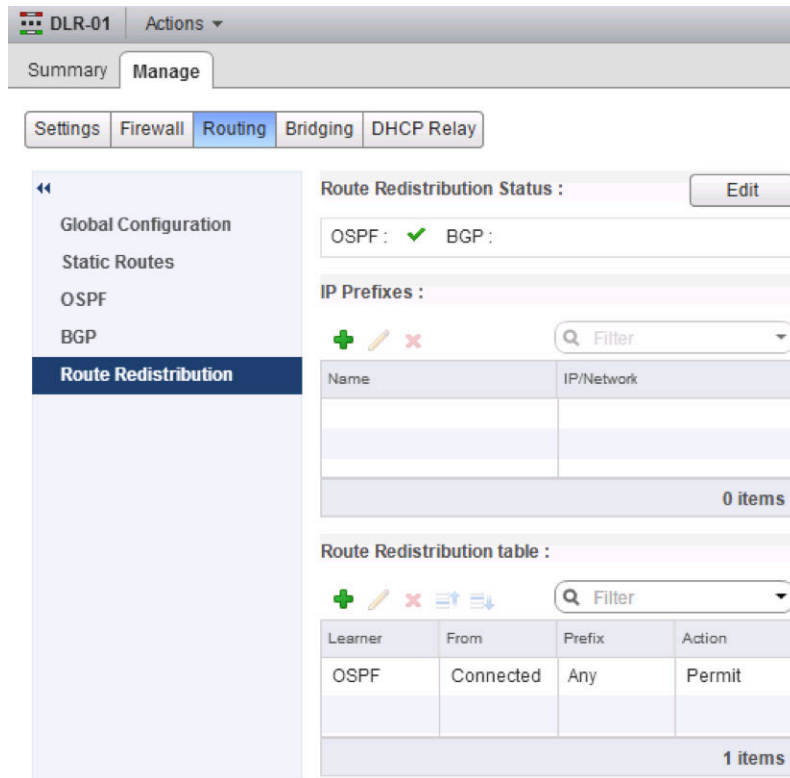
OK Cancel

Redistribución de la ruta

Agregar una entrada en la "tabla de redistribución de la ruta" (Route Redistribution table) no habilita automáticamente la redistribución para el protocolo "Learner" seleccionado. Esto se debe realizar explícitamente a través de "Editar" (Edit) el "Estado de redistribución de la ruta" (Route Redistribution Status).

El DLR se configura con una redistribución de los enrutadores conectados en OSPF por defecto, mientras que la ESG no.

La "tabla de redistribución de la ruta" (Route Redistribution table) se procesa de arriba a abajo y dicho proceso se para tras la primera coincidencia. Para excluir de la redistribución algunos prefijos, incluya más entradas específicas en la parte de arriba.



Resolución de problemas de enrutamiento de NSX

NSX proporciona varias herramientas para asegurar el funcionamiento del enrutamiento.

CLI del enrutamiento de NSX

Hay una serie de comandos de CLI que permiten a los operadores examinar el estado de ejecución de varias partes del subsistema de enrutamiento de NSX.

Debido a la naturaleza distribuida del subsistema de enrutamiento de NSX, hay un varias CLI disponibles, accesibles en varios componentes de NSX. Desde la versión 6.2 de NSX, NSX también centralizó la CLI que ayuda a reducir el tiempo necesario para acceder y registrarse en varios componentes distribuidos. Esto proporciona acceso a la mayor parte de la información desde una única ubicación: el shell de NSX Manager.

Comprobar los requisitos previos

Existen dos requisitos previos principales que cada host ESXi debe cumplir:

- Todos los conmutadores lógicos conectados al DLR deben estar en buen estado.
- El host ESXi debe estar correctamente preparado para VXLAN.

Comprobar el buen estado del conmutador lógico

El enrutamiento de NSX trabaja conjuntamente con el conmutador lógico de NSX. Para comprobar el buen estado de los conmutadores lógicos conectados al DLR:

- Busque el ID del segmento (VNI de VXLAN) de cada conmutador lógico conectado al DLR en cuestión (por ejemplo, 5004..5007).

Logical Switches						
NSX Manager: 192.168.110.42						
<div> + ✗ ✎ ✖ 🔍 ⚙️ Actions </div>						
Name	1 ▲	Status	Transport Zone	Segment ID	Control Plane Mode	Description
LS A		✓ Normal	Global-Transport-Zone	5004	Unicast	
LS B		✓ Normal	Global-Transport-Zone	5005	Unicast	
LS C		✓ Normal	Global-Transport-Zone	5006	Unicast	
LS D		✓ Normal	Global-Transport-Zone	5007	Unicast	

- En los hosts ESXi en los que se esté ejecutando la máquina virtual que utiliza este DLR como servidor, compruebe el plano de control de VXLAN de los conmutadores lógicos conectados a este DLR.

```
# esxcli network vswitch dvs vmware vxlan network list --vds-name=Compute_VDS
```

VXLAN ID	Multicast IP	Control Plane	Controller Connection	Port Count
Count	MAC Entry Count	ARP Entry Count		
5004	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.201	
(up)	2	0		
5005	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202	
(up)	1	0		
5006	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.203	
(up)	1	0		
5007	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202	
(up)	1	0		

Compruebe lo siguiente para cada VXLAN relevante:

- Para conmutadores lógicos en modo híbrido o de unidifusión:
 - El plano de control está "Habilitado" (Enabled).
 - El "proxy de multidifusión" y el "proxy ARP" aparecen en la lista aunque la detección de IP esté deshabilitada.
 - Aparece un dirección IP de controladora válida en la lista en "Controladora" (Controller) y la "Conexión" (Connection) está "activa".
- El recuento de puertos ("Port Count") es correcto: habrá al menos 1, aunque no haya ninguna máquina virtual en ese host conectada al conmutador lógico en cuestión. Este puerto es el vdrPort, que es un puerto dvPort especial conectado al módulo kernel DLR del host ESXi.

- Ejecute el siguiente comando para asegurarse de que el vdrPort está conectado todas las VXLAN relevantes.

```
~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5004
Switch Port ID  VDS Port ID  VMKNIC ID
-----
50331656      53           0
50331650      vdrPort      0

~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5005
Switch Port ID  VDS Port ID  VMKNIC ID
-----
50331650      vdrPort      0
```

- En el ejemplo anterior, VXLAN 5004 tiene una máquina virtual y una conexión DLR, mientras que VXLAN 5005 tiene solo una conexión DLR.
- Compruebe si la máquina virtual apropiada se cableó correctamente con sus VXLAN correspondientes, por ejemplo web-sv-01a en VXLAN 5004.

```
~ # esxcfg-vswitch -l
DVS Name      Num Ports  Used Ports  Configured Ports  MTU  Uplinks
Compute_VDS   1536      10          512              1600  vmnic0

  DVPort ID      In Use      Client
[.skipped..]
  53              1           web-sv-01a.eth0
```

Comprobar la preparación de VXLAN

Como parte de la configuración de VXLAN en un host ESXi, también se instala el módulo kernel DLR, se configura y se conecta a un dvPort en un DVS preparado para VXLAN.

- 1 Ejecute `show cluster all` para obtener el ID del clúster.
- 2 Ejecute `show cluster cluster-id` para obtener el ID del host.
- 3 Ejecute `show logical-router host hostID connection` para obtener la información de estado.

```
nsxmgr-01a# show logical-router host <hostID> connection

Connection Information:
-----

DvsName      VdrPort      NumLifs  VdrVmac
-----
Compute_VDS  vdrPort      4        02:50:56:56:44:52
  Teaming Policy: Default Teaming
  Uplink      : dvUplink1(50331650): 00:50:56:eb:41:d7(Team member)
```

Stats : Pkt Dropped	Pkt Replaced	Pkt Skipped
Input : 0	0	1968734458
Output : 303	7799	31891126

- El DVS habilitado con VXLAN tendrá creado un vdrPort, compartido por todas las instancias de DLR de dicho host ESXi.
- "NumLifs" hace referencia al número que se obtiene a partir de la suma de los LIF de todas las instancias de DLR que hay en este host.
- "VdrVmac" es la vMAC que el DLR usa en todos los LIF en todas las instancias. Esta MAC es la misma en todos los hosts. No se ven en ninguna trama que viaje por la red física fuera de los hosts ESXi.
- Para cada dvUplink de DVS habilitado con VXLAN, existe una conexión VTEP, excepto en casos en los que se utiliza LACP / modo de formación de equipo Etherchannel, cuando solo se crea un VTEP independientemente del número de dvUplinks.
 - El tráfico enrutado por el DLR (SRC MAC = vMAC) cuando abandone el host obtendrá el SRC MAC cambiado a pMAC del correspondiente dvUplink.
 - Tenga en cuenta que el origen de la máquina virtual original se usa para determinar el dvUplink (en cada paquete, se conserva en sus metadatos de DVS).
 - Si hay varios VTEP en el host y uno de los dvUplinks falla, el VTEP asociado con el dvUplink fallido se enviará a uno de los dvUplinks restantes junto con todas las máquinas virtuales que están ancladas a ese VTEP. Esto se realiza para evitar cambios que congestionen el plano de control que puedan estar asociados con el desplazamiento de varias máquinas virtuales a distintos VTEP.
- El número que hay entre "()" junto a cada "dvUplinkX" es el número del dvPort. Resulta útil para la captura de paquetes en el enlace de subida individual.
- La dirección MAC que se muestra para cada "dvUplinkX" es una "pMAC" asociada a ese dvUplink. Esta dirección MAC se utiliza para el tráfico de origen desde el DLR, por ejemplo, las consultas ARP generadas por el DLR y cualquier paquete enrutado por el DLR cuando dichos paquetes abandonan el host ESXi. Esta dirección MAC se puede ver en la red física (directamente, si el LIF de DLR es de tipo VLAN o dentro de los paquetes VXLAN para los LIF de VXLAN).
- Pkt Dropped / Replaced / Skipped hace referencia a los recuentos relacionados con los detalles de implementación interna del DLR y no se suelen utilizar para solucionar problemas o supervisar.

Resumen breve del enrutamiento

Para solucionar correctamente los problemas relacionados con el enrutamiento, le recomendamos que consulte su funcionamiento y las tablas de información relacionadas.

- 1 Reciba un paquete para enviarlo a una dirección IP de destino.
- 2 Consulte la tabla de enrutamiento y determine la dirección IP del salto siguiente.

- 3 Determine cuál de sus interfaces de red puede llegar a él.
- 4 Obtenga una dirección MAC del salto siguiente mencionado (mediante ARP).
- 5 Cree una trama de Capa 2.
- 6 Saque la trama de la interfaz.

Para llevar a cabo el enrutamiento, necesita:

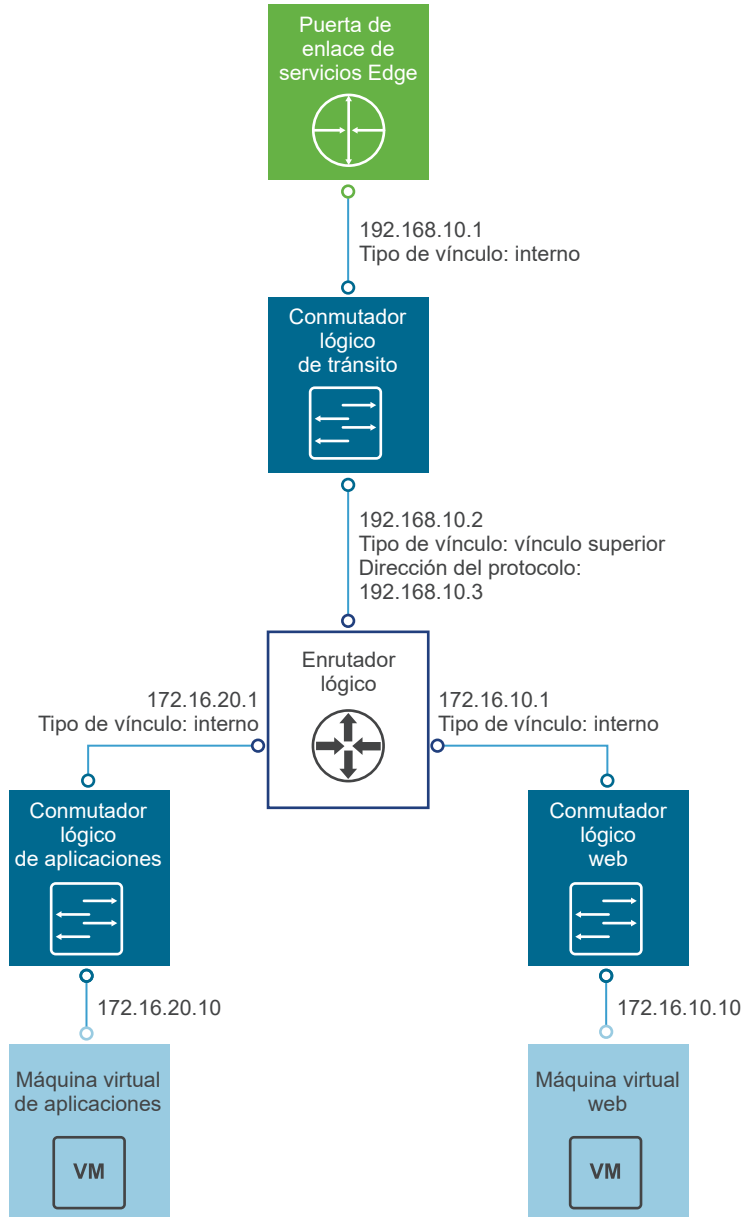
- Una tabla de interfaz (con las máscaras de red y las direcciones IP de la interfaz)
- Una tabla de enrutamiento
- Una tabla ARP

Comprobar el estado del DLR mediante una muestra de topología en red

Esta sección le informa sobre cómo verificar la información que el DLR necesita para enrutar los paquetes.

Use una muestra de topología en red y establezca una configuración de conmutadores lógicos y un DLR para crear en NSX.

Figura 3-7. Muestra de topología en red



El siguiente diagrama muestra:

- 4 conmutadores lógicos, cada uno con su propia subred
- 3 máquinas virtuales conectadas a través de un conmutador lógico
 - Cada una tiene su propia dirección IP y su propia puerta de enlace IP
 - Cada una tiene una dirección MAC (se muestran los dos últimos octetos)
- Uno de los DLR está conectado a los cuatro conmutadores lógicos; de los cuales, uno es para el enlace de subida («Uplink»), mientras que el resto son internos.
- Una puerta de enlace externa, que puede ser una ESG, sirve como puerta de enlace ascendente para el DLR.

El asistente Listo para finalizar (Ready to complete) aparece para dicho DLR.

New NSX Edge

Ready to complete

Name and description
 Name: DLR1
 Install Type: Logical (Distributed) Router
 Tenant:
 HA: Disabled

Management Interface Configuration
 Connected To: Mgmt_Edge_VDS - Mgmt

IP Address	Subnet Prefix Length

NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
Management and Edge Cluster		ds-site-a-nfs01	

Interfaces

Name	IP Address	Subnet Prefix Length	Connected To
LS A	172.16.10.1*	24	LS A
LS B	172.16.20.1*	24	LS B
LS C	172.16.30.1*	24	LS C
LS D	192.168.10.2*	29	LS D

Back Next Finish Cancel

Cuando se finaliza la implementación del DLR, los comandos de la CLI de ESXi se pueden usar para comprobar y validar los estados de distribución del DLR en cuestión en los hosts participantes.

Confirmación de instancias de DLR

Lo primero que se debe confirmar es si se creó la instancia de DLR y si su plano de control está activo.

- 1 En el shell de NSX Manager, ejecute `show cluster all` para obtener el ID del clúster.
- 2 Ejecute `show cluster cluster-id` para obtener el ID del host.
- 3 Ejecute `show logical-router host hostID dlr all verbose` para obtener la información de estado.

```
nsxmgr# show logical-router host host-id dlr all verbose
```

VDR Instance Information :

```
-----
Vdr Name:          default+edge-1
Vdr Id:            1460487509
Number of Lifes:   4
Number of Routes:  5
State:             Enabled
Controller IP:     192.168.110.201
Control Plane Active: Yes
Control Plane IP:  192.168.210.51
Edge Active:       No
```


Puntos que debe tener en cuenta:

- Este comando muestra todas las instancias de DLR que se encuentran en un host ESXi dado.
- “Nombre de Vdr” consta de “Arrendatario” + “Id de Edge Id”. En el ejemplo, “Arrendatario” no se especificó, por tanto, se utiliza la palabra “predeterminado”. El “Id de Edge” es “edge-1”, lo que se puede ver en la interfaz de usuario de NSX.
 - En los casos en los que haya muchas instancias de DLR en un host, una forma de encontrar la instancia correcta es buscar el “ID de Edge” que aparece en “NSX Edges” de la interfaz de usuario.
- “Id de Vdr” resulta útil para realizar más búsquedas, incluidos los registros.
- “Número de Lifs” hace referencia a las LIF que hay en esta instancia de DLR individual.
- El “Número de rutas” es, en este caso 5, y se compone de 4 rutas directamente conectadas (una para cada LIF) y una ruta predeterminada.
- “Estado”, “IP de controladora” y “Plano de control activo” hacen referencia al estado del plano de control del DLR y debe mostrar la IP correcta de la controladora, con plano de control activo: sí. Recuerde que la función de DLR necesita controladoras en funcionamiento; los resultados anteriores muestran lo que debe mostrarse para una instancia de un DLR en buen estado.
- “IP de plano de control” hace referencia a la dirección IP que el host ESXi utiliza para comunicarse con la controladora. Esta IP es siempre la que está asociada al vmknics de administración del host ESXi, que en la mayoría de los casos es vmk0.
- “Edge activo” muestra si es o no en este host donde se está ejecutando la máquina virtual de control para esta instancia de DLR y si está en estado activo.
 - La colocación de la máquina virtual de control de DLR activo determina qué host ESXi se utiliza para realizar un puente de Capa 2 de NSX, si está habilitado.
- También existe una “breve” versión del comando anterior que genera unos resultados resumidos para una introducción rápida. Tenga en cuenta que “Id de Vdr” se muestra aquí en formato hexadecimal:

```
nsxmgr# show logical-router host host-id dlr all brief
```

VDR Instance Information :

State Legend: [A: Active], [D: Deleting], [X: Deleted], [I: Init]

State Legend: [SF-R: Soft Flush Route], [SF-L: Soft Flush LIF]

Vdr Name	Vdr Id	#Lifs	#Routes	State	Controller Ip	CP Ip
-----	-----	-----	-----	-----	-----	-----
default+edge-1	0x570d4555	4	5	A	192.168.110.201	192.168.210.51

Los estados de “vaciado ligero” hacen referencia a estados transitorios breves del ciclo de vida de LIF y no se suelen ver en un DLR en buen estado.

Interfaces lógicas de DLR

Tras comprobar que se ha creado el DLR, asegúrese de que están presentes todas las interfaces lógicas de DLR y que tienen la configuración correcta.

- 1 En el shell de NSX Manager, ejecute `show cluster all` para obtener el ID del clúster.
- 2 Ejecute `show cluster cluster-id` para obtener el ID del host.
- 3 Ejecute `show logical-router host hostID dlr all brief` para obtener el dlrID (Vdr Name).
- 4 Ejecute `show logical-router host hostID dlr dlrID interface all brief` para obtener un resumen de la información del estado de todas las interfaces.
- 5 Ejecute `show logical-router host hostID dlr dlrID interface (all | intName) verbose` para obtener la información del estado de todas las interfaces o para una interfaz específica.

```
nsxmgr# show logical-router host hostID dlr dlrID interface all verbose
```

VDR default+edge-1:1460487509 LIF Information :

```
Name:          570d45550000000a
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5000
Ip(Mask):      172.16.10.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2388
DHCP Relay:    Not enabled
```

```
Name:          570d45550000000c
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5002
Ip(Mask):      172.16.30.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2288
DHCP Relay:    Not enabled
```

```
Name:          570d45550000000b
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5001
Ip(Mask):      172.16.20.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2388
DHCP Relay:    Not enabled
```

```

Name:          570d455500000002
Mode:          Routing, Distributed, Uplink
Id:            Vxlan:5003
Ip(Mask):      192.168.10.2(255.255.255.248)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2208
DHCP Relay:    Not enabled
  
```

Puntos que debe tener en cuenta:

- El nombre ("Name") del LIF es único en todas las instancias del DLR en el host. Es el mismo en los hosts y en el nodo de la controladora principal de DLR.
- El modo ("Mode") del LIF muestra si este está enrutado o actúa como puente y si es interno o un enlace de subida.
- La "Id" muestra el tipo de LIF y la ID del servicio correspondiente (VXLAN y VNI o VLAN y VID).
- "IpMask" se muestra para los LIF enrutados ("Routing").
- Si se conecta un LIF a una VXLAN en modo híbrido o de unidifusión, el plano de control de VXLAN ("VXLAN Control Plane") está habilitado ("Enabled").
- Para los LIF de VXLAN donde la VXLAN tiene un modo de unidifusión, se muestra la IP de multidifusión de VXLAN ("VXLAN Multicast IP") como "0.0.0.1"; de lo contrario, se muestra la dirección IP de multidifusión actual.
- El estado ("State") debe aparecer habilitado ("Enabled") para los LIF en red. Para los LIF en puente, está habilitado ("Enabled") en el host que actúe como puente e Iniciado ("Inhit") en el resto de hosts.
- Las marcas ("Flags") es un resumen de la presentación en el estado del LIF y muestra:
 - si el LIF está enrutado o en puente.
 - si el LIF de VLAN es una DI.
 - si tiene habilitada una transmisión DHCP.
 - Es importante la marca 0x0100, que se configura cuando el DLR causa una unión de VNI de VXLAN (en oposición a un host que tiene una máquina virtual en esa VXLAN)
 - Las marcas se muestran en un formato más cómodo para la lectura en el modo breve ("brief").

```
nsxmgr# show logical-router host hostID dlr dlrID interface all brief
```

VDR default+edge-1 LIF Information :

```

State Legend: [A:Active], [d:Deleting], [X:Deleted], [I:Init],[SF-L:Soft Flush LIF]
Modes Legend: [B:Bridging],[E: Empty], [R:Routing],[S:Sedimented],[D:Distributed]
Modes Legend: [In:Internal],[Up:Uplink]
  
```

Lif Name	Id	Mode	State	Ip(Mask)
-----	--	-----	-----	-----
570d455500000000a	Vxlan:5001	R,D,In	A	172.16.10.1(255.255.255.0)
570d455500000000c	Vxlan:5003	R,D,In	A	172.16.30.1(255.255.255.0)
570d455500000000b	Vxlan:5002	R,D,In	A	172.16.20.1(255.255.255.0)
570d4555000000002	Vxlan:5000	R,D,Up	A	192.168.10.5(255.255.255.248)

Rutas de DLR

Tras establecer que aparece un DLR en buen estado y que cuenta con todos los LIF, lo siguiente que debe comprobar es la tabla de enrutamiento.

- 1 En el shell de NSX Manager, ejecute `show cluster all` para obtener el ID del clúster.
- 2 Ejecute `show cluster cluster-id` para obtener el ID del host.
- 3 Ejecute `show logical-router host hostID dlr all brief` para obtener el dlrID (Vdr Name).
- 4 Ejecute `show logical-router host hostID dlr dlrID route` para obtener la información del estado de todas las interfaces.

```
nsxmgr# show logical-router host hostID dlr dlrID route
```

VDR default+edge-1:1460487509 Route Table
 Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
 Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
-----	-----	-----	-----	---	-----	-----	-----
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	10068944	570d4555000000002
172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000000a
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000000b
172.16.30.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000000c
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10068944	570d4555000000002

Puntos que debe tener en cuenta:

- La Interfaz ("Interface") muestra el LIF de salida que se seleccionará para la Destinación ("Destination") correspondiente. Esto se configura al nombre del LIF ("Lif Name") de uno de los LIF del DLR.
- Para las rutas ECMP, existen más de una ruta con la misma destinación (Destination), GenMask e interfaz (Interface), pero con una puerta de enlace diferente. También se incluye la marca "E" para mostrar la naturaleza ECMP de estas rutas.

Tabla ARP de DLR

El DLR debe poder resolver las solicitudes de ARP del salto siguiente de la dirección IP para los paquetes que reenvía. Los resultados del proceso de resolución están almacenados de forma local en las instancias de DLR de los hosts individuales.

Los controladores no tienen ninguna función en este proceso y no se utilizan para distribuir las entradas de ARP resultantes a otros hosts.

Las entradas inactivas en caché se almacenan durante 600 segundos, luego se eliminan. Para tener más información sobre el proceso de resolución de ARP de DLR, consulte [Proceso de resolución del ARP de DLR](#).

- 1 En el shell de NSX Manager, ejecute `show cluster all` para obtener el ID del clúster.
- 2 Ejecute `show cluster cluster-id` para obtener el ID del host.
- 3 Ejecute `show logical-router host hostID dlr all brief` para obtener el dlrID (Vdr Name).
- 4 Ejecute `show logical-router host hostID dlr dlrID arp` para obtener la información del estado de todas las interfaces.

```
nsxmgr# show logical-router host hostID dlr dlrID arp
```

VDR default+edge-1:1460487509 ARP Information :

Legend: [S: Static], [V: Valid], [P: Proxy], [I: Interface]

Legend: [N: Nascent], [L: Local], [D: Deleted]

Network	Mac	Flags	Expiry	SrcPort	Interface	Refcnt
-----	---	-----	-----	-----	-----	-----
172.16.10.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000a	1
172.16.10.11	00:50:56:a6:7a:a2	VL	147	50331657	570d45550000000a	2
172.16.30.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000c	1
172.16.30.11	00:50:56:a6:ba:09	V	583	50331650	570d45550000000c	2
172.16.20.11	00:50:56:a6:84:52	VL	568	50331658	570d45550000000b	2
172.16.20.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000b	1
192.168.10.2	02:50:56:56:44:52	VI	permanent	0	570d455500000002	1
192.168.10.1	00:50:56:8e:ee:ce	V	147	50331650	570d455500000002	1

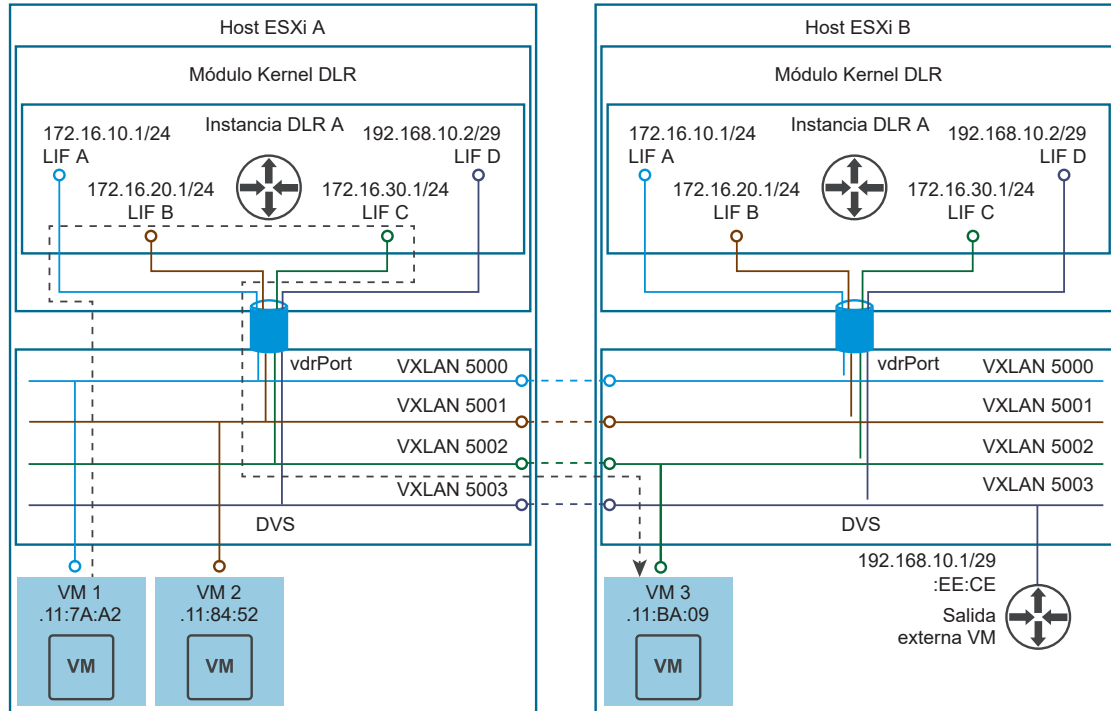
Tenga en cuenta:

- Todas las entradas de ARP para los propios LIF de DLR (marca "I") son las mismas y se muestran en el mismo vMAC que se menciona en [Comprobar la preparación de VXLAN](#).
- Las entadas de ARP con la marca "L" se corresponden con las máquinas virtuales que se ejecutan en el host donde se ejecuta el comando de la CLI.
- SrcPort muestra la ID de dvPort donde se originó la entrada ARP. En los casos en los que una entrada ARP se origine en otro host, se muestra la ID de dvPort de dvUplink. Esta ID del dvPort puede ser una referencia cruzada con la ID de dvPort de dvUplink mencionada en [Comprobar la preparación de VXLAN](#)
- No suele aparecer la marca "Nascent". Se configura mientras el DLR espera la llegada de la respuesta de ARP. Cualquier entrada con esta marca puede indicar que existe un problema con la resolución de ARP.

DLR y los componentes del host relacionado que están visibles

El diagrama siguiente muestra dos hosts: el host ESXi A y el host ESXi B, donde nuestro ejemplo "Instancia de DLR A" está configurado para las cuatro LIF de VXLAN y conectado a ellas.

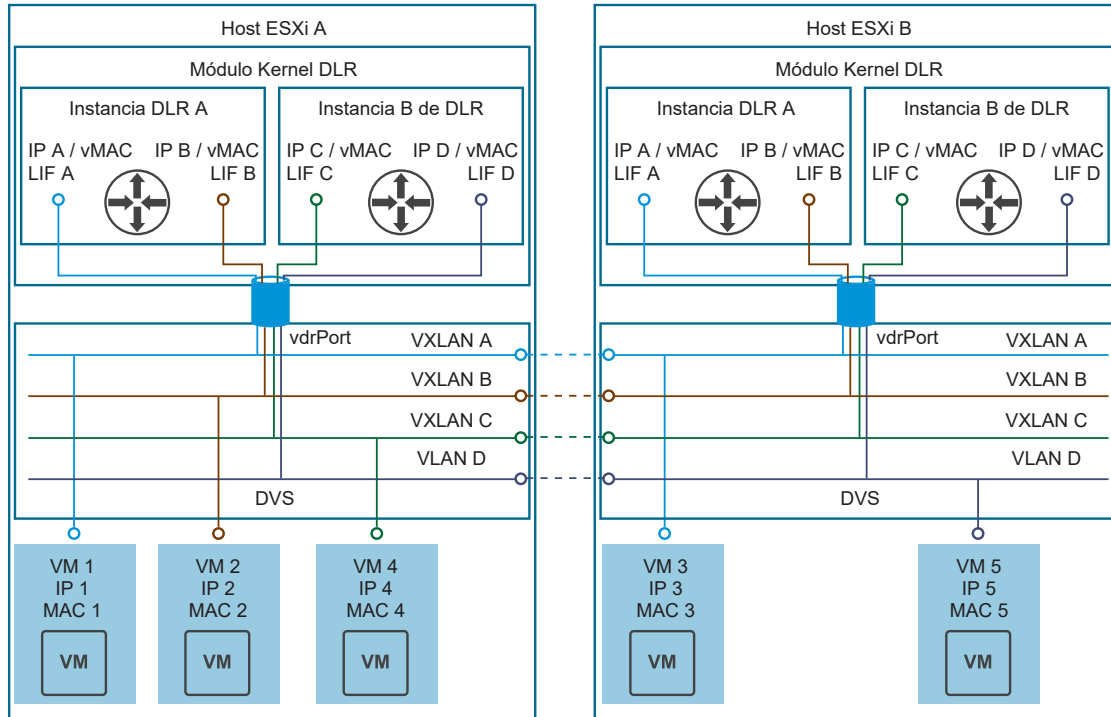
Figura 3-8. Dos hosts con una instancia de DLR simple



- Cada host tiene un conmutador Capa 2 (DVS) y un "Router on a stick" (módulo kernel DLR) conectado a ese conmutador a través de una interfaz troncal (vdrPort).
 - Tenga en cuenta que este tronco puede conectar todas las VLAN y VXLAN; sin embargo, no existen 801.Q ni encabezados de UDP o VXLAN presentes en estos paquetes que pasen por vdrPort. Sin embargo, DVS usa un método de etiquetado de los metadatos internos para enviar esta información al módulo kernel DLR.
- Cuando el DVS capta una trama con destino MAC = vMAC, sabe que es por el DLR y reenvía esa trama a vdrPort.
- Tras la llegada de los paquetes al módulo kernel de DLR a través del vdrPort, se examinan sus metadatos para determinar a qué VNI de VXLAN o ID de VLAN pertenecen. Esta información se usa para determinar a qué LIF o a qué instancia de DLR pertenece ese paquete.
 - El efecto secundario de este sistema es que no se puede conectar más de una instancia de DLR a una VLAN o VXLAN ya dada.

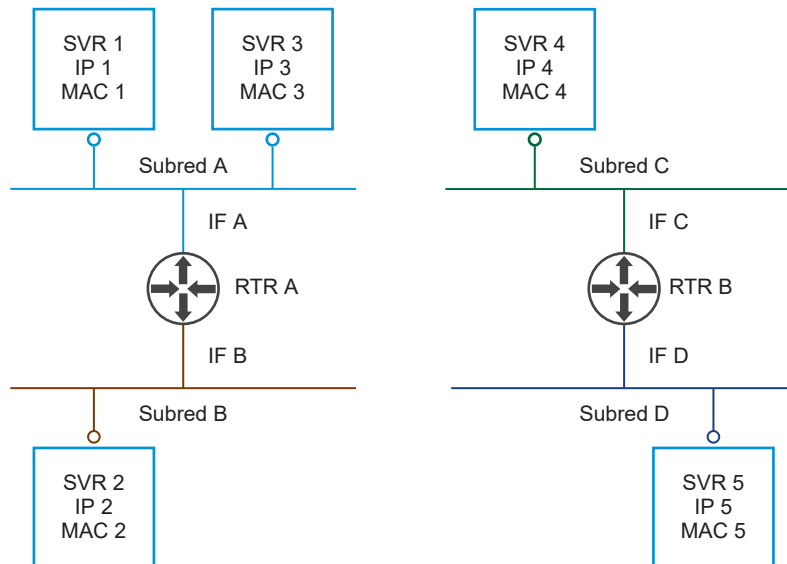
En los casos en los que exista más de una instancia de DLR, el diagrama anterior pasa a ser el siguiente:

Figura 3-9. Dos hosts con dos instancias de DLR



Esto correspondería a una topología de red con dos dominios de red independientes que operan totalmente separados uno de otro, potencialmente con direcciones IP superpuestas.

Figura 3-10. Topología de red que se corresponde con dos hosts y dos instancias de DLR



Arquitectura del subsistema de enrutamiento distribuido

Las instancias de DLR de los hosts de ESXi tienen acceso a toda la información que se necesita para realizar un enrutamiento de Capa 3.

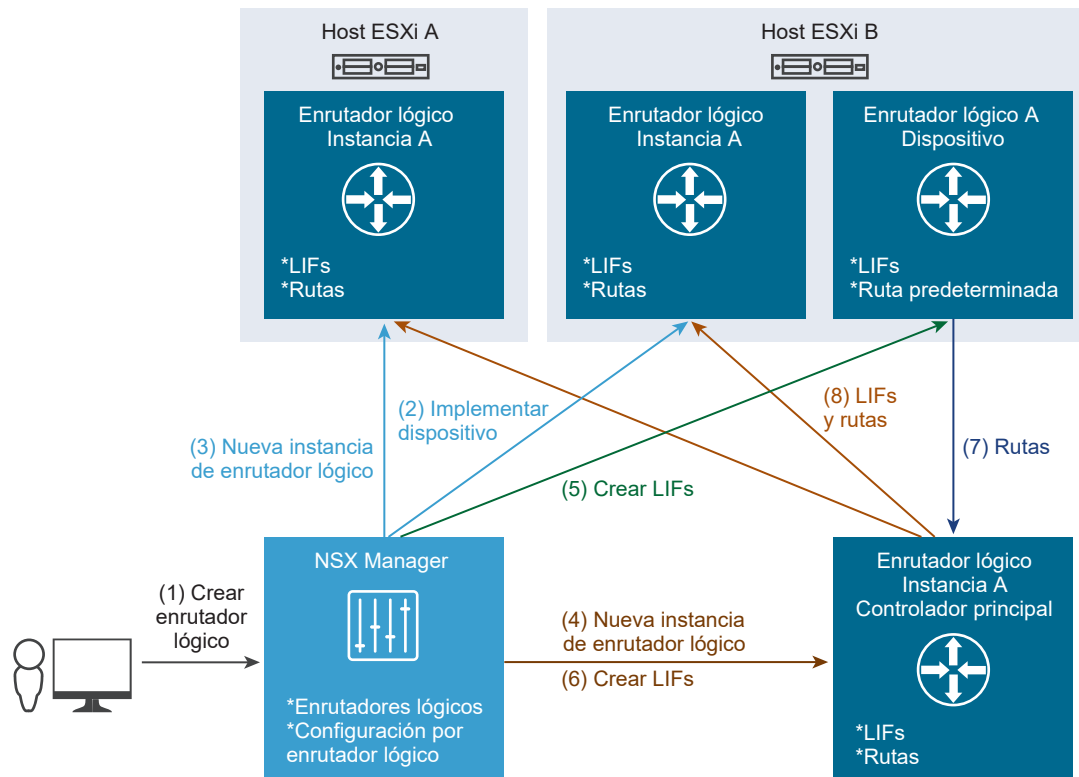
- Las redes se conectan directamente (esta función la adquieren de la configuración de las interfaces).
- Saltos siguientes de cada subred (se buscan en la tabla de enrutamiento)
- Dirección MAC que se va a introducir en las tramas de salida para comunicarse con los saltos siguientes (tabla ARP)

Esta información se envía a las instancias distribuidas en varios hosts ESXi.

Proceso de creación de DLR

El diagrama siguiente es una ilustración de alto nivel del proceso que NSX sigue para crear un nuevo DLR.

Figura 3-11. Proceso de creación de DLR



Al enviar un asistente de interfaz de usuario mediante el botón “Finalizar” o realizar una llamada API para implementar un nuevo DLR, el sistema procesa los pasos siguientes:

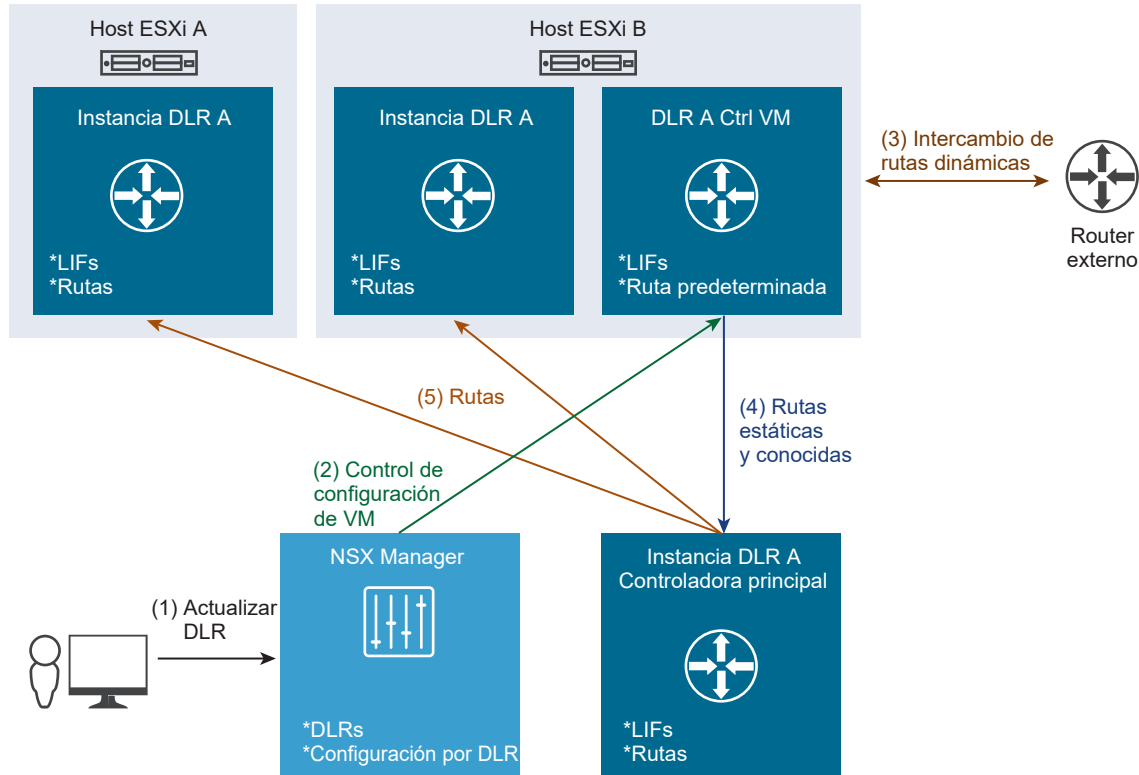
- 1 NSX Manager recibe una llamada API para implementar un nuevo DLR (directamente o desde vSphere Web Client, invocado por el asistente de interfaz de usuario).

- 2 NSX Manager realiza una llamada a su vCenter Server vinculado para implementar una máquina virtual de control de DLR (o un par si se solicitó HA).
 - a La máquina virtual de control de DLR se enciende y se vuelve a conectar a NSX Manager, que está listo para recibir la configuración.
 - b Si se implementó un par HA, NSX Manager configura una regla de antiafinidad que mantendrá al par HA ejecutándose en distintos hosts. A continuación, DRS realiza las acciones necesarias para separarlo.
- 3 NSX Manager crea una instancia de DLR en los hosts:
 - a NSX Manager busca los conmutadores lógicos que se van a conectar al nuevo DLR para determinar a qué zona de transporte pertenecen.
 - b A continuación busca una lista de los clústeres que están configurados en esta zona de transporte y crea el nuevo DLR en todos los hosts de estos clústeres.
 - c Llegado este punto, los hosts sólo conocen el ID del nuevo DLR, pero no disponen de la información correspondiente (sobre las LIF ni las rutas).
- 4 NSX Manager crea una instancia del nuevo DLR en el clúster de la controladora.
 - a El clúster de la controladora asigna uno de los nodos de la controladora para que sea el nodo principal de esta instancia de DLR.
- 5 NSX Manager envía la configuración, incluidas las LIF, a la máquina virtual de control de DLR.
 - a Los hosts ESXi (incluido el host en el que se está ejecutando la máquina virtual de control de DLR) reciben información de segmentación del clúster de la controladora, determinan qué nodo de la controladora es responsable de la instancia del nuevo DLR y se conectan al nodo de la controladora (si no existe ninguna conexión).
- 6 Tras la creación de LIF en la máquina virtual de control de DLR, NSX Manager crea las LIF del nuevo DLR en el clúster de la controladora.
- 7 La máquina virtual de control de DLR se conecta al nodo de la controladora de la instancia del nuevo DLR y envía al nodo de la controladora las rutas:
 - a En primer lugar, el DLR traduce su tabla de enrutamiento a la tabla de reenvío (mediante la resolución de prefijos para las LIF).
 - b A continuación, el DLR envía la tabla resultante al nodo de la controladora.
- 8 El nodo de la controladora envía las LIF y las rutas a otros hosts en los que existe la instancia del nuevo DLR a través de la conexión establecida en el paso 5.a.

Agregar enrutamiento dinámico a DLR

Cuando el DLR se crea mediante una llamada "directa" de API (en lugar de utilizar la interfaz de usuario de vSphere Web Client), es posible suministrarlo con una configuración completa que incluya el enrutamiento dinámico(1).

Figura 3-12. Enrutamiento dinámico en el DLR



- 1 NSX Manager recibe una llamada API para cambiar la configuración de DLR existente, en este caso, para agregar el enrutamiento dinámico.
- 2 NSX Manager envía la configuración nueva a la máquina virtual de control de DLR.
- 3 La máquina virtual de control de DLR aplica la configuración y sigue el proceso de establecimiento de las adyacencias del enrutamiento, de intercambio de información del enrutamiento, etc.
- 4 Después de que se realice el intercambio de enrutamiento, la máquina virtual de control de DLR calcula la tabla de reenvío y la envía al nodo de la controladora principal de DLR.
- 5 El nodo de la controladora principal de DLR distribuye las rutas actualizadas a los hosts ESXi en los que se encuentra la instancia de DLR.

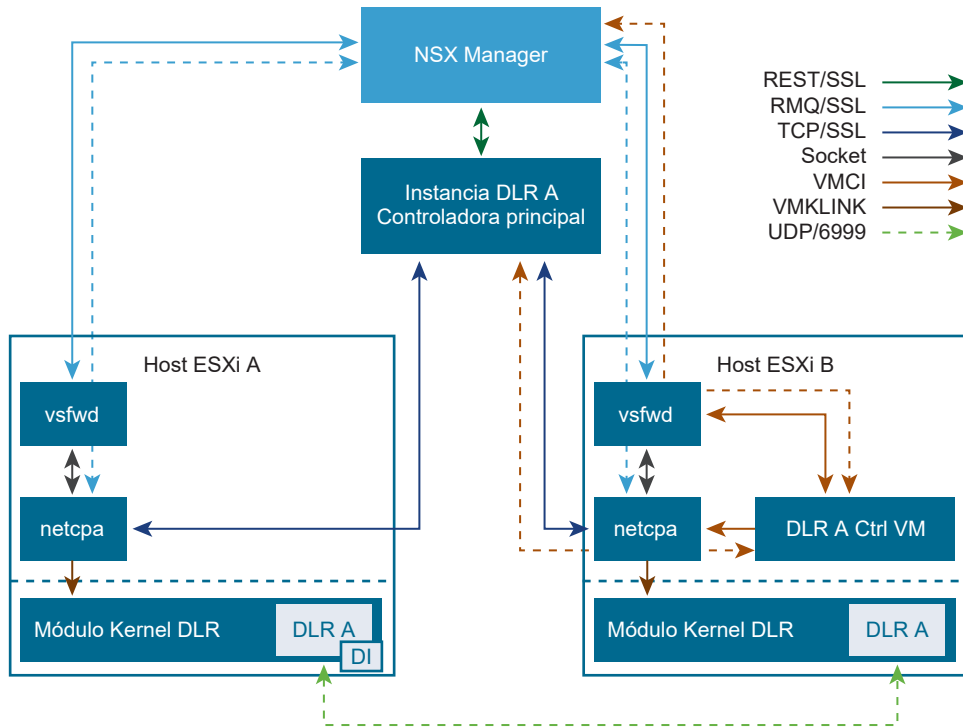
Tenga en cuenta que la instancia de DLR del host ESXi donde se está ejecutando la máquina virtual de control de DLR recibe sus LIF y sus rutas únicamente desde el nodo de la controladora principal del DLR y nunca directamente desde la máquina virtual de control de DLR ni de NSX Manager.

Comunicaciones y componentes del plano de administración y control de DLR

En esta sección se proporciona una breve introducción sobre los componentes de los planos de administración y control de DLR.

Esta figura muestra los componentes y los canales de comunicación correspondientes entre ellos.

Figura 3-13. Componentes del plano de administración y control de DLR



- **NSX Manager:**
 - Tiene comunicación directa con el clúster de la controladora
 - Tiene una conexión permanente y directa con el proceso del cliente de bus de mensajería (**vsfwd**) que se ejecuta en cada host preparado para NSX
- Para cada instancia de DLR, un nodo de la controladora (de los 3 disponibles) se elige como el principal
 - La función principal puede desplazarse a otro nodo de la controladora si se produce algún error en el nodo de la controladora original
- Cada host ESXi ejecuta dos agentes del ámbito del usuario (UWA): el cliente del bus de mensajería (**vsfwd**) y el agente de plano de control (**netcpa**)
 - **netcpa** solicita información de NSX Manager para poder funcionar (por ejemplo, dónde puede encontrar controladoras y cómo puede autenticarse en ellas). A esta información se accede mediante la conexión de bus de mensajería que proporciona **vsfwd**
 - **netcpa** también se comunican con el módulo kernel DLR para programarlo con la información relevante que recibe de las controladoras
- Para cada instancia de DLR, hay una máquina virtual de control de DLR que se ejecuta en uno de los hosts ESXi. La máquina virtual del control de DLR tiene dos canales de comunicación:
 - El canal **VMCI** con NSX Manager mediante **vsfwd**, que se utiliza para configurar la máquina virtual de control

- El canal VMCI con la controladora principal de DLR mediante netcpa, que se utiliza para enviar la tabla de enrutamiento de DLR a la controladora
- En los casos en los que el DLR tenga una LIF de VLAN, la controladora designa uno de los hosts ESXi participantes como una instancia designada (DI). El módulo kernel DLR de otros hosts ESXi solicita que la DI realice las consultas de ARP del proxy en el VLAN asociado.

Componentes del subsistema de enrutamiento de NSX

El subsistema de enrutamiento de NSX se habilita mediante varios componentes.

- NSX Manager
- Clúster de controladoras
- Módulos del host ESXi (kernel y UWA)
- Máquinas virtuales de control de DLR
- ESGs

NSX Manager

NSX Manager proporciona las siguientes funciones relevantes para el enrutamiento de NSX:

- Actúa como un plano de administración centralizada que proporciona el punto de acceso de API unificado de todas las operaciones de administración de NSX
- Instala los agentes del ámbito del usuario y el módulo kernel de enrutamiento distribuido en los hosts para prepararlos para las funciones de NSX
- Crea o destruye los LIF de DLR y los DLR
- Implementa o elimina la máquina virtual de control de DLR a través de vCenter
- Configura el clúster de la controladora a través de los hosts y la API de REST mediante un bus de mensajería:
 - Proporciona agentes de plano de control del host con las direcciones IP de las controladoras
 - Genera y distribuye los certificados a los hosts y las controladoras para proteger las comunicaciones de plano de control
- Configura ESGs y máquinas virtuales de control de DLR a través del bus de mensajería
 - Tenga en cuenta que las ESG pueden implementarse en hosts no preparados, en cuyo caso VIX se utilizará en lugar del bus de mensajería

Clúster de controladoras

El enrutamiento distribuido de NSX necesita controladoras integrados en un clúster para escalarlos y para que estén disponibles. Estos proporcionan las siguientes funciones:

- Admitir el plano de control de enrutamiento lógico y el VXLAN
- Proporcionar la interfaz CLI para los estados del tiempo de ejecución y las estadísticas

- Elegir un nodo de la controladora principal para cada instancia de DLR
 - El nodo principal recibe la información de enrutamiento de la máquina virtual de control de DLR y la distribuye a los hosts
 - Envía la tabla de LIF a los hosts
 - Realiza un seguimiento del host en el que se encuentra la máquina virtual de control de DLR
 - Selecciona la instancia designada para los LIF de VLAN y comunica esta información a los hosts. Supervisa el host de DI a través de los keepalive del plano de control (el tiempo de espera es de 30 segundos y el tiempo de detección oscila entre 20 y 40 segundos). Envía una actualización a los hosts si el host de DI desaparece

Módulos del host ESXi

El enrutamiento de NSX utiliza directamente dos agentes del ámbito del usuario (UWA) y un módulo kernel de enrutamiento. Se basa en el módulo kernel de VXLAN para la conectividad VXLAN.

A continuación le indicamos un resumen de las funciones de cada uno de estos componentes:

- El agente del plano de control (netcpa) es un cliente TCP (SSL) que se comunica con la controladora a través del protocolo del plano de control. Puede conectarse a varias controladoras. netcpa se comunica con el cliente del bus de mensajería (vsfwd) para recuperar la información relacionada con el plano de control de NSX Manager.
- Implementación y empaquetado de netcpa:
 - El agente se empaqueta en el VIB de VXLAN (paquete de instalación de vSphere)
 - NSX Manager lo instala a través de EAM (ESX Agent Manager) durante la preparación del host
 - Se ejecuta como un demonio de servicio en netcpa ESXi
 - Se puede iniciar, detener o consultar a través de su script de inicio /etc/init.d/netcpad
 - Se puede reiniciar de forma remota a través de Instalación de interfaz de usuario de Networking and Security (Networking and Security UI Installation) -> Preparación del host (Host Preparation) -> Estado de instalación (Installation Status) en los hosts individuales o en un clúster completo
- El módulo kernel DLR (vdrb) se integra con el DVS para habilitar el reenvío de Capa 3
 - Configurado por netcpa
 - Se instala como parte de la implementación del VIB de VXLAN
 - Se conecta al DVS a través de un tronco especial denominado "vdrPort", que admite redes VLAN y VXLAN
 - Contiene la siguiente información para cada instancia de DLR:
 - Tablas de rutas y LIF
 - Caché de ARP local del host

- Las máquinas virtuales de control de DLR, las ESG y netcpa utilizan el cliente del bus de mensajería (vsfwd) para comunicarse con NSX Manager
 - vsfwd obtiene la dirección IP de NSX Manager de /UserVars/RmqIpAddress que establece vCenter a través de vpxa o hosd e inicia sesión en el servidor del bus de mensajería con las credenciales por host que se almacenan en otras variables de /UserVars/RmqIpAddress
- netcpa que se ejecuta en un host ESXi se basa en vsfwd para hacer lo siguiente:
 - Obtener el certificado y la clave privada SSL del plano de control del host de NSX Manager. Estas se almacenan en /etc/vmware/ssl/rui-for-netcpa.*
 - Obtener las huellas digitales SSL y las direcciones IP de las controladoras de NSX Manager. Estas se almacenan a continuación en /etc/vmware/netcpa/config-by-vsm.xml.
 - Crear y eliminar instancias de DLR en sus hosts según las instrucciones de NSX Manager
- Empaquetado e implementación
 - Al igual que netcpa, es parte del VIB de VXLAN.
 - Se ejecuta como un demonio de servicio en vsfwd de ESXi.
 - Se puede iniciar, detener o consultar a través de su script de inicio /etc/init.d/ vShield-Stateful-Firewall
- Las máquinas virtuales de control de DLR y las ESG utilizan el canal VMCI a vsfwd para recibir la configuración de NSX Manager

ESGs y máquinas virtuales de control de DLR

- La máquina virtual de control de DLR es un "procesador de rutas" para su instancia de DLR
 - Tiene interfaces de un "vNIC real" o un "marcador de posición" para cada LIF de DLR junto con la configuración de IP
 - Puede ejecutar uno o dos protocolos de enrutamiento dinámico disponibles (BGP o OSPF) y/o utilizar rutas estáticas
 - Necesita al menos un LIF de "enlace de subida" para poder ejecutar OSPF o BGP
 - Calcula la tabla de reenvío de las rutas dinámicas y estáticas y las subredes conectadas directamente (LIF) y las envía a la controladora principal de la instancia de DLR a través de su vínculo de MCI a netcpa
 - Admite HA en la configuración par de la máquina virtual en espera o activa
- La ESG es un enrutador independiente de una máquina virtual
 - Es completamente independiente del subsistema de enrutamiento del DLR de NSX (no hay integración del plano de control de NSX)
 - Se suele utilizar como una puerta de enlace ascendente para uno o varios DLR
 - Admite más de un protocolo de enrutamiento dinámico en ejecución simultánea

CLI del plano de control del enrutamiento de NSX

Además de los componentes del host, el enrutamiento de NSX emplea servicios del clúster de la controladora y las máquinas de control de DLR, cada una de las cuales es el origen de la información del plano de control de DLR e incluye su propia CLI usada para examinarlo.

Controladora principal de la instancia de DLR

Cada instancia del DLR se procesa en uno de los nodos de la controladora. Los siguientes comandos de CLI permiten ver la información que tiene este nodo de la controladora para la instancia de DLR de la que es la principal:

```
nsx-controller # show control-cluster logical-routers instance 1460487509
LR-Id      LR-Name      Hosts[]      Edge-Connection Service-Controller
1460487509 default+edge-1 192.168.210.57      192.168.110.201
              192.168.210.51
              192.168.210.52
              192.168.210.56
              192.168.110.51
              192.168.110.52

nsx-controller # show control-cluster logical-routers interface-summary 1460487509
Interface      Type  Id      IP[]
570d455500000002  vxlan  5003    192.168.10.2/29
570d45550000000b  vxlan  5001    172.16.20.1/24
570d45550000000c  vxlan  5002    172.16.30.1/24
570d45550000000a  vxlan  5000    172.16.10.1/24

nsx-controller # show control-cluster logical-routers routes 1460487509
LR-Id      Destination      Next-Hop
1460487509  0.0.0.0/0        192.168.10.1
```

- El subcomando "instancia" (instance) del subcomando "mostrar los enrutadores lógicos del clúster de la controladora" (show control-cluster logical-routers) muestra una lista de los hosts que están conectados a esta controladora para esta instancia de DLR. En un entorno que funcione correctamente, esta lista debe incluir todos los host de todos los clústeres en los que exista el DLR.
- El "resumen de la interfaz" (interface-summary) muestra los LIF que la controladora adquirió de NSX Manager. Esta información se envía a los hosts.
- Las "rutas" (routes) muestran la tabla de enrutamiento que la máquina virtual de control de DLR envió a esta controladora. Tenga en cuenta que, a diferencia de los hosts ESXi, esta tabla no incluye subredes conectadas directamente, ya que la configuración de LIF proporciona esta información.

Máquina virtual de control de DLR

La máquina de control de DLR tiene LIFs y tablas de enrutamiento y reenvío. La salida principal del ciclo de vida de la máquina virtual de control de DLR es la tabla de enrutamiento de DLR, que es producto de las interfaces y las rutas.

```
edge-1-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2

Total number of routes: 5

S      0.0.0.0/0          [1/1]      via 192.168.10.1
C      172.16.10.0/24     [0/0]      via 172.16.10.1
C      172.16.20.0/24     [0/0]      via 172.16.20.1
C      172.16.30.0/24     [0/0]      via 172.16.30.1
C      192.168.10.0/29    [0/0]      via 192.168.10.2

edge-1-0> show ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route
R>* 0.0.0.0/0 via 192.168.10.1, vNic_2
C>* 172.16.10.0/24 is directly connected, VDR
C>* 172.16.20.0/24 is directly connected, VDR
C>* 172.16.30.0/24 is directly connected, VDR
C>* 192.168.10.0/29 is directly connected, vNic_2
```

- El objetivo de las tablas de reenvío es mostrar qué interfaz de DLR se selecciona como salida de una subred de destino dada.
 - La interfaz de "VDR" se muestra para todas los LIF de tipo "interno" (Internal). La interfaz de VDR es una pseudointerfaz que no corresponde a ninguna vNIC.

Las interfaces de la máquina virtual de control de DLR se pueden mostrar de la siguiente forma:

```
edge-1-0> show interface
Interface VDR is up, line protocol is up
index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,NOARP>
HWaddr: be:3d:a1:52:90:f4
inet6 fe80::bc3d:a1ff:fe52:90f4/64
inet 172.16.10.1/24
inet 172.16.20.1/24
inet 172.16.30.1/24
proxy_arp: disabled
Auto-duplex (Full), Auto-speed (2460Mb/s)
input packets 0, bytes 0, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 0, bytes 0, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```



```
Interface vNic_0 is up, line protocol is up
index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:1c:fb
inet6 fe80::250:56ff:fe8e:1cfb/64
inet 169.254.1.1/30
inet 10.10.10.1/24
proxy_arp: disabled
Auto-duplex (Full), Auto-speed (2460Mb/s)
input packets 582249, bytes 37339072, dropped 49, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 4726382, bytes 461202852, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0

Interface vNic_2 is up, line protocol is up
index 9 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:ae:08
inet 192.168.10.2/29
inet6 fe80::250:56ff:fe8e:ae08/64
proxy_arp: disabled
Auto-duplex (Full), Auto-speed (2460Mb/s)
input packets 361446, bytes 30167226, dropped 0, multicast packets 361168
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 361413, bytes 30287912, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

Notas de interés:

- La interfaz de "VDR" no tiene ningún NIC de máquina virtual (vNIC) asociado. Es una "pseudointerfaz" única que está configurada con todas las direcciones IP para todas los LIF "internos" (Internal) de DLR.
- La interfaz vNic_0 de este ejemplo es la interfaz de HA.
 - La salida anterior se realizó desde un DLR implementado con HA habilitado y a la interfaz HA se le asigna una dirección IP. Esto aparece como dos direcciones IP, 169.254.1.1/30 (autoasignada para HA) y 10.10.10.1/24, asignada de forma manual a la interfaz de HA.
 - En una ESG, el operador puede asignar de forma manual una de estas vNIC como HA o mantener su valor predeterminado para que el sistema elija automáticamente desde interfaces "internas" (Internal) disponibles. Es necesario tener el tipo "interno" (Internal) o HA fallará.
- La interfaz vNIC_2 es de tipo Uplink; por lo tanto se representa como una vNIC real.
 - Tenga en cuenta que la dirección IP que se ve en esta interfaz es la misma que el LIF de DLR; sin embargo, la máquina virtual de control de DLR no responderá a las solicitudes de ARP para la dirección IP de LIF (en este caso, 192.168.10.2/29). Hay un filtro ARP aplicado en esta dirección MAC de vNIC que hace que ocurra.

- El punto anterior se puede aplicar hasta que se configure un protocolo de enrutamiento dinámico en el DLR, momento en el cual la dirección IP se eliminará junto con el filtro de ARP y se reemplazará con la dirección "IP del protocolo" (Protocol IP) especificada durante la configuración del protocolo de enrutamiento dinámico.
- El protocolo de enrutamiento dinámico ejecutado en la máquina virtual de control de DLR utiliza este vNIC para comunicarse con los demás enrutadores para anunciar y aprender rutas.
- Después de que Edge se desconecte y tras la conmutación por error de HA, la dirección IP de la interfaz de Edge desconectada se elimina de la base de información de enrutamiento del Edge activo (RIB) o de la base de información de reenvío (FIB). Sin embargo, la tabla FIB del Edge en espera o el comando `show ip forwarding` aún muestra la IP y no se elimina de la tabla FIB. Este es el comportamiento esperado.

Efectos y modos de errores del subsistema de enrutamiento de NSX

En este capítulo se incluyen los escenarios de errores típicos que pueden afectar a los componentes del subsistema de enrutamiento de NSX y se describen los efectos de estos errores.

NSX Manager

Tabla 3-2. Efectos y modos de errores de NSX Manager

Modo de error	Efectos de errores
Pérdida de conectividad de red a la máquina virtual NSX Manager	<ul style="list-style-type: none"> ■ Interrupción total de todas las funciones de NSX Manager, incluidas las operaciones CRUD para el enrutamiento o el puente de NSX ■ No se pierden datos de configuración ■ No se pierden el plano de control ni los datos
Pérdida de la conectividad de red entre NSX Manager y los hosts ESXi o error en el servidor RabbitMQ	<ul style="list-style-type: none"> ■ Si la máquina virtual de control de DLR o la ESG se ejecutan en los hosts afectados, se produce un error en las operaciones CRUD en ellos ■ Se produce un error al crear o eliminar instancias de DLR en hosts afectados ■ No se pierden datos de configuración ■ No se pierden el plano de control ni los datos ■ Las actualizaciones del enrutamiento dinámico siguen funcionando

Tabla 3-2. Efectos y modos de errores de NSX Manager (continuación)

Modo de error	Efectos de errores
Pérdida de conectividad de red entre NSX Manager y las controladoras	<ul style="list-style-type: none"> ■ Se produce un error en las operaciones de creación, actualización y eliminación en el puente y el enrutamiento distribuido de NSX ■ No se pierden datos de configuración ■ No se pierden el plano de control ni los datos
La máquina virtual de NSX Manager se destruye (error en el almacén de datos)	<ul style="list-style-type: none"> ■ Interrupción total de todas las funciones de NSX Manager, incluidas las operaciones CRUD para el enrutamiento o el puente de NSX ■ Riesgo de que un subconjunto de instancias de enrutamiento o puente se convierta en huérfano si NSX Manager se restaura a una configuración anterior. Se solicitará una limpieza manual y una reconciliación ■ No se pierden datos ni el plano de control a menos que se requiere una reconciliación

Clúster de la controladora

Tabla 3-3. Efectos y modos de errores de NSX Controller

Modo de error	Efectos de errores
El clúster de la controladora pierde conectividad de red con los hosts ESXi	<ul style="list-style-type: none"> ■ Pérdida total de las funciones del plano de control de DLR (creación, actualización y eliminación de rutas, incluidas las dinámicas) ■ Pérdida de las funciones del plano de administración de DLR (creación, actualización y eliminación de los LIF en los hosts) ■ El reenvío de VXLAN se ve afectado, lo que puede provocar también un error en el proceso completo de reenvío (Capa 2 + Capa 3) ■ El plano de datos sigue funcionando según el último estado conocido
Una o dos controladoras pierden conectividad con los hosts ESXi	<ul style="list-style-type: none"> ■ Si una controladora afectada puede seguir llegando a otras controladoras del clúster, las instancias del DLR que utiliza esta controladora experimentan los mismos efectos que los descritos anteriormente. Otras controladoras no se reemplazan automáticamente
Una controladora pierde la conectividad de red con otras controladoras (o la pierde por completo)	<ul style="list-style-type: none"> ■ Dos controladoras restantes reemplazan a las VXLAN y los DLR que utiliza la controladora aislada ■ La controladora afectada pasa a modo de solo lectura, coloca sus sesiones en los hosts y rechaza las nuevas

Tabla 3-3. Efectos y modos de errores de NSX Controller (continuación)

Modo de error	Efectos de errores
Las controladoras pierden la conectividad entre ellas	<ul style="list-style-type: none"> ■ Todas las controladoras pasarán al modo de solo lectura, cerrarán la conexión a los hosts y rechazarán las nuevas ■ Se produce un error en las operaciones de creación, actualización y eliminación en las rutas (incluidas las dinámicas) y los LIF de todos los DLR ■ La configuración del enrutamiento de NSX (LIFs) puede perder la sincronización entre NSX Manager y el clúster de la controladora, lo que permite solicitar que se intervenga de forma manual para volver a realizar la sincronización ■ Los hosts seguirán funcionando en el último estado conocido del plano de control
Se pierde una máquina virtual de la controladora	<ul style="list-style-type: none"> ■ El clúster de la controladora pierde redundancia ■ El plano de control o de administración sigue funcionando con normalidad
Se pierden dos máquinas virtuales de la controladora	<ul style="list-style-type: none"> ■ La controladora restante pasará al modo de solo lectura. El efecto es el mismo que el que se produce cuando las controladoras pierden conectividad entre ellas (como se indica anteriormente). Es posible que se requiera recuperar el clúster manualmente

Módulos del host

netcpa se basa en el certificado y la clave SSL del host, así como en huellas digitales SSL para establecer comunicaciones seguras con las controladoras. Se obtienen de NSX Manager a través del bus de mensajería que proporciona vsfwd.

Si se produce un error en el proceso de intercambio de certificados, netcpa no podrá conectarse correctamente a las controladoras.

Nota: en esta sección no se incluyen los errores de los módulos kernel, ya que su efecto es grave (PSOD) y no suele producirse.

Tabla 3-4. Efectos y modos de errores del módulo del host

Modo de error	Efectos de errores
vsfwd utiliza la autenticación por contraseña o nombre de usuario para acceder al servidor del bus de mensajería, el cual puede caducar	<ul style="list-style-type: none"> ■ Si un vsfwd de un host ESXi que se preparó recientemente no puede llegar a NSX Manager en dos horas, la contraseña o el inicio de sesión temporales que se proporcionaron durante la instalación caducan y el bus de mensajería de este host deja de funcionar
Los efectos de errores del cliente del bus de mensajería (vsfwd) dependen del tiempo.	

Tabla 3-4. Efectos y modos de errores del módulo del host (continuación)

Modo de error	Efectos de errores
Si se produce un error antes de que otras partes del plano de control de NSX puedan llegar al estado en ejecución estable	<ul style="list-style-type: none"> ■ El enrutamiento dinámico de los hosts deja de funcionar porque el host no puede comunicarse con las controladoras ■ El host no conoce las instancias de DLR de NSX Manager
Si se produce un error después de que el host llegue al estado estable	<ul style="list-style-type: none"> ■ Las ESG y las máquinas virtuales de control de DLR que se ejecutan en el host no podrán recibir las actualizaciones de configuración ■ El host no conoce los DLR nuevos y no puede eliminar los DLR existentes ■ La ruta de datos del host seguirá funcionando según la configuración que el host tenía cuando se produjo el error

Tabla 3-5. Efectos y modos de errores de netcpa

Modo de error	Efectos de errores
Los efectos de errores del agente del plano de control (netcpa) dependen del tiempo	
Si se produce un error antes de que los módulos kernel de la ruta de datos de NSX puedan llegar al estado en ejecución estable	<ul style="list-style-type: none"> ■ El enrutamiento distribuido del host deja de funcionar
Si se produce un error después de que el host llegue al estado estable	<ul style="list-style-type: none"> ■ Las máquinas virtuales de control de DLR que se ejecutan en el host no pondrán enviar sus actualizaciones de la tabla de reenvío a las controladoras ■ La ruta de datos del enrutamiento distribuido no recibirá las actualizaciones de rutas ni los LIF de las controladoras, pero seguirá funcionando según el estado que tuviera antes de producirse el error

Máquina virtual de control de DLR

Tabla 3-6. Efectos y modos de error de la máquina virtual de control de DLR

Modo de error	Efectos de errores
La máquina virtual de control de DLR se perdió o se apagó	<ul style="list-style-type: none"> ■ Se produce un error en las operaciones de creación, actualización y eliminación en las rutas y los LIF de este DLR ■ Las actualizaciones de la ruta dinámica no se enviarán a los hosts (incluida la retirada de prefijos que se reciben a través de las adyacencias que ya no funcionan)
La máquina virtual de control de DLR pierde conectividad con NSX Manager y las controladoras	<ul style="list-style-type: none"> ■ Los mismos efectos que se describieron anteriormente, excepto si la máquina virtual de control de DLR y sus adyacencias de enrutamiento siguen estando activas. El tráfico de y hacia los prefijos conocidos no se verá afectado

Tabla 3-6. Efectos y modos de error de la máquina virtual de control de DLR (continuación)

Modo de error	Efectos de errores
La máquina virtual de control de DLR pierde conexión con NSX Manager	<ul style="list-style-type: none"> ■ Se produce un error en las operaciones de creación, actualización y eliminación de NSX Manager en las rutas y los LIF de este DLR y no se vuelve a intentar realizar estas operaciones ■ Las actualizaciones del enrutamiento dinámico siguen propagándose
La máquina virtual de control de DLR pierde conexión con las controladoras	<ul style="list-style-type: none"> ■ Los cambios de enrutamiento (estático o dinámico) de este DLR no se propagan a los hosts

Registros NSX relevantes para el enrutamiento

Le recomendamos que configure todos los componentes de NSX para que envíen sus registros a un recopilador centralizado, donde se podrán examinar en un solo lugar.

Si es necesario, puede cambiar el nivel del registro de los componentes NSX. Para obtener más información, consulte el tema "Configurar el nivel de registros de los componentes de NSX" en *Eventos del sistema y de registro de NSX*.

Registros de NSX Manager

- `show log` en la CLI de NSX Manager.
- Paquete de registro de soporte técnico (Tech Support Log), recopilado a través de la interfaz de usuario de NSX Manager.

NSX Manager Virtual Appliance Management



El registro de NSX Manager contiene información relacionada con el plano de administración, que incluye crear, leer, actualizar y eliminar (CRUD) operaciones.

Registro de los controladores

Los controladores contienen varios módulos, muchos de ellos con sus propios archivos de registro. Para acceder a los registros de los controladores, utilice el comando `show log <log file> [filtered-by <string>]`. Los archivos de registros relevantes para el enrutamiento son los siguientes:

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: este registro administra la configuración y el servidor interno de la API.
- `cloudnet/cloudnet.nsx-controller.log`: este es el registro de los procesos principales del controlador.

- `cloudnet/cloudnet_cpp.log.nsx-controller.log`: este registro administra las agrupaciones y los arranques.
- `cloudnet/cloudnet_cpp.log.ERROR`: este archivo está presente si ocurre cualquier error.

Los registros de los controladores están detallados y en la mayoría de los casos solo son necesarios cuando el equipo de ingenieros de VMware está ocupado solucionando problemas en casos más complejos.

Además de la CLI de `show log`, los archivos de registro individuales se pueden ver en tiempo real mientras se actualizan a través del comando `watch log <logfile> [filtered-by <string>]`.

Los registros están incluidos en el paquete de soporte del controlador, que puede generar y descargar si selecciona un nodo del controlador en la interfaz de usuario de NSX y hace clic en el icono **Descargar registros de soporte técnico** (Download tech support logs).

Registros del host ESXi

Los componentes de NSX que se ejecutan en los host ESXi escriben varios archivos de registro:

- Registros de VMkernel: `/var/log/vmkernel.log`
- Registros del agente del plano de control: `/var/log/netcpa.log`
- Registros del cliente de la mensajería bus: `/var/log/vsfwd.log`

Los registros también se pueden recopilar como parte del paquete de soporte de la máquina virtual generado desde vCenter Server. Únicamente los usuarios o el grupo de usuario que tengan el privilegio *raíz* pueden acceder a los archivos de registro.

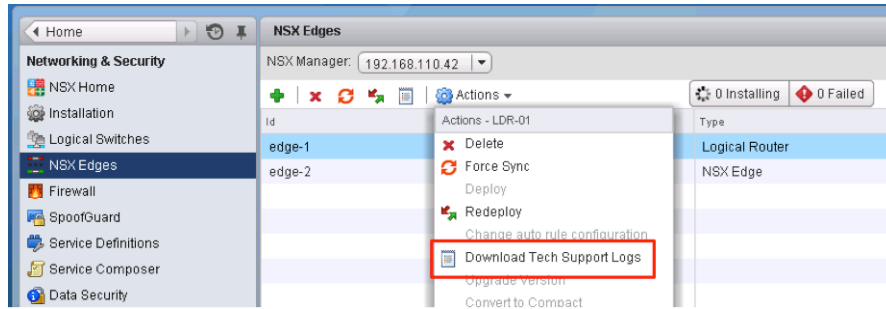
Registros de la máquina virtual de control de ESG/DLR

Existen dos maneras para acceder a los archivos de registro de las máquinas virtuales de control de ESG y DLR: mostrarlos a través de una CLI o bien descargar el paquete de soporte técnico mediante la CLI o la interfaz de usuario.

El comando de la CLI para mostrar los registros es `show log [follow | reverse]`.

Para descargar el paquete de soporte técnico:

- En la CLI, introduzca el modo `enable` y, a continuación, ejecute el comando `export tech-support <[scp | ftp]> <URI>`.
- Desde vSphere Web Client, seleccione la opción **Descargar informes del soporte técnico** (Download Tech Support Logs) en el menú de **Acciones** (Actions).



Otros archivos útiles y sus ubicaciones

Aparte de los registros, hay una serie de archivos que pueden ser útiles para entender y solucionar los problemas de enrutamiento de NSX.

- La configuración del agente del plano de control, `/etc/vmware/netcpa/config-by-vsm.xml` contiene información sobre los siguientes componentes:
 - Habilitar/deshabilitar SSL, huellas digitales de certificados, puertos TCP, direcciones IP y controladores.
 - Enlaces de subida dvUplinks de DVS habilitados con VXLAN (directivas de formación de equipo, nombres y UUID).
 - Instancias de DLR que el host conoce (nombre e ID del DLR).
- La configuración del agente del plano de control, `/etc/vmware/netcpa/netcpa.xml` contiene varias opciones de configuración para netcpa, incluido el nivel de registro (que por defecto está como **info**).
- Archivos de certificado del plano de control: `/etc/vmware/ssl/rui-for-netcpa.*`
 - Dos archivos: certificado del host y clave privada del host:
 - Se usan para autenticar las conexiones del host para los controladores.

Todos estos archivos los crea el agente del plano de control utilizando la información que recibe desde NSX Manager a través de la conexión del bus de mensajería que proporciona vsfwd.

Correcciones y escenarios de errores comunes

Los escenarios de errores más comunes se dividen en dos categorías.

Estos son los problemas del plano de control y de la configuración. Los problemas relacionados con el plano de administración son posibles pero no son muy comunes.

Corrección de errores y problemas de la configuración

Los problemas de configuración comunes y sus efectos se describen en la [Tabla 3-7. Efectos y problemas de configuración comunes](#).

Tabla 3-7. Efectos y problemas de configuración comunes

Problemas	Efectos
Las direcciones IP de reenvío y el protocolo se invierten para el enrutamiento dinámico	La adyacencia del protocolo dinámico no se establece
La zona de transporte no se alinea con el límite del DVS	El enrutamiento distribuido no funciona en un subconjunto de hosts ESXi (que no aparecen en la zona de transporte)
La configuración del protocolo de enrutamiento dinámico no coincide (temporizadores, MTU, ASN de BGP, contraseñas, interfaz de asignación de áreas de OSPF)	La adyacencia del protocolo dinámico no se establece
A la interfaz de HA de DLR se le asigna una dirección IP y se habilita la redistribución de las rutas conectadas	La máquina virtual de control de DLR puede atraer el tráfico de la subred de la interfaz de HA y bloquear el tráfico

Para solucionar estos problemas, revise la configuración y aplique las correcciones que estime oportunas.

Cuando sea necesario, utilice los comandos de CLI `debug ip ospf` o `debug ip bgp` y consulte los registros en la máquina virtual de control de DLR o en la consola de ESG (no a través de una sesión de SSH) para detectar problemas relacionados con la configuración de protocolos.

Corrección de errores y problemas del plano de control

Los problemas del plano de control que puede ver suelen producirse por las siguientes razones:

- El agente de plano de control del host (`netcpa`) no puede conectarse a NSX Manager mediante el canal de bus de mensajería que proporciona `vsfwd`.
- El clúster de la controladora tiene problemas para manipular la función principal de las instancias de DLR o VXLAN.

Los problemas del clúster de la controladora relacionados con la manipulación de funciones principales se pueden resolver si se reinicia una de las controladoras de NSX (`restart controller` en la CLI de la controladora).

Para obtener más información sobre cómo solucionar los problemas del panel de control, acceda a <http://kb.vmware.com/kb/2125767>

Obtener datos para solucionar problemas

Esta sección ofrece un resumen de los comandos de CLI que se usan normalmente para solucionar los problemas del enrutamiento de NSX.

NSX Manager

Iniciar NSX 6.2, los comandos que se ejecutaban antes en NSX Controller y otros componentes NSX para solucionar los problemas del enrutamiento de NSX se ejecutan directamente desde NSX Manager.

- Lista de instancias de DLR
- Lista de LIFs para cada instancia de DLR
- Lista de rutas para cada instancia de DLR

- Lista de direcciones MAC para cada instancia puente de DLR
- Interfaces
- Tabla de enrutamiento y de reenvío
- Estado de los protocolos de enrutamiento dinámicos (OSPF o BGP)
- Se envía la configuración a la máquina virtual de control de DLR o ESG a través de NSX Manager

Máquina virtual de control DLR y ESG

La máquina virtual de control DLR y ESG proporciona la función de capturar paquetes en sus interfaces. La captura de paquetes puede servir como ayuda para solucionar problemas de protocolos de enrutamiento.

- 1 Ejecute este comando `show interfaces` para realizar una lista de los nombres de las interfaces.
- 2 Ejecute `debug packet [display | capture] interface <interface name>`.
 - Si usa las capturas, los paquetes se guardan en un archivo `.pcap`.
- 3 Ejecute `debug show files` para realizar una lista de las capturas guardadas.
- 4 Ejecute `debug copy [scp | ftp] ...` para descargar capturas y poder realizar un análisis sin conexión.

```
d1r-01-0> debug packet capture interface vNic_2
tcpdump: listening on vNic_2, link-type EN10MB (Ethernet), capture size 65535 bytes
43 packets captured
48 packets received by filter
0 packets dropped by kernel
```

```
d1r-01-0> debug show files
total 4.0K
-rw----- 1 3.6K Mar 30 23:49 tcpdump_vNic_2.0
```

```
d1r-01-0> debug copy
  scp  use scp to copy
  ftp  use ftp to copy
```

```
d1r-01-0> debug copy scp
  URL  user@<remote-host>:<path-to>
```

El comando `debug packet` utiliza `tcpdump` en segundo plano y puede aceptar modificadores de los filtros con formatos de los modificadores de los filtros `tcpdump` en UNIX. La única consideración es que los espacios en blanco en las expresiones de los filtros se deben reemplazar por guiones bajos ("_").

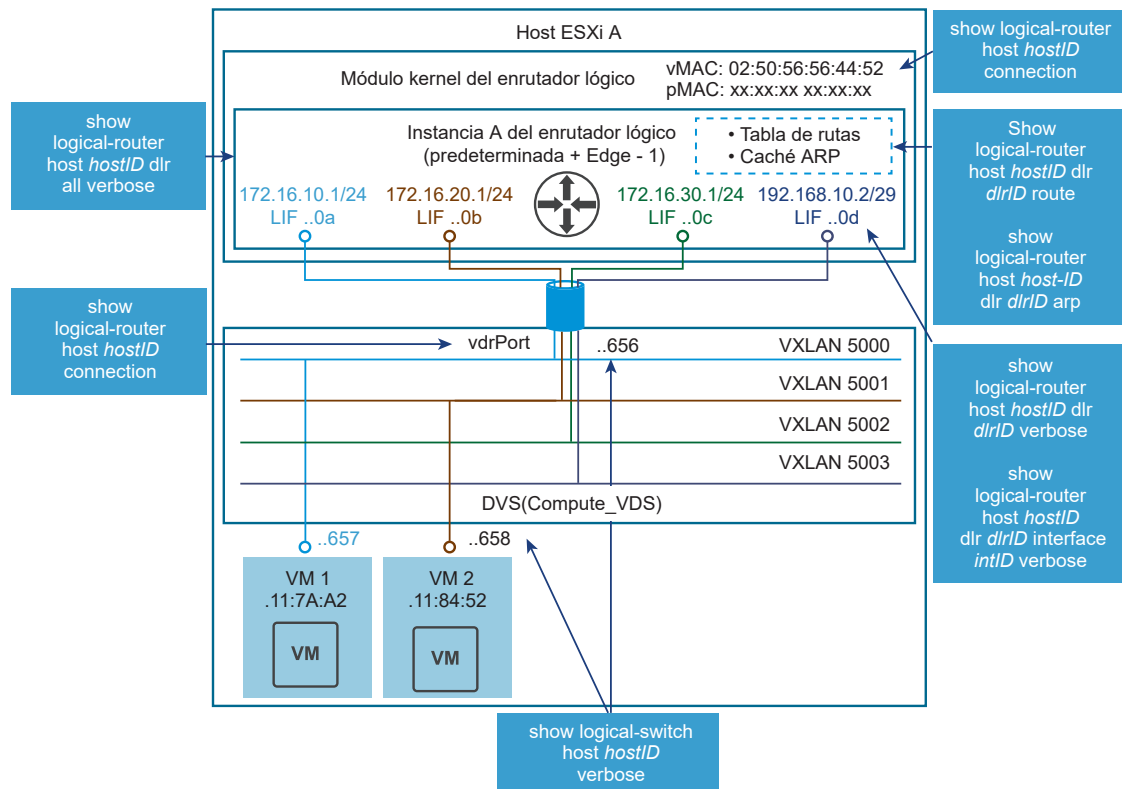
Por ejemplo, el siguiente comando muestra todo el tráfico a través de vNic_0 excepto SSH, para evitar acceder al tráfico perteneciente a una sesión interactiva.

```
plr-02-0> debug packet display interface vNic_0 port_not_22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vNic_0, link-type EN10MB (Ethernet), capture size 65535 bytes
04:10:48.197768 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 4191398894:4191398913,
ack 2824012766, win 913, length 19: BGP, length: 19
04:10:48.199230 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [.], ack 19, win 2623, length 0
04:10:48.299804 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [P.], seq 1:20, ack 19, win 2623,
length 19: BGP, length: 19
04:10:48.299849 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [.], ack 20, win 913, length 0
04:10:49.205347 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 19:38, ack 20, win 913,
length 19: BGP, length: 19
```

Hosts ESXi

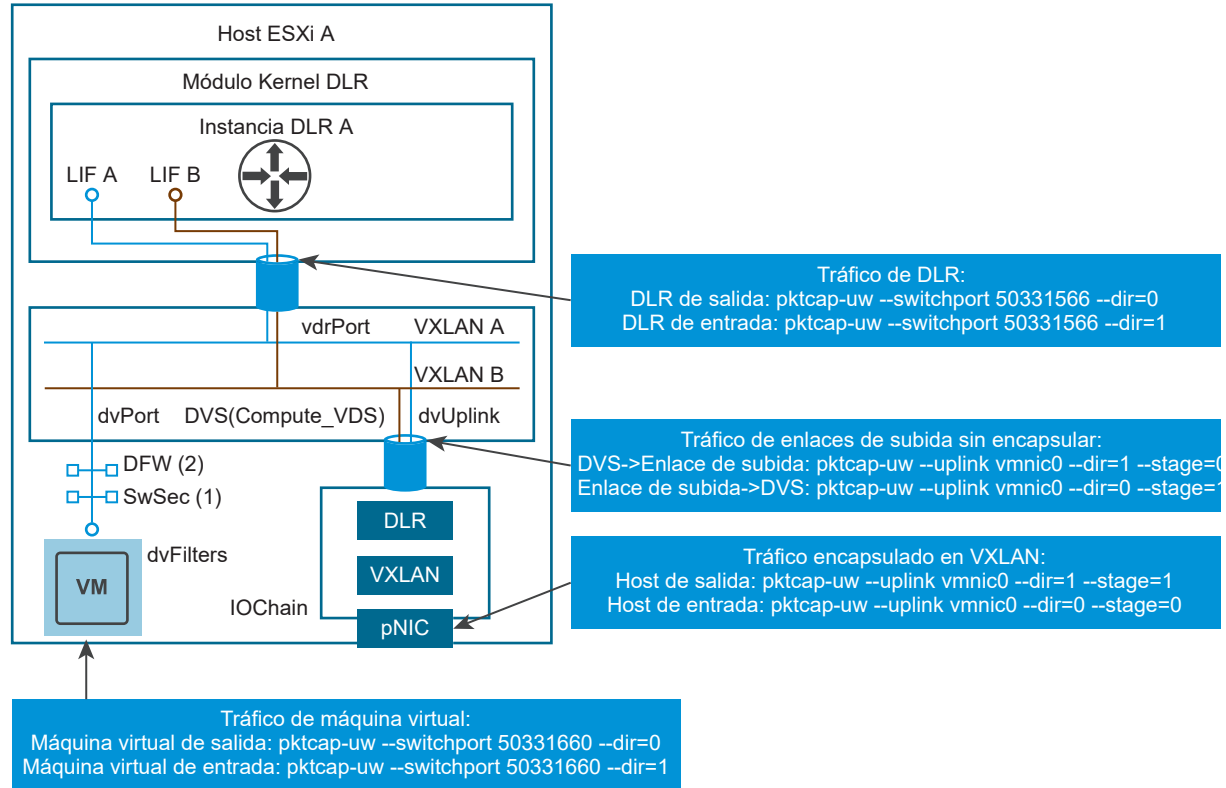
Los hosts están conectados al enrutamiento de NSX. [Figura 3-14. Componentes del host relacionados con la solución de problemas del enrutamiento de NSX](#) muestra de forma visual los componentes que participan en el subsistema de enrutamiento y los comandos de la CLI de NSX Manager suelen mostrar información sobre ellos:

Figura 3-14. Componentes del host relacionados con la solución de problemas del enrutamiento de NSX



La captura de paquetes en la ruta de datos puede servir de asistencia para identificar problemas en varias etapas del reenvío del paquete. [Figura 3-15. Puntos de captura y comandos de la CLI relacionados](#) muestra los puntos de captura más importantes y los comandos de la CLI que se deben usar.

Figura 3-15. Puntos de captura y comandos de la CLI relacionados



Solucionar problemas de NSX Edge

4

Esta sección proporciona información para comprender y solucionar los problemas de VMware NSX Edge.

Para solucionar los problemas con un dispositivo de NSX Edge, compruebe que cada paso especificado a continuación se puede aplicar a su entorno. Cada paso proporciona instrucciones o un enlace a un documento para eliminar posibles causas y realizar las acciones necesarias para corregirlas. Los pasos se ordenan en la secuencia más apropiada para aislar el problema e identificar la solución correcta. No se salte ningún paso.

Revise las notas de las versiones actuales para comprobar si ya se ha resuelto el problema.

Asegúrese que se cumplen los requisitos mínimos del sistema cuando se instale VMware NSX Edge. Consulte la *Guía de instalación de NSX*.

Problemas de instalación y actualización

- Compruebe que el problema que se ha encontrado no está relacionado con el problema del "Would Block". Para obtener más información, consulte <https://kb.vmware.com/kb/2107951>.
- Si se realiza correctamente la actualización o la reimplementación pero no existe conexión para la interfaz de Edge, compruebe la conectividad en el conmutador de Capa 2 back-end. Consulte <https://kb.vmware.com/kb/2135285>.
- Si se produce el siguiente error en la implementación o la actualización de Edge:

```
/sbin/ifconfig vNic_1 up failed : SIOCSIFFLAGS: Invalid argument
```

O

- Si se actualiza o se implementa correctamente, pero no hay conexión con las interfaces de Edge:

- Ejecute el comando `show interface` si los registros de Edge Support muestra entradas similares a:

```
vNic_0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether 00:50:56:32:05:03 brd ff:ff:ff:ff:ff:ff
    inet 21.12.227.244/23 scope global vNic_0
    inet6 fe80::250:56ff:fe32:503/64 scope link tentative dadfailed
    valid_lft forever preferred_lft forever
```

En ambos casos, el conmutador del host no está listo o tiene algún problema. Para solucionarlo, revisa el conmutador del host.

Problemas de configuración

- Recopile la información del diagnóstico de NSX Edge. Consulte <https://kb.vmware.com/kb/2079380>.
Filtre los registros de NSX Edge mediante la búsqueda la cadena `vse_die`. Los registros sobre esta cadena pueden proporcionar información sobre el error en la configuración.

Uso elevado de CPU

Si está sometiendo a su CPU a un uso elevado en NSX Edge, compruebe el rendimiento del dispositivo mediante el comando `esxtop` en el host ESXi. Revise los siguientes artículos de la base de conocimientos:

- <https://kb.vmware.com/kb/1008205>
- <https://kb.vmware.com/kb/1008014>
- <https://kb.vmware.com/kb/1010071>
- <https://kb.vmware.com/kb/2096171>

Consulte también <https://communities.vmware.com/docs/DOC-9279>.

Un valor alto en el proceso `ksoftirqd` indica un valor alto del paquete de entrada. Revise si el registro está habilitado en la ruta de datos así como para reglas del firewall. Ejecute el comando `show log follow` para determinar si se están almacenando un gran número de registros.

Mostrar estadísticas de colocación de paquetes

A partir de NSX for vSphere 6.2.3, puede utilizar el comando `show packet drops` para mostrar las estadísticas de colocación de paquetes en los siguientes elementos:

- Interfaz
- Controlador
- Capa 2
- Capa 3
- Firewall

Para ejecutar el comando, inicie sesión en la CLI de NSX Edge e introduzca el modo básico. Para obtener más información, consulte la *Referencia de la interfaz de línea de comandos de NSX*. Por ejemplo:

```
show packet drops
```

vShield Edge Packet Drop Stats:

Driver Errors

=====

	TX	TX	TX	RX	RX	RX
Interface	Dropped	Error	Ring	Full	Dropped	Error Out Of Buf
vNic_0	0	0	0	0	0	0
vNic_1	0	0	0	0	0	0
vNic_2	0	0	0	0	0	2
vNic_3	0	0	0	0	0	0
vNic_4	0	0	0	0	0	0
vNic_5	0	0	0	0	0	0

Interface Drops

=====

Interface	RX Dropped	TX Dropped
vNic_0	4	0
vNic_1	2710	0
vNic_2	0	0
vNic_3	2	0
vNic_4	2	0
vNic_5	2	0

L2 RX Errors

=====

Interface	length	crc	frame	fifo	misses
vNic_0	0	0	0	0	0
vNic_1	0	0	0	0	0
vNic_2	0	0	0	0	0
vNic_3	0	0	0	0	0
vNic_4	0	0	0	0	0
vNic_5	0	0	0	0	0

L2 TX Errors

=====

Interface	aborted	fifo	window	heartbeat
vNic_0	0	0	0	0
vNic_1	0	0	0	0
vNic_2	0	0	0	0
vNic_3	0	0	0	0
vNic_4	0	0	0	0
vNic_5	0	0	0	0

L3 Errors

=====

IP:

ReasmFails : 0
InHdrErrors : 0

```

InDiscards : 0
FragFails : 0
InAddrErrors : 0
OutDiscards : 0
OutNoRoutes : 0
ReasmTimeout : 0
ICMP:
InTimeExcds : 0
InErrors : 227
OutTimeExcds : 0
OutDestUnreachs : 152
OutParmProbs : 0
InSrcQuenchs : 0
InRedirects : 0
OutSrcQuenchs : 0
InDestUnreachs : 151
OutErrors : 0
InParmProbs : 0

Firewall Drop Counters
=====

Ipv4 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 119 30517 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 101 4040 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0

```

Comportamiento previsto cuando se administra NSX Edge

- En vSphere Web Client, cuando configura una VPN de Capa 2 en una instancia de NSX Edge y agrega, elimina o modifica los **Detalles de configuración del sitio** (Site Configuration Details), esta acción hará que todas las conexiones existentes se desconecten y se vuelvan a conectar. Este comportamiento es correcto.

- NSX Edge es una máquina virtual y consta de varios archivos que se almacenan en un dispositivo de almacenamiento. Los archivos clave son el archivo de configuración, los archivos de disco virtual, el archivo de configuración NVRAM, el archivo de intercambio y el archivo de registro. Según la ubicación manual o el perfil aplicado de almacenamiento de máquinas virtuales, los archivos de configuración de máquina virtual, el archivo del disco virtual y el archivo de intercambio se pueden colocar en la misma ubicación o en ubicaciones separadas de almacén de datos diferentes. Si los archivos de la máquina virtual se encuentran en diferentes ubicaciones, NSX Manager muestra y usa el almacén de datos que tiene el archivo VMX para la implementación de máquinas virtuales. Durante las operaciones de actualización o reimplementación, NSX Manager implementa las máquinas virtuales de NSX Edge en el almacén de datos configurado o el almacén de datos directo que almacena los archivos VMX. El *nombre del almacén de datos* y el *ID del almacén de datos* (que aloja el archivo VMX de la máquina virtual) se devuelven como parte del parámetro *Appliance* y se muestra en la interfaz de usuario o se proporciona como una respuesta a REST API. Debe consultar vCenter Server para obtener más información sobre el diseño exacto de cada archivo de la máquina virtual NSX Manager y uno o varios almacenes de datos donde los archivos se ubican. Para obtener más información, consulte la siguiente documentación.
 - *Administrar máquinas virtuales de vSphere.*
 - *Administrar recursos de vSphere.*
 - *Administrar vCenter Server y hosts.*

Este capítulo incluye los siguientes temas:

- [Problemas en la colocación de paquetes del firewall](#)
- [Problemas de conectividad en red de Edge](#)
- [Problemas de comunicación de NSX Manager y Edge](#)
- [Depuración de mensajería bus](#)
- [Diagnóstico y recuperación de Edge](#)

Problemas en la colocación de paquetes del firewall

Mostrar estadísticas de colocación de paquetes del firewall

A partir de NSX for vSphere 6.2.3, puede utilizar el comando `show packet drops` para mostrar las estadísticas de colocación de paquetes del firewall.

Para ejecutar el comando, inicie sesión en la CLI de NSX Edge e introduzca el modo básico. Para obtener más información, consulte la *Referencia de la interfaz de línea de comandos de NSX*. Por ejemplo:

```
show packet drops
```

```
vShield Edge Packet Drop Stats:
```

```

Firewall Drop Counters
=====

Ipv4 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 119 30517 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 101 4040 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0

```

Problemas del firewall del paquete de Edge

Para ejecutar un comando, inicie sesión en la CLI de NSX Edge e introduzca el modo básico. Para obtener más información, consulte la *Referencia de la interfaz de línea de comandos de NSX*.

- 1 Compruebe la tabla de reglas del firewall con el comando `show firewall`. La tabla `usr_rules` muestra las reglas configuradas.

```

nsxedge> show firewall
Chain PREROUTING (policy ACCEPT 3146M packets, 4098G bytes)
rid  pkts bytes target  prot opt in  out  source  destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target  prot opt in  out  source  destination
0    78903 16M ACCEPT  all -- lo   *    0.0.0.0/0 0.0.0.0/0
0      0 0 DROP    all -- *    0.0.0.0/0 0.0.0.0/0
state INVALID
0    140K 9558K block_in all -- *    0.0.0.0/0 0.0.0.0/0
0    23789 1184K ACCEPT  all -- *    0.0.0.0/0 0.0.0.0/0
state RELATED,ESTABLISHED
0    116K 8374K usr_rules all -- *    0.0.0.0/0 0.0.0.0/0
0      0 0 DROP    all -- *    0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy ACCEPT 3146M packets, 4098G bytes)
rid  pkts bytes target  prot opt in  out  source  destination

Chain OUTPUT (policy ACCEPT 173K packets, 22M bytes)
rid  pkts bytes target  prot opt in  out  source  destination

```

```
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target    prot opt in     out     source        destination
0     78903 16M ACCEPT    all  --  *      lo      0.0.0.0/0     0.0.0.0/0
0     679K 41M DROP      all  --  *      *       0.0.0.0/0     0.0.0.0/0
state INVALID
0     3146M 4098G block_out all  --  *      *       0.0.0.0/0     0.0.0.0/0
0      0 0 ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
PHYSDEV match --physdev-in tap0 --physdev-out vNic_+
0      0 0 ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out tap0
0      0 0 ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
PHYSDEV match --physdev-in na+ --physdev-out vNic_+
0      0 0 ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out na+
0     3145M 4098G ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
state RELATED,ESTABLISHED
0     221K 13M usr_rules all  --  *      *       0.0.0.0/0     0.0.0.0/0
0      0 0 DROP      all  --  *      *       0.0.0.0/0     0.0.0.0/0

Chain block_in (1 references)
rid  pkts bytes target    prot opt in     out     source        destination

Chain block_out (1 references)
rid  pkts bytes target    prot opt in     out     source        destination

Chain usr_rules (2 references)
rid  pkts bytes target    prot opt in     out     source        destination
131074 70104 5086K ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
match-set 0_131074-os-v4-1 src
131075 116K 8370K ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
match-set 1_131075-ov-v4-1 dst
131073 151K 7844K ACCEPT    all  --  *      *       0.0.0.0/0     0.0.0.0/0
```

Revise si hay algún valor aumentado de alguna regla DROP invalid en la sección del comando POST_ROUTING show firewall. Entre las razones más habituales se incluyen:

- Problemas de rutas asimétricas
- Aplicaciones basadas en TCP inactivas durante más de una hora. Si existen problemas de tiempo de espera inactivo y las aplicaciones están inactivas durante mucho tiempo, aumente la configuración del tiempo de espera inactivo mediante REST API. Consulte <https://kb.vmware.com/kb/2101275>

2 Recopile la salida del comando show ipset.

```
nsxedge> show ipset
Name: 0_131074-os-v4-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
```

```
Members:
vse (vShield Edge Device)

Name: 0_131074-os-v6-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 1_131075-ov-v4-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=6, DestPort=179, SrcPort=Any      (encoded: 0.6.0.179,0.6.0.0/16)
Proto=89, DestPort=Any, SrcPort=Any     (encoded: 0.89.0.0/16,0.89.0.0/16)

Name: 1_131075-ov-v6-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=89, DestPort=Any, SrcPort=Any     (encoded: 0.89.0.0/16,0.89.0.0/16)
Proto=6, DestPort=179, SrcPort=Any      (encoded: 0.6.0.179,0.6.0.0/16)
```

- 3 Habilite el registro en una regla del firewall en particular a través de la API de REST o la interfaz del usuario de Edge y supervise los registros con el comando `show log follow`.

Si los registros no están visibles, habilítelos en la regla `DROP Invalid` mediante la siguiente API de REST.

```
URL : https://NSX_Manager_IP/api/4.0/edges/{edgeId}/firewall/config/global

PUT Method
Input representation
<globalConfig>    <!-- Optional -->
<tcpPickOngoingConnections>false</tcpPickOngoingConnections>    <!-- Optional. Defaults to false -->
>
<tcpAllowOutOfWindowPackets>false</tcpAllowOutOfWindowPackets>    <!-- Optional. Defaults to false -->
<tcpSendResetForClosedVsePorts>true</tcpSendResetForClosedVsePorts>    <!-- Optional. Defaults to true -->
<dropInvalidTraffic>true</dropInvalidTraffic>    <!-- Optional. Defaults to true -->
```

```
<logInvalidTraffic>true</logInvalidTraffic>      <!-- Optional. Defaults to false -->
<tcpTimeoutOpen>30</tcpTimeoutOpen>             <!-- Optional. Defaults to 30 -->
<tcpTimeoutEstablished>3600</tcpTimeoutEstablished> <!-- Optional. Defaults to 3600 -->
<tcpTimeoutClose>30</tcpTimeoutClose>            <!-- Optional. Defaults to 30 -->
<udpTimeout>60</udpTimeout>                      <!-- Optional. Defaults to 60 -->
<icmpTimeout>10</icmpTimeout>                   <!-- Optional. Defaults to 10 -->
<icmp6Timeout>10</icmp6Timeout>                 <!-- Optional. Defaults to 10 -->
<ipGenericTimeout>120</ipGenericTimeout>         <!-- Optional. Defaults to 120 -->
</globalConfig>
Output representation
No payload
```

Utilice el comando `show log follow` para buscar registros similares a:

```
2016-04-18T20:53:31+00:00 edge-0 kernel: nf_ct_tcp: invalid TCP flag combination IN= OUT=
SRC=172.16.1.4 DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=43343 PROTO=TCP
SPT=5050 DPT=80 SEQ=0 ACK=1572141176 WINDOW=512 RES=0x00 URG PSH FIN URGP=0
2016-04-18T20:53:31+00:00 edge-0 kernel: INVALID IN= OUT=vNic_1 SRC=172.16.1.4
DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=43343 PROTO=TCP SPT=5050 DPT=80
WINDOW=512 RES=0x00 URG PSH FIN URGP=0
```

- 4 Compruebe las conexiones coincidentes en la tabla de estado del firewall de Edge con el comando `show flowtable rule_id`:

```
nsxedge> show flowtable
1: tcp 6 21554 ESTABLISHED src=192.168.110.10 dst=192.168.5.3 sport=25981
d port=22 pkts=52 bytes=5432 src=192.168.5.3 dst=192.168.110.10 sport=22 dport=259
81 pkts=44 bytes=7201 [ASSURED] mark=0 rid=131073 use=1
2: tcp 6 21595 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=53194
dport=10 001 pkts=33334 bytes=11284650 src=127.0.0.1 dst=127.0.0.1 sport=10001 dport=5319
4 pkts=33324 bytes=1394146 [ASSURED] mark=0 rid=0 use=1
```

Compare el número de conexiones activas y el número máximo permitido con el comando `show flowstats`:

```
nsxedge> show flowstats
Total Flow Capacity: 65536
Current Statistics :
cpu=0 searched=3280373 found=3034890571 new=52678 invalid=659946 ignore=77605
delete=52667 delete_list=49778 insert=49789 insert_failed=0 drop=0 early_drop=0
error=0 search_restart=0
```

- 5 Compruebe los registros de Edge con el comando `show log follow` y busque cualquier colocación ALG. Busque cadenas similares a `tftp_alg`, `msrpc_alg` u `oracle_tns`. Para obtener información adicional, consulte:

- <https://kb.vmware.com/kb/2126674>
- <https://kb.vmware.com/kb/2137751>

Problemas de conectividad en red de Edge

- 1 Inicie el tráfico controlado para un cliente utilizando el comando `ping <destination_IP_address>`.
- 2 Capture el tráfico de forma simultánea en ambas interfaces, registre la salida en un archivo y expórtelo a través de SCP.

Por ejemplo:

Capte el tráfico en la interfaz de ingreso con este comando:

```
debug packet display interface vNic_0 -n_src_host_1.1.1.1
```

Capte el tráfico en la interfaz de salida con este comando:

```
debug packet display interface vNic_1 -n_src_host_1.1.1.1
```

Para captura de paquetes simultáneas, utilice la herramienta de captura de paquetes `pktcap-uw` en ESXi. Consulte <https://kb.vmware.com/kb/2051814>.

Si la colocación de paquetes es constante, revise los errores de la configuración relacionados con:

- la dirección y las rutas IP
 - las reglas de firewall o de NAT
 - las rutas asimétricas
 - las comprobaciones de los filtros RP
- a Compruebe las interfaces de la IP y de las subredes con el siguiente comando `show interface`.
 - b Si no se encuentran algunas rutas en el plano de datos, ejecute los siguientes comandos:
 - `show ip route`
 - `show ip route static`
 - `show ip route bgp`
 - `show ip route ospf`
 - c Ejecute el comando `show ip forwarding` para revisar la tabla de enrutamiento para las rutas necesarias.
 - d Si tiene varias rutas, ejecute el comando `show rpfilter`.

```
nsxedge> show rpfilter
net.ipv4.conf.VDR.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.br-sub.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.vNic_0.rp_filter = 1
net.ipv4.conf.vNic_1.rp_filter = 1
```

```
net.ipv4.conf.vNic_2.rp_filter = 1
net.ipv4.conf.vNic_3.rp_filter = 1
net.ipv4.conf.vNic_4.rp_filter = 1
net.ipv4.conf.vNic_5.rp_filter = 1
net.ipv4.conf.vNic_6.rp_filter = 1
net.ipv4.conf.vNic_7.rp_filter = 1
net.ipv4.conf.vNic_8.rp_filter = 1
net.ipv4.conf.vNic_9.rp_filter = 1

nsxedge> show rpfstats
RPF drop packet count: 484
```

Para revisar las estadísticas de RPF, ejecute el comando `show rpfstats`.

```
nsxedge> show rpfstats
RPF drop packet count: 484
```

Si la colocación de paquetes aparece de forma aleatoria, compruebe las limitaciones del recurso:

a Para la CPU o el uso de la memoria, ejecute los siguientes comandos:

- `show system cpu`
- `show system memory`
- `show system storage`
- `show process monitor`
- `top`

Para ESXi, ejecute el comando `esxtop n`.

```
PCPU USED(%): 2.5 5.0 3.7 77 AVG: 22
PCPU UTIL(%): 0.5 2.7 3.3 92 AVG: 24
```

ID	GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT
98255269	98255269	esxtop.11224149	1	67.04	69.86	0.00	6.26
2	2	system	139	3.03	4.61	0.00	12053.58
86329	86329	app-01a	6	0.69	0.57	0.00	466.09
78730	78730	db-01a	6	0.48	0.67	0.00	441.44
90486	90486	app-02a	6	0.38	0.32	0.00	463.42

%VMWAIT	%RDY	%IDLE	%OVRLP	%CSTP	%MLMTD	%SWPWT
11.01	-	0.39	0.00	0.09	0.00	0.00
600.00	53.81	0.10	93.13	0.00	0.00	0.00
13900.00	-	28.68	0.00	2.69	0.00	0.00
600.00	53.81	0.10	93.13	0.00	0.00	0.00
600.00	0.00	0.19	151.92	0.00	0.00	0.00

Problemas de comunicación de NSX Manager y Edge

NSX Manager se comunica con NSX Edge a través de VIX o mensajería bus. NSX Manager lo elige cuando el Edge se implementa y nunca cambia.

Nota VIX no es compatible con NSX 6.3.0 y versiones posteriores.

VIX

- VIX se usa para NSX Edge si el host ESXi no está preparado.
- NSX Manager obtiene credenciales de los hosts desde vCenter Server para conectarse primero al host ESXi.
- NSX Manager usa las credenciales de Edge para iniciar sesión en el dispositivo Edge.
- El proceso `vmtoolsd` de Edge gestiona la comunicación VIX.

Los errores de VIX se producen por los siguientes motivos:

- NSX Manager no se puede comunicar con vCenter Server.
- NSX Manager no se puede comunicar con el host ESXi.
- Existen problemas internos en NSX Manager.
- Existen problemas internos en Edge.

Depuración de VIX

Revise los errores de VIX `VIX_E_<error>` en los registros de NSX Manager para delimitar la causa. Busque errores similares a los siguientes:

```
Vix Command 1126400 failed, reason com.vmware.vshield.edge.exception.VixException: vShield
Edge:10013:Error code 'VIX_E_FILE_NOT_FOUND' was returned by VIX API.:null

Health check failed for edge edge-13 VM vm-5025 reason:
com.vmware.vshield.edge.exception.VixException: vShield Edge:10013:Error code
'VIX_E_VM_NOT_RUNNING' was returned by VIX API.:null
```

En general, si se reproduce el fallo en varios dispositivos Edge al mismo tiempo, el problema no está en Edge.

Depuración de mensajería bus

La mensajería bus se utiliza para la comunicación de NSX Edge cuando el host ESXi está preparado.

Cuando se encuentra algún problema, los registros de NSX Manager deben tener entradas similares a:

```
GMT ERROR taskScheduler-6 PublishTask:963 - Failed to configure VSE-vm index 0, vm-id vm-117,
edge edge-5. Error: RPC request timed out
```


Este problema ocurre si:

- Edge está en mal estado
- se perdió la conexión de la mensajería bus

Para diagnosticar el problema en Edge:

- Para comprobar la conexión mq, ejecute este comando:

```
nsxedge> show messagebus messages
-----
Message bus is enabled
cmd conn state : listening
init_req      : 1
init_resp     : 1
init_req_err   : 0
...
```

- Para comprobar la conexión vmci, ejecute este comando:

```
nsxedge> show messagebus forwarder
-----
Forwarder Command Channel
vmci_conn      : up
app_client_conn : up
vmci_rx        : 3649
vmci_tx        : 3648
vmci_rx_err    : 0
vmci_tx_err    : 0
vmci_closed_by_peer: 8
vmci_tx_no_socket : 0
app_rx         : 3648
app_tx         : 3649
app_rx_err     : 0
app_tx_err     : 0
app_conn_req   : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
Forwarder Event Channel
vmci_conn      : up
app_client_conn : up
vmci_rx        : 1143
vmci_tx        : 13924
vmci_rx_err    : 0
vmci_tx_err    : 0
vmci_closed_by_peer: 0
vmci_tx_no_socket : 0
app_rx         : 13924
app_tx         : 1143
app_rx_err     : 0
app_tx_err     : 0
app_conn_req   : 1
app_closed_by_peer : 0
```

```
app_tx_no_socket    : 0
-----
cli_rx              : 1
cli_tx              : 1
cli_tx_err          : 0
counters_reset      : 0
```

En el ejemplo, la salida `vmci_closed_by_peer: 8` indica el número de veces que el agente host cerró la conexión. Si el número está aumentando y la `vmci conn` está baja, el agente host no puede conectarse al agente RMQ. En `show log follow`, busque errores repetidos en los registros de Edge: `VmciProxy: [daemon.debug] VMCi Socket is closed by peer`

Para diagnosticar el problema el host ESXi:

- Para comprobar si el host ESXi se conecta al agente RMQ, ejecute el siguiente comando:

```
esxcli network ip connection list | grep 5671

tcp    0    0  10.32.43.4:43329  10.32.43.230:5671  ESTABLISHED    35854  newreno
vsfwd
tcp    0    0  10.32.43.4:52667  10.32.43.230:5671  ESTABLISHED    35854  newreno
vsfwd
tcp    0    0  10.32.43.4:20808  10.32.43.230:5671  ESTABLISHED    35847  newreno
vsfwd
tcp    0    0  10.32.43.4:12486  10.32.43.230:5671  ESTABLISHED    35847  newreno vsfwd
```

Diagnóstico y recuperación de Edge

Diagnóstico de Edge

- Compruebe si se está ejecutando `vmtoolsd` con el siguiente comando:

```
nsxedge> show process list
Perimeter-Gateway-01-0> show process list
%CPU %MEM    VSZ   RSZ STAT  STARTED      TIME COMMAND
 0.0  0.1   4244   720 Ss     May 16 00:00:15 init [3]
...
 0.0  0.1   4240   640 S      May 16 00:00:00 logger -p daemon debug -t vserrdd
 0.2  0.9  57192  4668 S      May 16 00:23:07 /usr/local/bin/vmtoolsd --plugin-pa
 0.0  0.4   4304  2260 SLs    May 16 00:01:54 /usr/sbin/watchdog
...
```

- Compruebe si Edge está en buen estado ejecutando este comando:

```
nsxedge> show eventmgr
-----
messagebus      : enabled
debug           : 0
```

```
profiling      : 0
cfg_rx         : 1
cfg_rx_msgbus  : 0
...
```

Use el comando `show eventmgr` para comprobar que el comando de consulta se recibió y se está procesando.

```
nsxedge> show eventmgr
-----
messagebus    : enabled
debug         : 0
profiling     : 0
cfg_rx        : 1
cfg_rx_msgbus : 0
cfg_rx_err    : 0
cfg_exec_err  : 0
cfg_resp      : 0
cfg_resp_err  : 0
cfg_resp_ln_err: 0
fastquery_rx  : 0 fastquery_err : 0
clearcmd_rx   : 0
clearcmd_err  : 0
ha_rx         : 0
ha_rx_err     : 0
ha_exec_err   : 0
status_rx     : 16
status_rx_err : 0
status_svr    : 10
status_evt    : 0
status_evt_push: 0
status_ha     : 0
status_ver    : 1
status_sys    : 5
status_cmd    : 0
status_svr_err: 0
status_evt_err: 0
status_sys_err: 0
status_ha_err : 0
status_ver_err: 0
status_cmd_err: 0
evt_report    : 1
evt_report_err: 0
hc_report     : 10962
hc_report_err : 0
cli_rx        : 2
cli_resp      : 1
cli_resp_err  : 0
counter_reset : 0
----- Health Status -----
system status : good
ha state      : active
cfg version   : 7
```

```

generation      : 0
server status   : 1
syslog-ng       : 1
haproxy         : 0
ipsec           : 0
sslvpn         : 0
l2vpn          : 0
dns             : 0
dhcp           : 0
heartbeat       : 0
monitor        : 0
gslb           : 0
----- System Events -----

```

Recuperación de Edge

Si el comando `vmtoolsd` no se ejecuta o NSX Edge está en mal estado, reinicie Edge.

Para recuperarse de un bloqueo, debería bastar con reiniciarlo. No debería ser necesario volver a implementarlo.

Nota Anote toda la información de registro de la implementación anterior de Edge cuando realice una nueva implementación.

Para depurar un bloqueo del kernel, debe obtener:

- El archivo `vmss` (suspensión máquina virtual) o `vmsn` (instantánea de máquina virtual) para la máquina virtual de Edge mientras siga estando bloqueada. Si hay un archivo `vmem`, también será necesario. Esto se puede utilizar para extraer un archivo de volcado de núcleo de kernel que el soporte de VMware pueda analizar.
- El registro de soporte técnico de Edge, generado justo después de que el Edge bloqueado se reiniciara (pero sin que se volviera a implementar). También puede comprobar los registros de Edge. Consulte <https://kb.vmware.com/kb/2079380>.
- Una instantánea de la consola de Edge también es útil, aunque esto no suele incluir el informe de errores completo.

Solución de problemas del firewall

5

En esta sección se incluye información sobre cómo solucionar problemas relacionados con el firewall.

Este capítulo incluye los siguientes temas:

- [Acerca de Distributed Firewall](#)
- [Firewall de identidad](#)

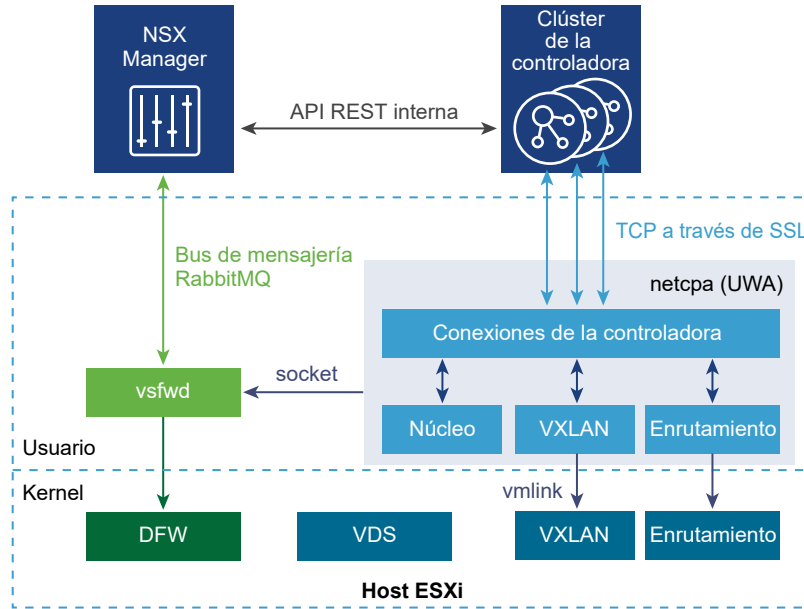
Acerca de Distributed Firewall

Se utiliza un bus de mensajería de RabbitMQ en la comunicación entre vsfwd (cliente RMQ) y el proceso del servidor RMA alojado en NSX Manager. NSX Manager utiliza el bus de mensajería para enviar información de diversa índole a los hosts ESXi entre la que incluye reglas de directivas que deben programarse en el firewall distribuido del kernel.

El Distributed Firewall de NSX es un firewall integrado en el kernel del hipervisor que proporciona visibilidad y control para las redes y las cargas de trabajo virtualizadas. Puede crear directivas para controlar el acceso basadas en los objetos de VMware vCenter como bases de datos y clústeres, nombres y etiquetas de máquinas virtuales, construcciones de red tales como direcciones IP, VLAN, y VXLAN, así como una identidad de grupo de usuarios desde Active Directory. Se han asegurado directivas constantes para controlar el acceso cuando una máquina virtual llega a vMotioned a través de hosts físicos sin tener que reescribir las reglas del firewall. Desde que el Distributed Firewall está integrado en el hipervisor, proporciona un rendimiento actualizado para habilitar una mayor consolidación de la carga de trabajo en los servidores físicos. La naturaleza distribuida del firewall proporciona una arquitectura de escalabilidad horizontal que extiende automáticamente la capacidad del firewall cuando se agregan hosts adicionales a un centro de datos.

La aplicación web de NSX Manager y los componentes de NSX de los hosts ESXi se comunican unos con otros a través del agente RabbitMQ, proceso que se ejecuta en la misma máquina virtual que la aplicación web de NSX Manager. El protocolo de comunicación que se utiliza es AMQP (Advanced Message Queueing Protocol) y se aseguran los canales a través del SSL. En un host ESXi, el proceso de VSFWD (vShield Firewall Daemon) establece y mantiene la conexión SSL con el agente y envía y recibe mensajes en nombre de otros componentes, que se comunican con él a través de la IPC.

Figura 5-1. Usuario del host ESXi y diagrama del espacio del kernel



Comandos de la CLI para DFW

Puede obtener más información sobre los firewalls distribuidos en la CLI central de NSX Manager.

Uso de los comandos Show dfw de la CLI central

Para profundizar más y obtener la información que desea, siga estos pasos:

- 1 Inicie sesión en la CLI central de NSX Manager con credenciales *administrativas*.
- 2 Ejecute los siguientes comandos:
 - a Ejecute el comando `show cluster all` para mostrar todos los clústeres.

```
nsxmgr>show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	Compute Cluster A	domain-c33	Datacenter Site A	Enabled
2	Management & Edge Cluster	domain-c41	Datacenter Site A	Enabled

- b Ejecute el comando `show cluster <clusterID>` para mostrar hosts en un clúster específico.

```
nsxmgr> show cluster domain-c33
```

Datacenter: Datacenter Site A

Cluster: Compute Cluster A

No.	Host Name	Host Id	Installation Status
1	esx-02a.corp.local	host-32	Enabled
2	esx-01a.corp.local	host-28	Enabled

- c Ejecute `show host <hostID>` para mostrar todas las máquinas virtuales de un host.

```
nsxmgr> show host host-28
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
No.  VM Name    VM Id    Power Status
1    web-02a     vm-219   on
2    web-01a     vm-216   on
3    win8-01a    vm-206   off
4    app-02a     vm-264   on
```

- d Ejecute el comando `show vm <vmID>` para mostrar información de una máquina virtual, incluidos nombres de filtros e ID de vNIC:

```
nsxmgr> show vm vm-264
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
Host-ID: host-28
VM: app-02a
Virtual Nics List:
1.
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Filters        nic-79396-eth0-vmware-sfw.2
```

- e Anote el ID de vNIC y ejecute más comandos como `show dfw vnic <vnicID>` y `show dfw host <hostID> filter <filter ID> rules`:

```
nsxmgr> show dfw vnic 502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Mac Address    00:50:56:ae:6c:6b
Port Group Id  dvportgroup-385
Filters        nic-79396-eth0-vmware-sfw.2

nsxmgr> show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules
ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmptype 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmptype 8 from addrset ip-securitygroup-10 to addrset
```

```
ip-securitygroup-11 accept;
    rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
    rule 1009 at 8 inout protocol icmp icmp type 8 from addrset ip-securitygroup-11 to addrset
ip-securitygroup-12 accept;
    rule 1003 at 9 inout protocol ipv6-icmp icmp type 136 from any to any accept;
    rule 1003 at 10 inout protocol ipv6-icmp icmp type 135 from any to any accept;
    rule 1002 at 11 inout protocol udp from any to any port 67 accept;
    rule 1002 at 12 inout protocol udp from any to any port 68 accept;
    rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
    # Filter rules
    rule 1004 at 1 inout ethertype any from any to any accept;
}
```

Uso del comando `export host-tech-support` de la CLI central

El comando `export host-tech-support` permite exportar un paquete de soporte de host ESXi a un servidor específico. Además, este comando recopila resultados y archivos relacionados con NSX en hosts específicos como, por ejemplo:

- Archivos de registro vsfwd y de VMKernel
- Lista de filtros
- Lista de reglas de DFW
- Lista de contenedores
- Detalles de SpoofGuard
- Información relacionada con el host
- Información relacionada con el descubrimiento de direcciones IP
- Resultados de comandos de RMQ
- Grupo de seguridad, perfil de servicios y detalles de la instancia
- Resultados relacionados con la CLI de ESX

Este comando también elimina los archivos temporales en NSX Manager.

Para recopilar resultados relacionados con NSX:

- 1 Inicie sesión en la CLI central de NSX Manager con credenciales *administrativas*.
- 2 Ejecute los siguientes comandos:
 - a `show cluster all`: para encontrar el ID de host necesario.
 - b `export host-tech-support host-id scp uid@ip:/path`: para generar el paquete de soporte técnico de NSX y copiarlo en un servidor específico.

Para obtener más información, consulte:

- [Referencia rápida de línea de comandos de NSX.](#)
- *Referencia de la interfaz de línea de comandos de NSX.*

Resolución de problemas de distributed firewall

Este tema proporciona información para entender y solucionar los problemas del Distributed Firewall de VMware NSX 6.x (DFW).

Problema

- Errores al publicar reglas en el distributed firewall.
- Errores al actualizar reglas en el distributed firewall.

Causa

Compruebe que cada paso para solucionar los problemas son adecuados para su entorno. Cada paso proporciona instrucciones o un vínculo a un documento para eliminar posibles causas y realizar las acciones necesarias para corregirlas. Los pasos se ordenan en la secuencia más apropiada para aislar el problema e identificar la solución correcta. Tras cada paso, vuelva a intentar actualizar y publicar las reglas del Distributed Firewall.

Solución

- 1 Compruebe que los VIB de NSX se instalaron correctamente en cada host ESXi del clúster. Para ello, ejecute estos comandos en cada host ESXi que se encuentra en el clúster.

```
# esxcli software vib list | grep vsip
esx-vsip                6.0.0-0.0.4744062  VMware  VMwareCertified  2017-01-04

# esxcli software vib list | grep vxlan
esx-vxlan                6.0.0-0.0.4744062  VMware  VMwareCertified  2017-01-04
```

Las versiones anteriores a NSX 6.2 tienen un VIB adicional:

```
# esxcli software vib list | grep dvfilter
esx-dvfilter-switch-security  5.5.0-0.0.2318233  VMware  VMwareCertified  2015-01-24
```

A partir de la versión NSX 6.3.3 con ESXi 6.0 o posterior, los VIB esx-vxlan y esx-vsip se reemplazan por esx-nsxv.

```
# esxcli software vib list | grep nsxv
esx-nsxv                6.0.0-0.0.6216823  VMware  VMwareCertified  2017-08-10
```

- 2 Compruebe en cada host ESXi que el servicio de vShield Stateful Firewall está ejecutándose.

Por ejemplo:

```
# /etc/init.d/vShield-Stateful-Firewall status

vShield-Stateful-Firewall is running
```

- 3 Compruebe que el bus de mensajería se comunica correctamente con NSX Manager.

El proceso comienza automáticamente a través del comando watchdog y reinicia el proceso si termina por alguna razón desconocida. Ejecute este comando en cada host ESXi del clúster.

Por ejemplo:

```
# ps | grep vsfwd

107557 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
```

Debe haber al menos 12 procesos vsfwd activos en los resultados del comando. Si hay menos (probablemente solo 2), significa que vsfwd no se está ejecutando correctamente.

- 4 Compruebe que el puerto 5671 está abierto para la comunicación en la configuración del firewall.

Este comando muestra la conectividad de VSFWD al agente RabbitMQ. Ejecute este comando en los hosts ESXi para visualizar una lista de conexiones desde el proceso vsfwd en el host ESXi hasta NSX Manager. Asegúrese de que el puerto 5671 está abierto a la comunicación en cualquiera de los firewalls externos del entorno. Por otra parte, el puerto 5671 debe tener al menos dos conexiones. Puede haber tantas conexiones en el puerto 5671 como máquinas virtuales de NSX Edge implementadas en el host ESXi que también se conecten al agente RMQ.

Por ejemplo:

```
# esxccli network ip connection list |grep 5671

tcp          0      0 192.168.110.51:30133      192.168.110.15:5671  ESTABLISHED
10949155 newreno vsfwd
tcp          0      0 192.168.110.51:39156      192.168.110.15:5671  ESTABLISHED
10949155 newreno vsfwd
```

- 5 Compruebe que VSFWD esté configurado.

Este comando debe mostrar la dirección IP de NSX Manager.

```
# esxcfg-advcfg -g /UserVars/RmqIpAddress
```

- 6 Si está utilizando un perfil de host para este host ESXi, compruebe que la configuración de RabbitMQ no se ha realizado en el perfil del host.

Consulte:

- <https://kb.vmware.com/kb/2092871>
- <https://kb.vmware.com/kb/2125901>

- 7 Compruebe que las credenciales de RabbitMQ del host ESXi no están sincronizadas con NSX Manager. Descargue los Registros de soporte tecnológico de NSX Manager (NSX Manager Tech Support Logs) Tras cumplir con todos los Registros de soporte tecnológico de NSX Manager (NSX Manager Tech Support Logs), busque todos los registros para entradas similares a:

Sustituya el host-420 por el ID de host en cuestión.

```
PLAIN login refused: user 'uw-host-420' - invalid credentials.
```

- 8 Si dichas entradas se encuentran en los registros del host ESXi en cuestión, vuelva a sincronizar el bus de mensajería.

Para volver a sincronizarlo, use la API de REST. Para comprender mejor este problema, recopile los registro inmediatamente después de volver a sincronizar el bus de mensajería.

```
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
Request:

POST https://NSX_Manager_IP/api/2.0/nwfabric/configure?action=synchronize

Request Body:

<nwFabricFeatureConfig>
<featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
<resourceConfig>
<resourceId>{HOST/CLUSTER MOID}</resourceId>
</resourceConfig>
</nwFabricFeatureConfig>
```

- 9 Ejecute el comando `export host-tech-support <host-id> scp <uid@ip:/path>` para obtener los registros del firewall específico del host.

Por ejemplo:

```
nsxmgr# export host-tech-support host-28 scp Administrator@192.168.110.10
Generating logs for Host: host-28...
```

- 10** Ejecute el comando `show dfw host host-id summarize-dvfilter` para comprobar que las reglas del firewall se implementan en un host y se aplican a las máquinas virtuales.

En la salida, módulo: `vsip` (module: `vsip`) muestra que el módulo DFW está cargado y en ejecución. El nombre (name) muestra el firewall que está en ejecución en cada vNic.

Puede obtener los ID del host si ejecuta el comando `show dfw cluster all` para mostrar los ID del dominio del clúster, seguido de `show dfw cluster domain-id` para tener acceso a los ID del host.

Por ejemplo:

```
# show dfw host host-28 summarize-dvfilter

Fastpaths:
agent: dvfilter-faulter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter
agent: ESXi-Firewall, refCount: 5, rev: 0x1010000, apiRev: 0x1010000, module: esxfw
agent: dvfilter-generic-vmware, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-generic-fastpath
agent: dvfilter-generic-vmware-swsec, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-switch-security
agent: bridgelearningfilter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: vdrb
agent: dvfg-igmp, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfg-igmp
agent: vmware-sfw, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module: vsip

Slowpaths:

Filters:
world 342296 vmm0:2-vm-RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979 vcUuid:'3f
43 54 76 8f 54 4e 5a-8d 01 59 65 4a 4e 99 79'
port 50331660 2-vm-RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979.eth1
vNic slot 2
  name: nic-342296-eth1-vmware-sfw.2
  agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
vNic slot 1
  name: nic-342296-eth1-dvfilter-generic-vmware-swsec.1
  agentName: dvfilter-generic-vmware-swsec
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Alternate Opaque Channel
port 50331661 (disconnected)
vNic slot 2
  name: nic-342296-eth2-vmware-sfw.2 <===== DFW filter
  agentName: vmware-sfw
  state: IOChain Detached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
```

```

    filter source: Dynamic Filter Creation
port 33554441 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979
vNic slot 2
    name: nic-342296-eth0-vmware-sfw.2<===== DFW filter
    agentName: vmware-sfw
    state: IOChain Attached
    vmState: Detached
    failurePolicy: failClosed
    slowPathID: none
    filter source: Dynamic Filter Creation

```

11 Ejecute el comando `show dfw host hostID filter filterID rules`.

Por ejemplo:

```

# show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules

ruleset domain-c33 {
    # Filter rules
    rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
    rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
    rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
    rule 1011 at 4 inout protocol icmp icmp type 8 from any to addrset dst1011 accept;
    rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
    rule 1010 at 6 inout protocol icmp icmp type 8 from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 accept;
    rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
    rule 1009 at 8 inout protocol icmp icmp type 8 from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 accept;
    rule 1003 at 9 inout protocol ipv6-icmp icmp type 136 from any to any accept;
    rule 1003 at 10 inout protocol ipv6-icmp icmp type 135 from any to any accept;
    rule 1002 at 11 inout protocol udp from any to any port 67 accept;
    rule 1002 at 12 inout protocol udp from any to any port 68 accept;
    rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
    # Filter rules
    rule 1004 at 1 inout ethertype any from any to any accept;
}

```

12 Ejecute el comando `show dfw host hostID filter filterID addrsets`.

Por ejemplo:

```

# show dfw host host-28 filter nic-342296-eth2-vmware-sfw.2 addrsets

addrset dst1011 {
ip 172.16.10.10,
ip 172.16.10.11,
ip 172.16.10.12,
}

```

```
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-10 {
ip 172.16.10.11,
ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-11 {
ip 172.16.20.11,
ip fe80::250:56ff:feae:23b9,
}
addrset ip-securitygroup-12 {
ip 172.16.30.11,
ip fe80::250:56ff:feae:d42b,
}
addrset src1013 {
ip 172.16.10.12,
ip 172.17.10.11,
ip fe80::250:56ff:feae:cf88,
ip fe80::250:56ff:feae:f86b,
}
```

- 13** Si realizó correctamente cada uno de los pasos anteriores para solucionar los problemas y no puede publicar reglas en el firewall para las máquinas virtuales, ejecute una sincronización forzada a nivel de host a través de la UI de NSX Manager o a través de la llamada a la API de REST siguiente.

```
URL : [https:]https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

Solución

Notas:

- Asegúrese de que VMware Tools se ejecuta en las máquinas virtuales si las reglas del firewall no utiliza direcciones IP. Para obtener más información, consulte <https://kb.vmware.com/kb/2084048>.

VMware NSX 6.2.0 incorpora la opción para detectar la dirección IP de las máquinas virtuales con intromisión DHCP o intromisión ARP. Estos mecanismos de detección nuevos permiten que NSX aplique las reglas de seguridad basadas en dirección IP en máquinas virtuales que no tienen VMware Tools instalado. Si desea obtener más información, consulte las notas de la versión NSX 6.2.0.

DFW se activa en cuanto se complete el proceso de preparación del host. Si una máquina virtual no necesita en absoluto el servicio de DFW, se puede agregar a la lista de exclusión de funcionalidad (por defecto, NSX Manager, los controladores NSX y las puertas de enlace de servicios Edge se excluyen automáticamente de la función del DFW). El acceso a vCenter Server puede bloquearse al crear una regla Negar todo (Deny all) en el DFW. Para obtener más información, consulte <https://kb.vmware.com/kb/2079620>.

- Cuando sea necesario solucionar problemas del distributed firewall (DFW) de VMware NSX 6X con VMware Technical Support, son necesarios los siguientes datos:
 - La salida del comando `show dfw host hostID summarize-dvfilter` de cada host ESXi del clúster.
 - La configuración del distributed firewall que se obtiene en la pestaña **Redes y seguridad > Firewall > General** (Networking and Security > Firewall > General) y hacer clic en **Exportar configuración** (Export Configuration). Estos pasos exportan la configuración del distributed firewall a formato XML.
 - Registros de NSX Manager. Para obtener más información, consulte <https://kb.vmware.com/kb/2074678>.
 - Registros de vCenter Server. Para obtener más información, consulte <https://kb.vmware.com/kb/1011641>.

Firewall de identidad

Problema

Se produce un error al publicar o actualizar las reglas del firewall de identidad.

Causa

El firewall de identidad (IDFW) permite normas del firewall distribuido establecidas por el usuario (DFW)

Las reglas del firewall distribuido establecidas por el usuario están determinadas por la pertenencia a un grupo Active Directory (AD). IDFW supervisa si los usuarios de Active Directory iniciaron sesión y asignan el registro a una dirección IP que usa el DFW para aplicar reglas del firewall. IDFW necesita el marco Guest Introspection o la extracción de los registros de eventos de Active Directory.

Solución

- 1 Asegúrese de que la sincronización completa/delta del servidor de Active Directory esté funcionando en NSX Manager.
 - a En vSphere Web Client, inicie sesión en el vCenter vinculado a NSX Manager.
 - b Desplácese hasta **Inicio > Redes y seguridad > NSX Manager** (Home > Networking & Security> NSX Managers) y, a continuación, seleccione el NSX Manager de la lista.
 - c Seleccione la pestaña **Administrar** (Manage) y, a continuación, la pestaña **Dominios** (Domains). Seleccione su dominio de la lista. Compruebe que en la columna **Estado de la última sincronización** (Last Synchronization Status) aparezca CORRECTO (SUCCESS) y que la **Hora de la última sincronización** (Last Synchronization Time) sea la actual.
- 2 Si el entorno de firewall utiliza el método de extracción de registros de eventos, siga estos pasos para comprobar que configuró un servidor de registro de eventos para el dominio:
 - a En vSphere Web Client, inicie sesión en el vCenter vinculado a NSX Manager.
 - b Desplácese hasta **Inicio > Redes y seguridad > NSX Manager** (Home > Networking & Security> NSX Managers) y, a continuación, seleccione el NSX Manager de la lista.
 - c Seleccione la pestaña **Administrar** (Manage) y, a continuación, la pestaña **Dominios** (Domains). Seleccione su dominio de la lista. Aquí puede ver y modificar la configuración detallada de dominios.
 - d Seleccione los **Servidores de registro de eventos** (Event Log Servers) de los detalles del dominio y compruebe que el servidor de registro de eventos esté agregado.
 - e Seleccione el servidor de registro de eventos y compruebe que en la columna **Estado de la última sincronización** (Last Synchronization Status) aparezca CORRECTO (SUCCESS) y que la **Hora de la última sincronización** sea la actual.
- 3 Si el entorno de firewall utiliza Guest Introspection, el marco de trabajo debe implementarse en los clústeres informáticos donde residirán las máquinas virtuales protegidas por IDFW. El Estado de servicio (Service Health Status) de la interfaz de usuario debe ser de color verde. Puede encontrar la información de diagnóstico de Guest Introspection en el siguiente artículo de la base de conocimientos sobre cómo solucionar problemas en vShield Endpoint o NSX Guest Introspection (<https://kb.vmware.com/kb/2094261>) y en el artículo sobre cómo recopilar registros en la máquina virtual de servicio universal de VMware NSX for vSphere 6.x Guest Introspection (<https://kb.vmware.com/kb/2144624>).

- 4 Después de comprobar que la configuración de su método de detección de inicio de sesión sea correcta, asegúrese de que NSX Manager reciba eventos de inicio de sesión:
 - a Inicie sesión como usuario de Active Directory.
 - b Ejecute el siguiente comando para consultar los eventos de inicio de sesión. Verifique que el usuario reciba los resultados. GET <https://<nsxmgr-ip>/1.0/identity/userIpMapping>.

```
Example output:
<UserIpMappings>
  <UserIpMapping>
    <ip>50.1.111.192</ip>
    <userName>user1_group20</userName>
    <displayName>user1_group20</displayName>
    <domainName>cd.ad1.db.com</domainName>
    <startTime class="sql-timestamp">2017-05-11 22:30:51.0</startTime>
    <startType>EVENTLOG</startType>
    <lastSeenTime class="sql-timestamp">2017-05-11 22:30:52.0</lastSeenTime>
    <lastSeenType>EVENTLOG</lastSeenType>
  </UserIpMapping>
</UserIpMappings>
```

- 5 Verifique que su grupo de seguridad se utilice en una regla de firewall o que tenga una directiva de seguridad asignada. Los grupos de seguridad no se procesarán en IDFW, a menos que una de estas condiciones sea cierta.
- 6 Después de comprobar que IDFW detecte los inicios de sesión correctamente, verifique que el host ESXi en el que reside la máquina virtual de escritorio reciba la configuración correcta. Estos pasos utilizarán la CLI central de NSX Manager. Para comprobar la dirección IP de la máquina virtual de escritorio que se rellena en la lista **ip-securitygroup**:
 - a Consulte [Comandos de la CLI para DFW](#) para recuperar el nombre del filtro aplicado en la máquina virtual de escritorio.
 - b Ejecute el comando `show dfw host hostID filter filterID rules` para ver los elementos de las reglas de ubicación de DFW.
 - c Ejecute el comando `show dfw host hostID filter filterID addrsets` para ver la dirección IP rellena en la lista **ip-securitygroup**. Verifique que su IP aparezca en la lista.

Solución

Nota: Esta información es útil para solucionar problemas relacionados con IDFW mediante el soporte técnico de VMware:

- Si utiliza los datos de escala de Active Directory de la extracción de registros de eventos:
 - Número de dominios para un único NSX Manager
 - Número de bosques
 - Número de usuarios por bosque
 - Número de usuarios por dominio

Número de grupos de Active Directory por dominio

Número de usuarios por grupo de Active Directory

Número de Active Directory por usuario

Número de controladores de dominio

Número de servidores de registro de Active Directory

- Datos de escala de inicio de sesión de usuario:
 - Número medio de usuarios por minuto
- Detalles de la implementación mediante IDFW con VDI:
 - Número de escritorios VDI por VC
 - Número de hosts por VC
 - Número de escritorios VDI por host
- Si utiliza Guest Introspection:
 - Versión de VMTools (controladores de Guest Introspection)
 - Versión del sistema operativo invitado Windows

Solucionar problemas del equilibrio de carga

6

El equilibrador de carga de NSX Edge permite que el tráfico de red siga varias rutas de acceso a un destino específico. Distribuye las solicitudes de servicio entrante de manera uniforme entre varios servidores de forma tal que la distribución de carga sea transparente para los usuarios. Existen dos tipos de servicios de equilibrio de carga que se pueden configurar en NSX: el modo one-arm (también denominado modo proxy) o el modo en línea (al que también se le conoce como el modo transparente). Para obtener más información, consulte la *Guía de administración de NSX*.

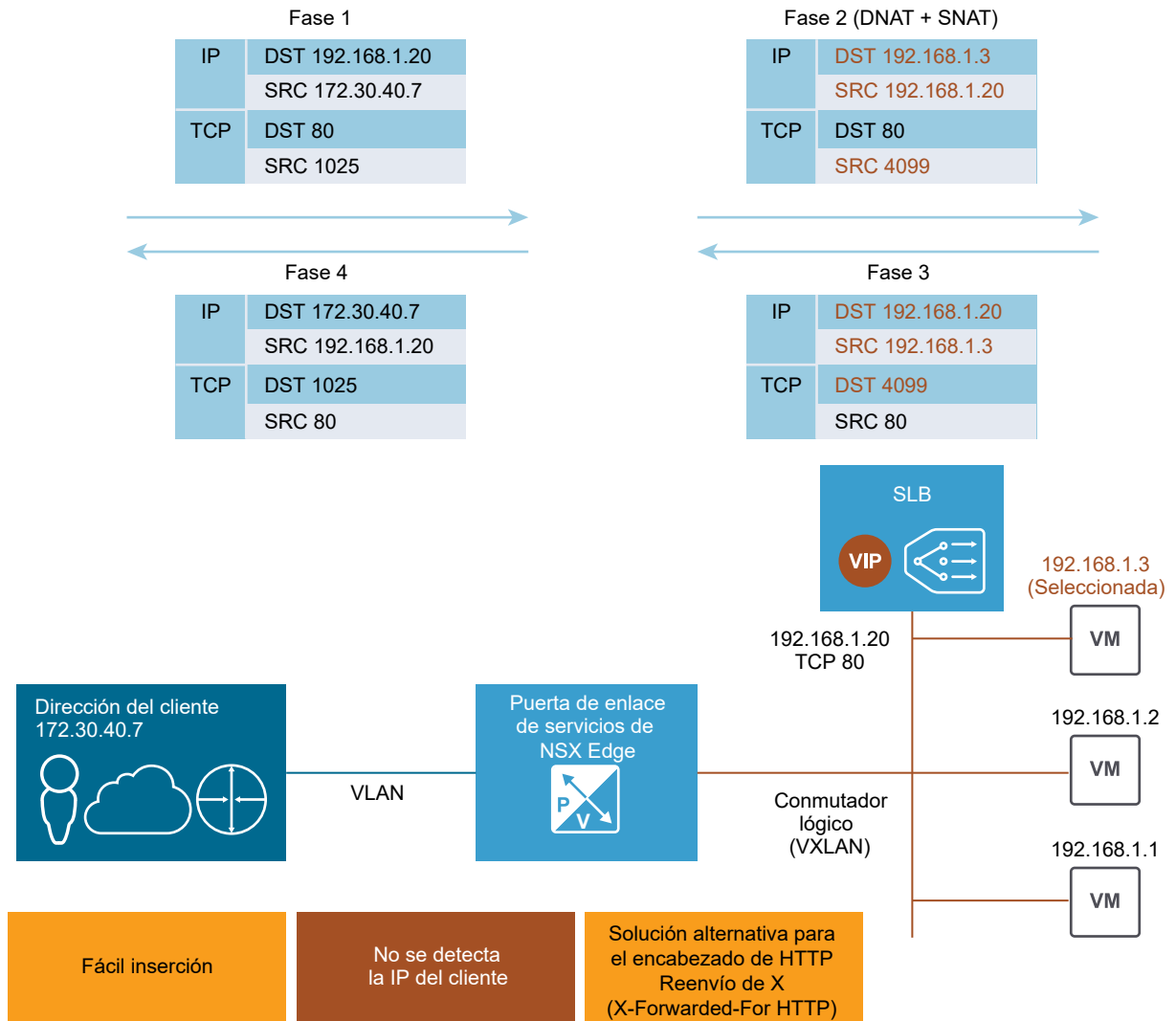
Antes de empezar a solucionar problemas y verificar la configuración, describa el error con precisión, cree un mapa de topología del cliente, el servidor virtual y el servidor backend, y consulte los requisitos de la aplicación. Por ejemplo, si un cliente no puede conectarse, no es igual que los errores de sesión que se pueden producir después de establecer la conexión. Al solucionar los problema relacionados con el equilibrador de carga, verifique siempre en primer lugar los errores de conectividad.

Este capítulo incluye los siguientes temas:

- [Configurar un equilibrador de carga one-armed](#)
- [Diagrama de flujo de solución de problemas del equilibrador de carga](#)
- [Verificación de configuración del equilibrador de carga y solución de problemas a través de la interfaz de usuario](#)
- [Resolución de problemas del equilibrador de carga a través de la CLI](#)
- [Problemas frecuentes del equilibrador de carga](#)

Configurar un equilibrador de carga one-armed

La puerta de enlace de servicio de Edge (ESG) puede estar concebida como un proxy para el tráfico de cliente entrante.



En modo proxy, el equilibrador de carga utiliza su propia dirección IP como dirección de origen para enviar solicitudes a un servidor backend. El servidor backend ve todo el tráfico que se envía desde el equilibrador de carga y responde directamente al equilibrador de carga. Este modo también se conoce como modo SNAT o modo no transparente. Para obtener más información, consulte la *Guía de administración de NSX*.

Se implementa un equilibrador de carga one-armed de NSX en la misma subred con sus servidores backend, aparte del enrutador lógico. El servidor virtual del equilibrador de carga de NSX atiende a una IP virtual para las solicitudes entrantes del cliente y distribuye las solicitudes a los servidores backend. Para el tráfico de retorno, es necesario que el NAT inverso cambie la dirección IP de origen desde el servidor backend a una dirección IP virtual (VIP) y que luego envíe la dirección IP virtual al cliente. Sin esta operación, se interrumpirá la conexión con el cliente.

Después de que la ESG reciba el tráfico, realiza dos operaciones: Traducción de operaciones de red de destino, DNAT (Destination Network Address Translation), para cambiar la dirección VIP de la dirección IP en una de las máquinas de equilibrador de carga y Traducción de direcciones de red de origen, SNAT (Source Network Address Translation), para intercambiar la dirección IP del cliente con la dirección IP de ESG.

A continuación, el servidor de ESG envía el tráfico al equilibrador de carga y el servidor de este último envía la respuesta de vuelta a ESG y luego de vuelta al cliente. Es más sencillo configurar esta opción que configurar el modo en línea, pero tiene dos advertencias potenciales. La primera es que este modo necesita un servidor ESG dedicado y la segunda es que el servidor del equilibrador de carga no conoce la dirección IP del cliente original. Una solución alternativa para las aplicaciones HTTP/HTTPS es habilitar Insertar el reenvío de X (Insert X-Forwarded-For) en el perfil de la aplicación de HTTP para que lleve la dirección IP del cliente en el encabezado del reenvío de X (X-Forwarded-For) en la solicitud enviada al servidor backend.

Si es necesaria la visibilidad de la dirección IP del cliente en el servidor backend para aplicaciones que no sean HTTP/HTTPS, puede configurar el grupo de IP para que sean transparentes. En caso de que los clientes no estén en la misma subred que el servidor backend, se recomienda el modo en línea. De lo contrario, debe usar la dirección IP del equilibrador de carga como puerta de enlace predeterminada del servidor backend.

Nota Normalmente, existen tres métodos para garantizar la integridad de la conexión:

- Modo en línea/transparente
- SNAT/proxy/modo no transparente (mencionado anteriormente)
- Direct Server Return (DSR): no compatible actualmente

En el modo DSR, el servidor backend responde directamente al cliente. Actualmente, el equilibrador de carga de NSX no admite DSR.

Procedimiento

- 1 Como ejemplo, puede configurar un servidor virtual one-armed con descarga de SSL. Haga doble clic en Edge para crear un certificado y, a continuación, seleccione **Administrar > Configuración > Certificado** (Manage > Settings > Certificate).

- Habilite el servicio de equilibrador de carga mediante la selección de **Administrar > Equilibrador de carga > Configuración global > Editar** (Manage > Load Balancer > Global Configuration > Edit).

Edit Load balancer global configuration

☒ Enable Load Balancer

☐ Enable Acceleration

☐ Logging

Log Level: Info ▼

☐ Enable Service Insertion

Service Definition:

Service Configuration:

Deployment Specification:

- Cree un perfil de aplicación HTTPS mediante la selección de **Administrar > Equilibrador de carga > Perfiles de aplicación** (Manage > Load Balancer > Application Profiles).

New Profile ?

Name:

Type: HTTPS ▼

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: None ▼

Cookie Name:

Mode: ▼

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certifica... Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

Nota La captura de pantalla anterior utiliza certificados autofirmados solo para documentación.

- De forma opcional, haga clic en **Administrar > Equilibrador de carga > Supervisión del servicio** (Manage > Load Balancer > Service Monitoring) y edite la supervisión del servicio por defecto para cambiarla de HTTP/HTTPS básicos a URL/URIs específicas, según sea necesario.

- 5 Cree grupos de servidores mediante la selección de **Administrar > Equilibrador de carga > Grupos** (Manage > Load Balancer > Pools).

Para usar el modo SNAT, deje la casilla **Transparente** (Transparent) sin marcar en la configuración del grupo.

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

☐ Transparent

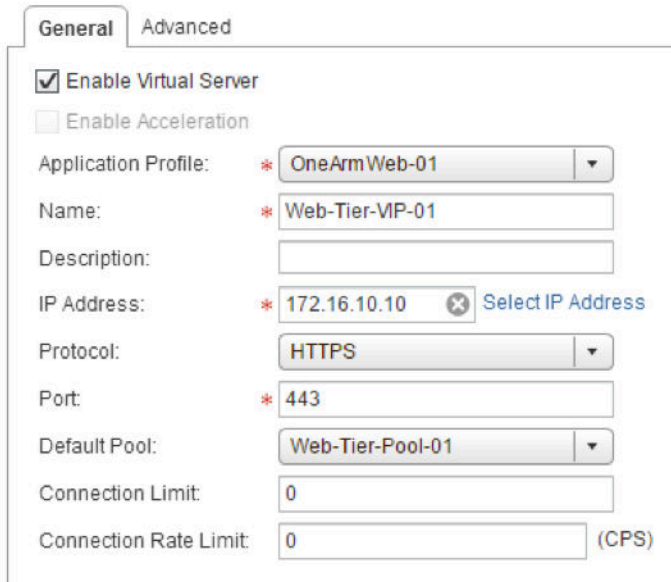
Compruebe que todas las máquinas virtuales están en la lista y habilitadas.

- 6 De forma opcional, haga clic en **Administrar > Equilibrador de carga > Grupos > Mostrar estadísticas de grupo** (Manage > Load Balancer > Pools > Show Pool Statistics) para revisar el estado.

Asegúrese de que el estado de miembro es LISTO (UP).

- 7 Cree un servidor virtual mediante la selección de **Administrar > Equilibrador de carga > Servidores virtuales** (Manage > Load Balancer > Virtual Servers).

Si quisiera utilizar el equilibrador de carga de Capa 4 para UDP o un rendimiento mayor de TCP, active **Habilitar aceleración** (Enable Acceleration). Si activa **Habilitar aceleración** (Enable Acceleration), asegúrese de que el estado del firewall es **Habilitado** (Enabled) en el equilibrador de carga de NSX Edge, porque se necesita un firewall para el SNAT de Capa 4.



General | Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

Application Profile: * OneArmWeb-01 ▼

Name: * Web-Tier-VIP-01

Description:

IP Address: * 172.16.10.10 ✕ Select IP Address

Protocol: HTTPS ▼

Port: * 443

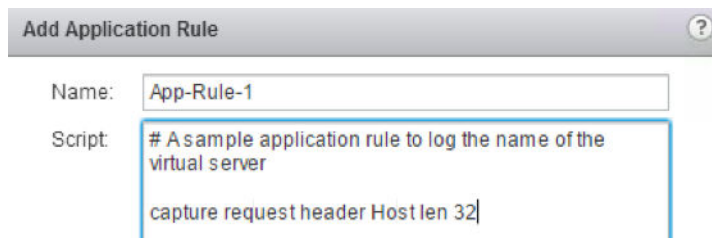
Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

Compruebe que la dirección IP está unida al grupo de servidores.

- 8 De forma opcional, si utiliza una regla de aplicaciones, compruebe la configuración en **Administrar > Equilibrador de carga > Reglas de aplicaciones** (Manage > Load Balancer > Application Rules).



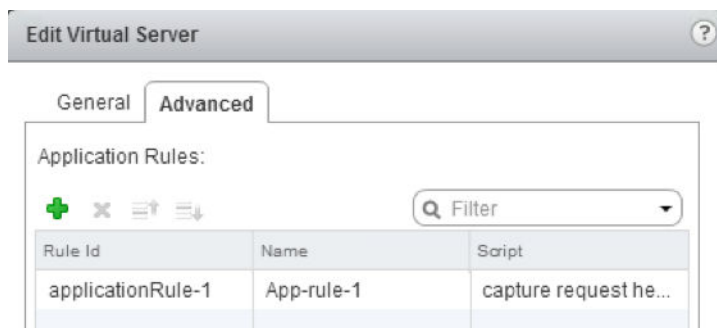
Add Application Rule ?

Name: App-Rule-1

Script: # A sample application rule to log the name of the virtual server
capture request header Host len 32

- 9 Si utiliza una regla de aplicaciones, asegúrese de que dicha regla está asociada con el servidor virtual en **Administrar > Equilibrador de carga > Servidores virtuales > Avanzado** (Manage > Load Balancer > Virtual Servers > Advanced).

Para ejemplos compatibles, consulte <https://communities.vmware.com/docs/DOC-31772>.



Edit Virtual Server ?

General | **Advanced**

Application Rules:

+ ✕ ⌵ ⌴ Filter

Rule Id	Name	Script
applicationRule-1	App-rule-1	capture request he...

En el modo no transparente, el servidor backend no puede consultar la IP del cliente, pero sí puede ver el equilibrador de carga de la dirección IP interna. Como solución alternativa al tráfico de HTTP/HTTPS, active el encabezado **Insertar X-Forwarded-For HTTP** (Insert X-Forwarded-For HTTP). Con esta opción activa, el equilibrador de carga de Edge agrega el encabezado "X-Forwarded-For" con el valor de la dirección IP de origen del cliente.

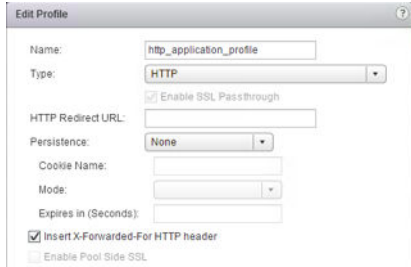
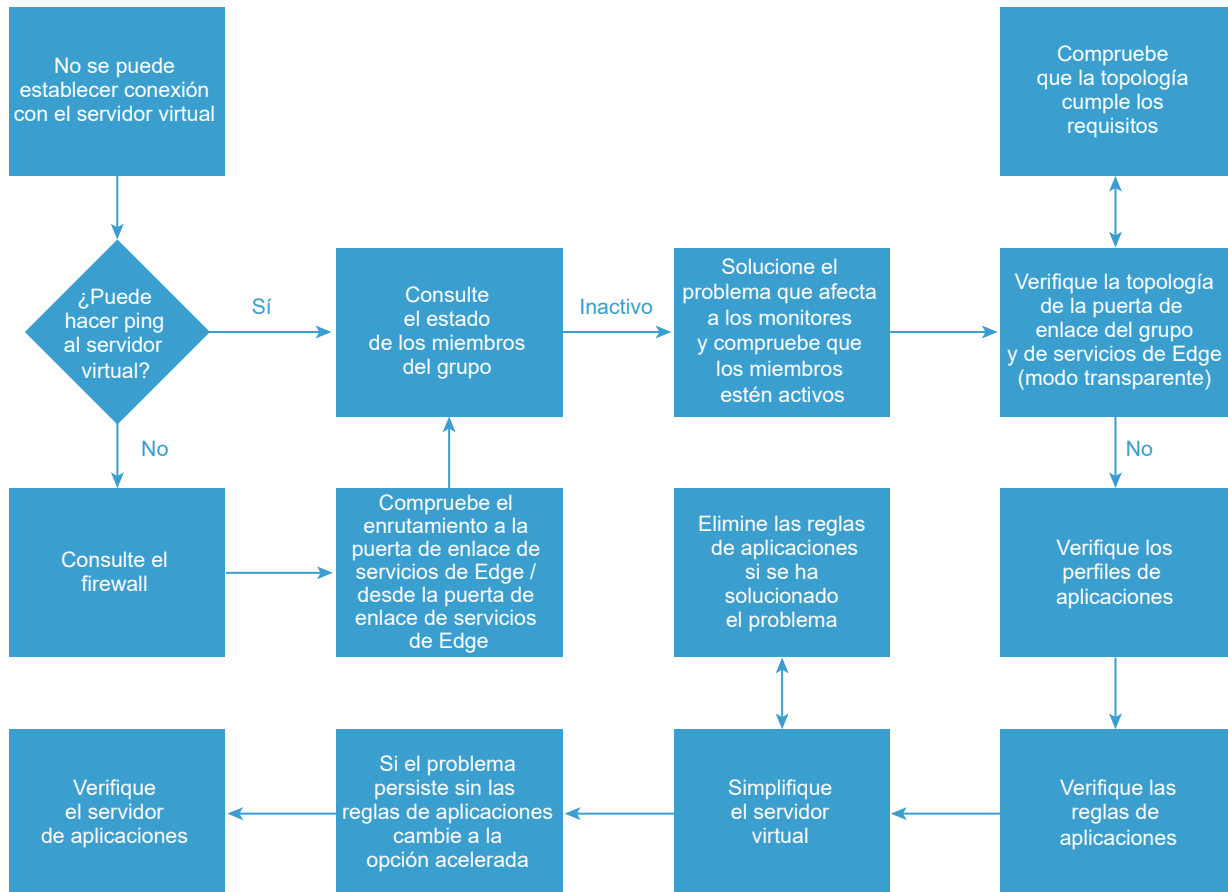


Diagrama de flujo de solución de problemas del equilibrador de carga

El diagrama de flujo ofrece una visión general de cómo solucionar los problemas del equilibrador de carga.



Verificación de configuración del equilibrador de carga y solución de problemas a través de la interfaz de usuario

Puede verificar la configuración del equilibrador de carga a través de vSphere Web Client. La interfaz de usuario permite solucionar algunos problemas relacionados con el equilibrador de carga.

Una vez que comprenda lo que debe funcionar y defina el problema, verifique la configuración a través de la interfaz de usuario de la siguiente manera.

Requisitos previos

Apunte la siguiente información:

- La IP, el protocolo y el puerto del servidor virtual.
- La IP y el puerto de los servidores de aplicaciones backend.
- La topología que desea utilizar: one-armed o en línea. Para obtener más información, consulte el tema sobre el equilibrador de carga lógico en la *Guía de administración de NSX*.
- Verifique la traceroute y utilice otras herramientas de conectividad de red para ver qué paquetes se dirigen a la ubicación correcta (puerta de enlace de servicios de Edge).
- Compruebe que los firewalls ascendentes permitan el tráfico correctamente.
- Defina su problema. Por ejemplo, los registros de DNS del servidor virtual son correctos, pero no se recibe contenido o este es incorrecto.

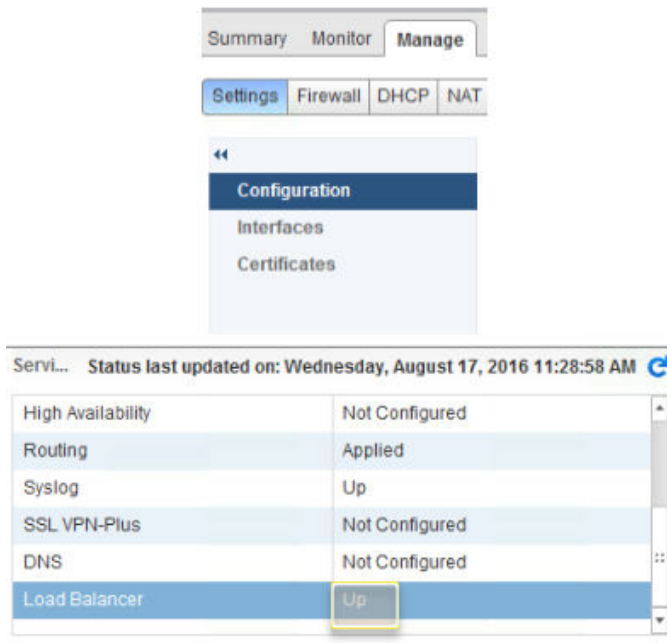
Problema

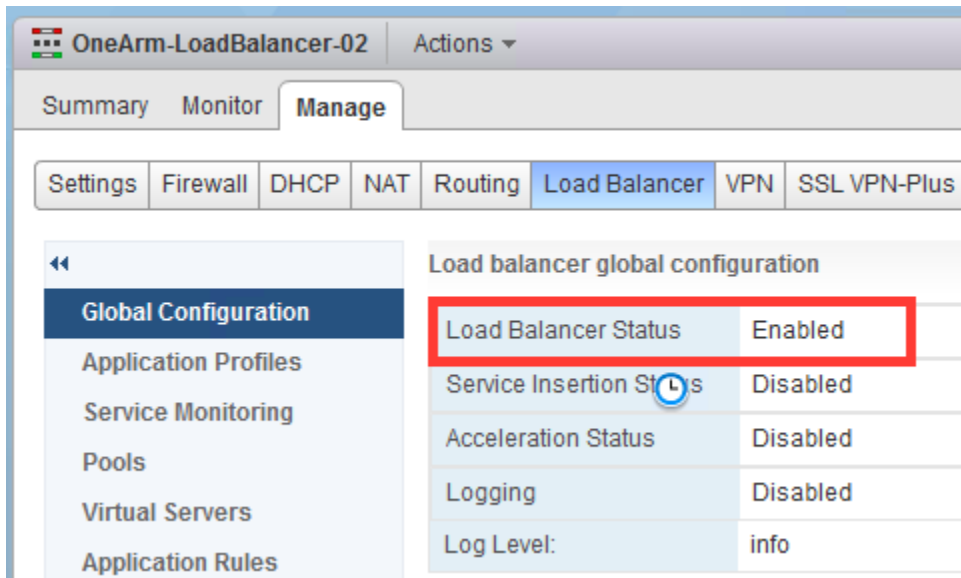
El equilibrador de carga no funciona según lo esperado.

Solución

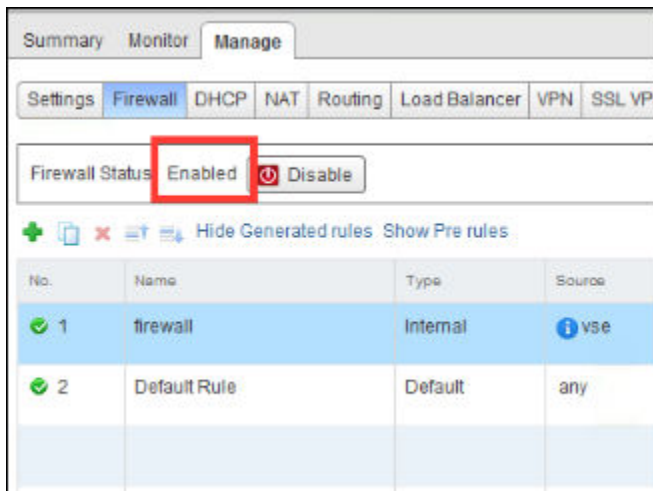
- 1 Compruebe estos requisitos: protocolos necesarios compatibles con el equilibrador de carga (TCP, UDP, HTTP, HTTPS), puertos, requisitos de persistencia y miembros del grupo.
 - ¿Están habilitados el firewall y el equilibrador de carga? ¿Tiene la puerta de enlace de servicios de Edge las rutas adecuadas?
 - ¿A qué dirección IP, puerto y protocolo debe atender el servidor virtual?
 - ¿Se utiliza la descarga de SSL? ¿Necesita SSL para comunicarse con los servidores backend?
 - ¿Está utilizando las reglas de aplicaciones?
 - ¿Cuál es la topología? El equilibrador de carga de NSX debe analizar todo el tráfico del cliente y del servidor.
 - ¿El equilibrador de carga de NSX es en línea o se traduce la dirección de origen del cliente para garantizar que el tráfico de retorno vuelve al equilibrador de carga?

- 2 Acceda a NSX Edge y verifique las configuraciones necesarias para habilitar el equilibrio de carga y permitir que el tráfico fluya de la siguiente manera:
 - a Compruebe que el equilibrador de carga esté **Activo** (Up).





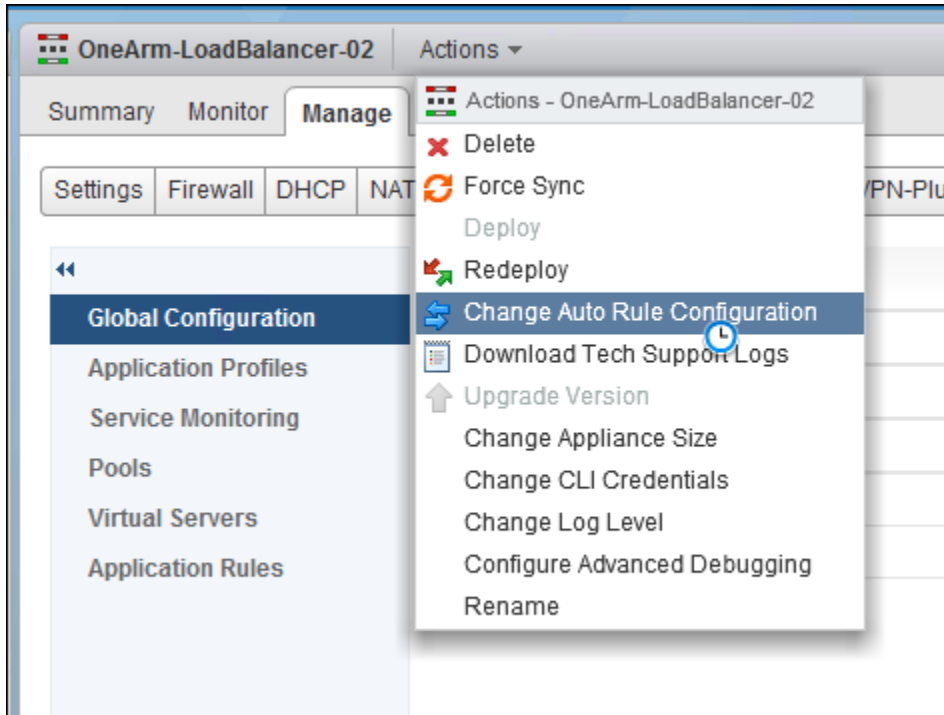
- b Verifique que el firewall esté **Habilitado** (Enabled). Debe estar habilitado en el caso de los servidores virtuales acelerados. La política de las VIP HTTP/HTTPS de Capa 7 y TPC no aceleradas debe permitir el tráfico. Tenga en cuenta que los filtros del firewall no afectarán a los servidores virtuales acelerados.



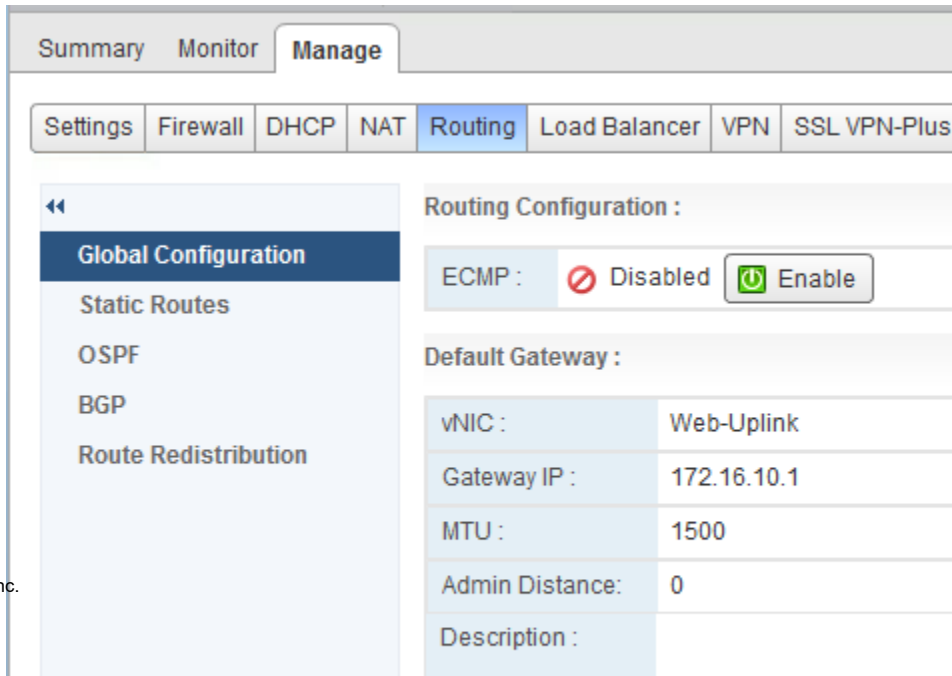
- c Verifique que las reglas NAT se crearon para el servidor virtual. En la pestaña **NAT** (NAT), haga clic en el vínculo **Ocultar reglas internas** (Hide internal rules) o **Mostrar reglas internas** (Unhide internal rules) para verificarlas.

Nota Si tiene el equilibrio de carga habilitado y los servicios configurados, pero no tiene ninguna regla NAT configurada, significa que no estaba habilitada la configuración de reglas automáticas.

- d Puede cambiar estas configuraciones. Para obtener más información, consulte el tema sobre cómo cambiar la configuración de reglas automáticas en la *Guía de administración de NSX*. Cuando implementa una puerta de enlace de servicios de NSX Edge tiene la opción de definir la configuración de reglas automáticas. Si no seleccionó esta opción al implementarla, debe habilitarla para que el equilibrador de carga funcione correctamente. Compruebe el estado del miembro del grupo a través de la interfaz de usuario.



- e Verifique el enrutamiento y compruebe que la puerta de enlace de servicios de Edge tenga una ruta predeterminada o estática a los sistemas del cliente y a los servidores backend. Si no hay ninguna ruta a los servidores, no se aprobará la comprobación de estado. Si utiliza un protocolo de enrutamiento dinámico, es posible que deba usar la CLI. Para obtener más información, consulte [CLI del enrutamiento de NSX](#).
- a Verifique la ruta predeterminada.



Edge tiene una interfaz en la subred. En muchas ocasiones, los servidores de aplicaciones están conectados a estos servidores.

0 Job(s) In Progress
 0 Job(s) Failed

aces of this NSX Edge.

Actions

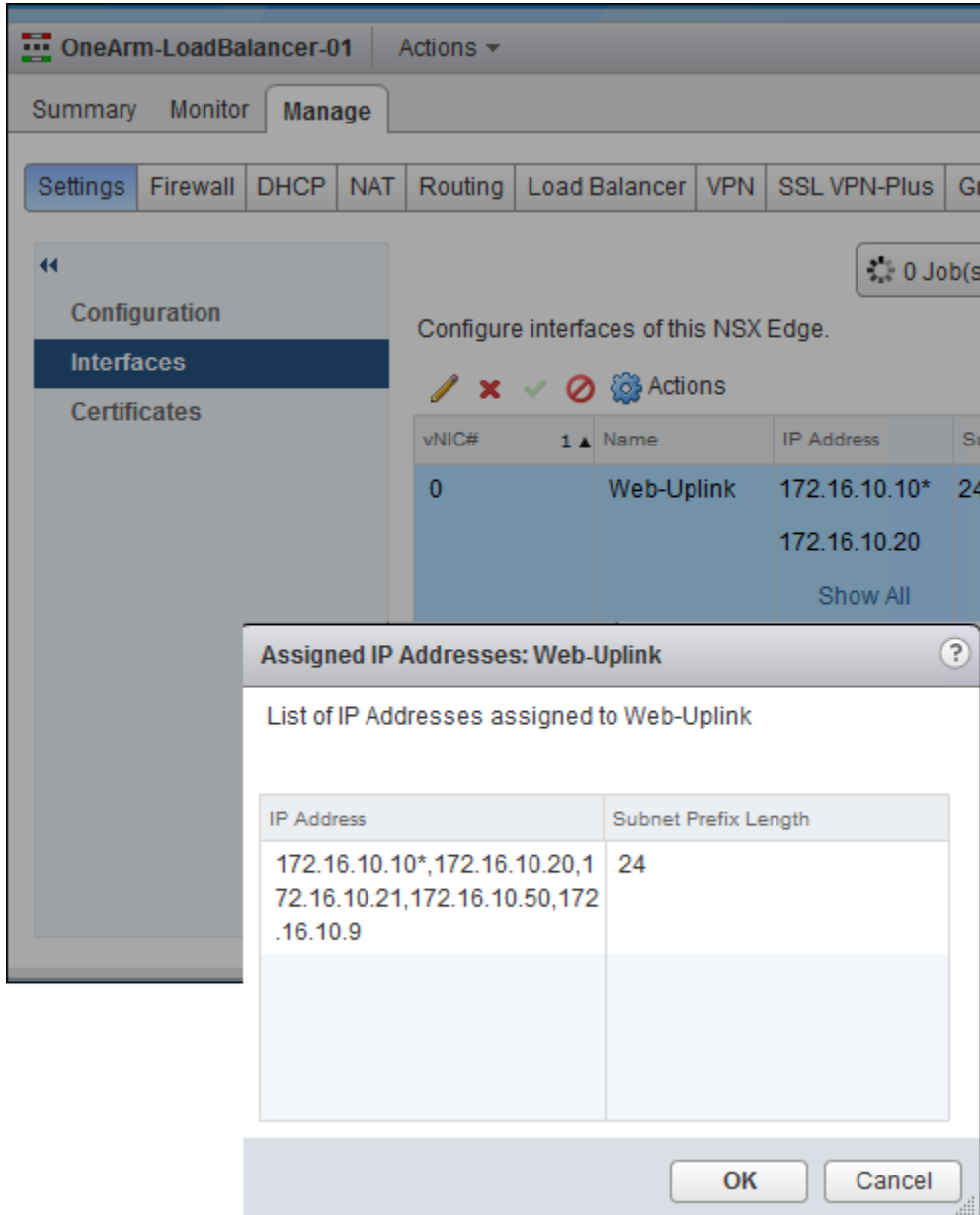
Filter

Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
Web-Uplink	172.16.10.10*	24	Web-Tier-01	Uplink	✓
	172.16.10.20				
	Show All				
INLINE_SUBNI	172.16.100.1*	24	INLINE_SUBNI	Internal	✓
vnic2				Internal	✗
vnic3				Internal	✗
vnic4				Internal	✗
vnic5				Internal	✗

- c Verifique las rutas estáticas en la pestaña **Enrutamiento** (Routing) > **Rutas estáticas** (Static Routes).

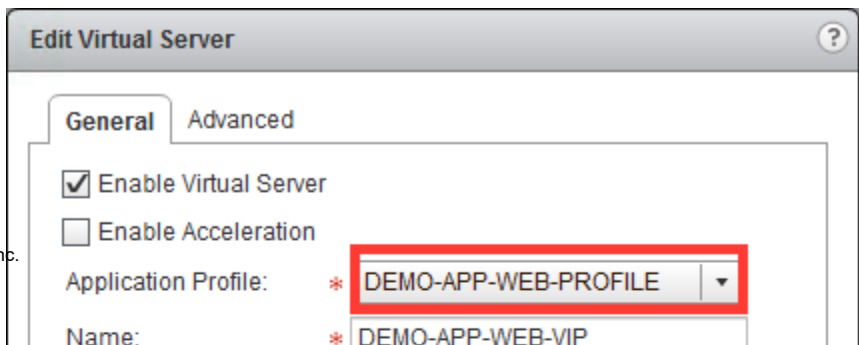
3 Compruebe la dirección IP, el puerto y el protocolo del servidor virtual.

- a Haga doble clic en NSX Edge y acceda a **Administrar (Manage) > Configuración (Settings) > Interfaces (Interfaces)**. Verifique que la dirección IP del servidor virtual se agregue a una interfaz.



- b Compruebe que el servidor virtual tenga configurados la dirección IP adecuada, los puertos y los protocolos adecuados compatibles con la aplicación.

- a Verifique el perfil de aplicación que utiliza el servidor virtual.



o HTTPS) del servidor virtual.

Edit Virtual Server

General | Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

Application Profile: * DEMO-APP-WEB-PROFILE ▼

Name: * DEMO-APP-WEB-VIP

Description:

IP Address: * 172.16.10.20 × [Select IP Address](#)

Protocol: HTTPS ▼

Port: * 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

OK Cancel

- c Verifique que el perfil de la aplicación se corresponda con el método persistente compatible, el tipo (protocolo) y SSL (si es necesario). Si utiliza SSL, el nombre y la fecha de caducidad deben ser correctos.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.CO	DEMO.WEB.APP.CO	Wed Apr 27 2016 - Sat
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- d Verifique si se utiliza el certificado correcto para que los clientes se conecten.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☒ Enable Pool Side SSL

Virtual Server Certificates **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.COF	DEMO.WEB.APP.COF	Wed Apr 27 2016 - Sa
<input type="radio"/>	VSM_SOLUTION_71f	VSM_SOLUTION_71f	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71f	VSM_SOLUTION_71f	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Th
<input type="radio"/>	VSM_SOLUTION_49c	VSM_SOLUTION_49c	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49c	VSM_SOLUTION_49c	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- e Compruebe si necesita un certificado de cliente, pero estos no están configurados. Además, debe verificar si ha seleccionado una lista de cifrado demasiado limitada (por ejemplo, si los clientes utilizan navegadores más antiguos).

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.CO	DEMO.WEB.APP.CO	Wed Apr 27 2016 - Sat
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- f Compruebe si necesita SSL para los servidores backend.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

4 Consulte la configuración y el estado del grupo de la siguiente manera:

- a Verifique el estado del grupo. Al menos un miembro debe estar activo para garantizar el tráfico, aunque es posible que uno no sea suficiente para todo el tráfico. Si no hay ninguno o el número de miembros del grupo activos es limitado, intente solucionar este problema siguiendo los pasos que se indican a continuación.

Pool ID

Pool Name

Pool Status

Pool ID

Pool Name

Pool Status

pool-1

TENANT-1-TCP-P...

UP

Member ID

Member Name

Member IP Address / VC Container

Member Status

Member ID

SERVER-1

10.10.10.100

UP

member-1

SERVER-2

10.10.10.101

UP

member-2

- b Verifique si la topología utilizada es correcta. El tráfico de cliente de SNAT se controla en la configuración del grupo. Si la puerta de enlace de servicios de Edge que aloja la función del equilibrador de carga no está en línea para ver todo el tráfico, se producirá un error. Para proteger la IP de origen del cliente, seleccione el modo **Transparente** (Transparent). Para obtener información, consulte la *Guía de administración de NSX*.

Edit Pool

Name:

* DEMO_APP_WEB_POOL

Description:

Algorithm:

ROUND-ROBIN

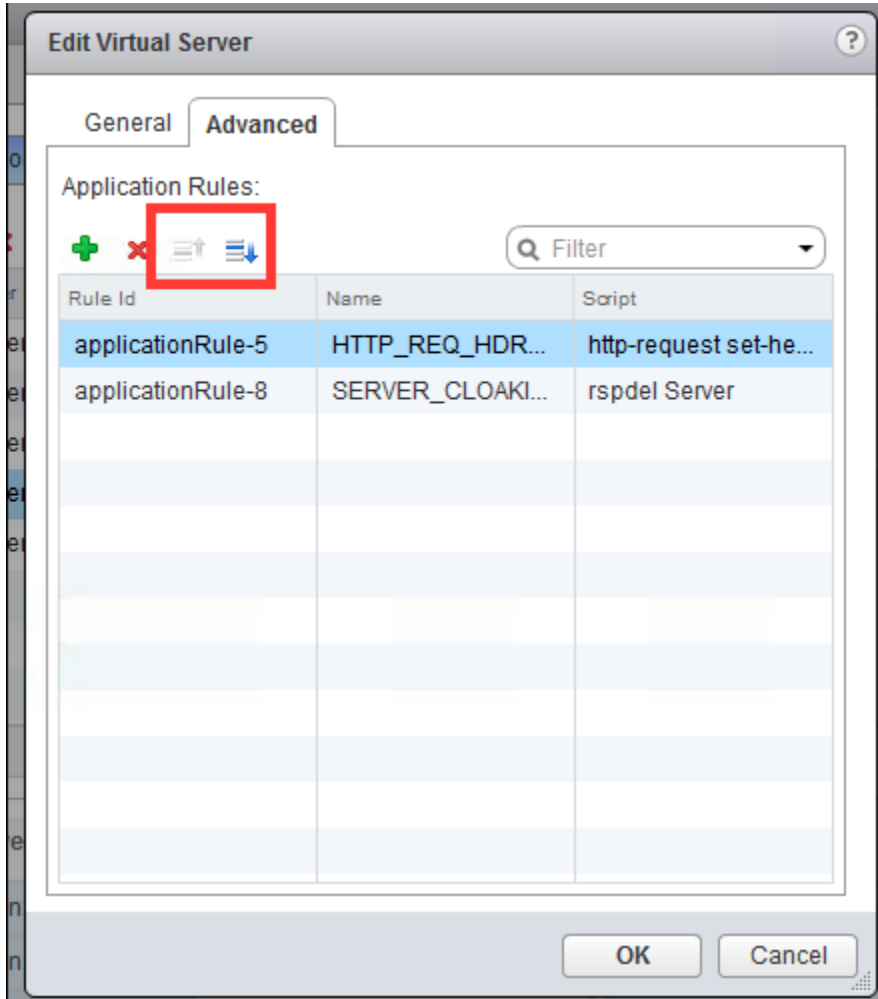
Algorithm Parameters:

Monitors:

default_http_monitor

Members:

- 5 Si utiliza reglas de aplicaciones, verifíquelas. Elimínelas si es necesario para ver si el tráfico fluye.
 - a Vuelva a organizar las reglas para ver si el orden hace que la lógica interrumpa el flujo del tráfico. Para obtener información sobre cómo agregar una regla de aplicación y ver ejemplos, consulte ese tema en la *Guía de administración de NSX*.



Pasos siguientes

Si no pudo localizar el problema, es posible que deba usar la CLI (interfaz de línea de comandos) para saber qué ocurre. Para obtener más información, consulte [Resolución de problemas del equilibrador de carga a través de la CLI](#).

Resolución de problemas del equilibrador de carga a través de la CLI

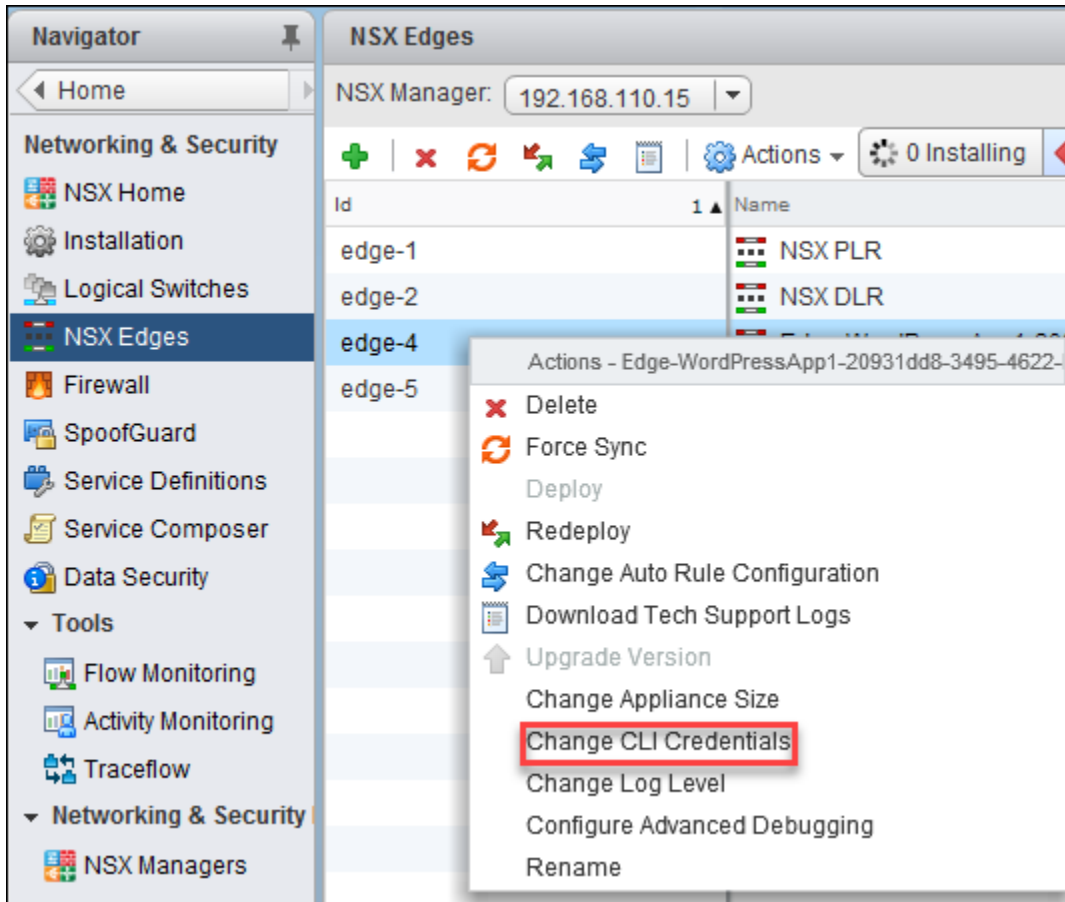
La CLI de NSX permite obtener copias detalladas del final del registro, tomar capturas de paquetes y consultar las métricas para la resolución de problemas del equilibrador de carga.

Problema

El equilibrio de carga no funciona según lo esperado.

Solución

- 1 Habilite el protocolo SSH o verifique que pueda asignarlo al dispositivo virtual. La puerta de enlace de servicios de Edge es un dispositivo virtual que tiene la opción de habilitar el protocolo SSH al implementarlo. Si necesita habilitarlo, seleccione el dispositivo necesario y, en el menú **Acciones** (Actions), haga clic en **Cambiar credenciales de CLI** (Change CLI Credentials).



- 2 La puerta de enlace de servicios de Edge tiene varios comandos de visualización para consultar el estado del tiempo de ejecución o de la configuración. Utilícelos para mostrar información sobre estadísticas y configuración.

```
nsxedge> show configuration loadbalancer
nsxedge> show configuration loadbalancer virtual [virtual-server-name]
nsxedge> show configuration loadbalancer pool [pool-name]
nsxedge> show configuration loadbalancer monitor [monitor-name]
nsxedge> show configuration loadbalancer profile [profile-name]
nsxedge> show configuration loadbalancer rule [rule-name]
```

- Para que las reglas NAT y el equilibrio de carga funcionen correctamente, el firewall debe estar habilitado. Utilice el comando `#show firewall`. Si no encuentra ningún resultado significativo, consulte la sección [Verificación de configuración del equilibrador de carga y solución de problemas a través de la interfaz de usuario](#).

```

NSX-edge-8-0> show firewall
Chain PREROUTING (policy ACCEPT 21947 packets, 7809K bytes)
:cid  pkts bytes target    prot opt in     out     source    destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target    prot opt in     out     source    destination
)      348 67915 ACCEPT    all  --  lo     *       0.0.0.0/0  0.0.0.0/0
)      134  5360 DROP      all  --  *      *       0.0.0.0/0  0.0.0.0/0      state INVALID
)     21482 7736K block_in all  --  *      *       0.0.0.0/0  0.0.0.0/0
)     20545 7671K ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      state RELATED
)       937 65139 usr_rules all  --  *      *       0.0.0.0/0  0.0.0.0/0
)         0 0 DROP      all  --  *      *       0.0.0.0/0  0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target    prot opt in     out     source    destination
Chain OUTPUT (policy ACCEPT 20673 packets, 1248K bytes)
:cid  pkts bytes target    prot opt in     out     source    destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target    prot opt in     out     source    destination
)      348 67915 ACCEPT    all  --  *      lo     0.0.0.0/0  0.0.0.0/0
)       34  1360 DROP      all  --  *      *       0.0.0.0/0  0.0.0.0/0      state INVALID
)     20295 1179K block_out all  --  *      *       0.0.0.0/0  0.0.0.0/0
)         0 0 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      PHYSDEV match
)         0 0 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      PHYSDEV match
)         0 0 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      PHYSDEV match
)         0 0 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      PHYSDEV match
)     14599 802K ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      state RELATED
)       5696 377K usr_rules all  --  *      *       0.0.0.0/0  0.0.0.0/0
)         0 0 DROP      all  --  *      *       0.0.0.0/0  0.0.0.0/0
Chain block_in (1 references)
:cid  pkts bytes target    prot opt in     out     source    destination
Chain block_out (1 references)
:cid  pkts bytes target    prot opt in     out     source    destination
Chain usr_rules (2 references)
:cid  pkts bytes target    prot opt in     out     source    destination
133137 4861 333K ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      match-set 0_
133138 0 0 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      match-set 1_
133139 936 65099 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      match-set 2_
133141 835 43459 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0      match-set 3_
133131 1 40 LOG      all  --  *      *       0.0.0.0/0  0.0.0.0/0      LOG flags 0
133131 1 40 ACCEPT    all  --  *      *       0.0.0.0/0  0.0.0.0/0

```

- 4 El equilibrador de carga necesita que las reglas NAT funcionen correctamente. Utilice el comando `show nat`. Si no encuentra ningún resultado significativo, consulte la sección [Verificación de configuración del equilibrador de carga y solución de problemas a través de la interfaz de usuario](#).

```

NSX-edge-8-0> show nat
Chain PREROUTING (policy ACCEPT 568 packets, 40044 bytes)
rid  pkts bytes target    prot opt in     out     source        destination
0     568 40044 int_dnat  all  --  *      *        0.0.0.0/0      0.0.0.0/0
0     568 40044 usr_dnat  all  --  *      *        0.0.0.0/0      0.0.0.0/0

Chain INPUT (policy ACCEPT 568 packets, 40044 bytes)
rid  pkts bytes target    prot opt in     out     source        destination

Chain OUTPUT (policy ACCEPT 896 packets, 46706 bytes)
rid  pkts bytes target    prot opt in     out     source        destination
0     896 46706 int_dnat  all  --  *      *        0.0.0.0/0      0.0.0.0/0
0     896 46706 usr_dnat  all  --  *      *        0.0.0.0/0      0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 896 packets, 46706 bytes)
rid  pkts bytes target    prot opt in     out     source        destination
0     896 46706 int_snat  all  --  *      *        0.0.0.0/0      0.0.0.0/0
0     896 46706 usr_snat  all  --  *      *        0.0.0.0/0      0.0.0.0/0

Chain int_dnat (2 references)
rid  pkts bytes target    prot opt in     out     source        destination

Chain int_snat (1 references)
rid  pkts bytes target    prot opt in     out     source        destination
0      0    0 ACCEPT    all  --  *      *        0.0.0.0/0      0.0.0.0/0

Chain usr_dnat (2 references)
rid  pkts bytes target    prot opt in     out     source        destination
0      0    0 DNAT      tcp  --  vNic_2  *        0.0.0.0/0      192.168.8.20
0      0    0 LOG       all  --  vNic_2  *        0.0.0.0/0      192.168.8.11
0      0    0 DNAT      all  --  vNic_2  *        0.0.0.0/0      192.168.8.11

Chain usr_snat (1 references)
rid  pkts bytes target    prot opt in     out     source        destination
0      0    0 LOG       all  --  *      vNic_2  10.10.10.101   0.0.0.0/0
0      0    0 SNAT      all  --  *      vNic_2  10.10.10.101   0.0.0.0/0
0      0    0 LOG       all  --  *      vNic_2  10.10.10.0/24  0.0.0.0/0
0      0    0 SNAT      all  --  *      vNic_2  10.10.10.0/24  0.0.0.0/0
NSX-edge-8-0>

```

- 5 Además de tener habilitado el firewall y de que el equilibrador de carga tenga reglas NAT, también debe asegurarse de que el proceso de equilibrio de carga esté habilitado. Utilice el comando `show service loadbalancer` para consultar el estado del motor del equilibrador de cara (Capa 4 o Capa 7).

```

nsxedge> show service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer   : running
-----
L7 Loadbalancer Statistics:
STATUS    PID      MAX_MEM_MB  MAX SOCK  MAX_CONN  MAX_PIPE  CUR_CONN  CONN_RATE

```



```

CONN_RATE_LIMIT MAX_CONN_RATE
running 1580 0 2081 1024 0 0 0
0 0
-----
L4 Loadbalancer Statistics:
MAX_CONN ACT_CONN INACT_CONN TOTAL_CONN
0 0 0 0

Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port Forward Weight ActiveConn InActConn

```

- a El comando `show service loadbalancer session` permite ver la tabla de sesiones del equilibrador de carga. Se mostrarán sesiones si hay tráfico en el sistema.

```

nsxedge> show service loadbalancer session
-----
L7 Loadbalancer Statistics:
STATUS PID MAX_MEM_MB MAX SOCK MAX_CONN MAX_PIPE CUR_CONN CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running 1580 0 2081 1024 0 0 0
0 0

-----L7 Loadbalancer Current Sessions:

0x2192df1f300: proto=unix_stream src=unix:1 fe=GLOBAL be=<NONE> srv=<none> ts=09 age=0s
calls=2 rq[f=c08200h,
i=0,an=00h,rx=20s,wx=,ax=] rp[f=008000h,i=0,an=00h,rx=wx,ax=] s0=[7,8h,fd=1,ex=]
s1=[7,0h,fd=-1,ex=] exp=19s

-----
L4 Loadbalancer Statistics:
MAX_CONN ACT_CONN INACT_CONN TOTAL_CONN
0 0 0 0

L4 Loadbalancer Current Sessions:

pro expire state source virtual destination

```

- b Consulte el comando `show service loadbalancer table` para ver el estado de la tabla estática de Capa 7 del equilibrador de carga. Tenga en cuenta que esta tabla no muestra información sobre servidores virtuales acelerados.

```

nsxedge> show service loadbalancer table
-----
L7 Loadbalancer Sticky Table Status:

TABLE TYPE SIZE(BYTE) USED(BYTE)

```

- 6 Si todos los servicios requeridos funcionan correctamente, consulte la tabla de enrutamiento. Debe tener una ruta al cliente y a los servidores. Utilice los comandos `show ip route` y `show ip forwarding` para asignar rutas a las interfaces.

```

NSX-edge-8-0> sh ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 4

S      0.0.0.0/0          [1/1]      via 192.168.8.2
C      10.10.10.0/24      [0/0]      via 10.10.10.1
C      169.254.1.4/30     [0/0]      via 169.254.1.5
C      192.168.8.0/24     [0/0]      via 192.168.8.3
NSX-edge-8-0> sh ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route

R>* 0.0.0.0/0 via 192.168.8.2, vNic_2
C>* 10.10.10.0/24 is directly connected, vNic_0
C>* 169.254.1.4/30 is directly connected, vNic_0
C>* 192.168.8.0/24 is directly connected, vNic_2
NSX-edge-8-0>

```

- 7 Asegúrese de que los sistemas y los servidores backend tienen una entrada de ARP, como la puerta de enlace o el salto siguiente. Para ello, utilice el comando `show arp`.

```

OneArm-LoadBalancer-01-0> show arp
-----
vShield Edge ARP Cache:
IP Address                Interface  MAC Address      State
fe80::250:56ff:feae:f86b  vNic_0    00:50:56:ae:f8:6b STALE
fe80::250:56ff:feae:5066  vNic_1    00:50:56:ae:50:66 STALE
fe80::250:56ff:feae:3e3d  vNic_0    00:50:56:ae:3e:3d STALE
172.16.100.11             vNic_1    00:50:56:ae:50:66 REACHABLE
172.16.10.1               vNic_0    02:50:56:56:44:52 REACHABLE
172.16.10.11             vNic_0    00:50:56:ae:3e:3d REACHABLE
OneArm-LoadBalancer-01-0>

```

- 8 Los registros proporcionan información para localizar el tráfico, lo cual puede resultar útil a la hora de diagnosticar problemas. Utilice los comandos `show log` o `show log follow` para seguir los registros que pueden ayudarle a ubicar el tráfico. Tenga en cuenta que, para ejecutar el equilibrador de carga, debe habilitar la opción **Registros** (Logging) y seleccionar **Información** (Info) o **Depuración** (Debug).

```

nsxedge> show log
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuacct
...

```

- 9 Después de verificar que los servicios básicos se están ejecutando con las rutas adecuadas a los clientes, debe saber lo que sucede en la capa de la aplicación. Utilice el comando `show service loadbalancer pool` para consultar el estado del grupo del equilibrador de cara (Capa 4 o Capa 7). Al menos un miembro del grupo debe estar activo para publicar contenido. Normalmente, se necesitan más porque el volumen de solicitudes supera la capacidad de carga de trabajo de uno. Si el estado del monitor lo proporciona la comprobación de estado integrada, el resultado muestra la hora del último cambio de estado (last state change time) y el motivo del error (failure reason) cuando falla la comprobación de estado. Si procede del servicio de supervisión, además de los dos resultados anteriores, se muestra la hora de la última comprobación (last check time).

```
nsxedge> show service loadbalancer pool
-----
Loadbalancer Pool Statistics:

POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
```

- 10 Consulte el estado de supervisión del servicio, que puede ser CORRECTO (OK) , ADVERTENCIA (WARNING) o CRÍTICO (CRITICAL), para conocer el estado de todos los servidores backend configurados.

```
nsxedge> show service loadbalancer monitor
-----
Loadbalancer Health Check Statistics:

MONITOR PROVIDER    POOL            MEMBER          HEALTH STATUS
built-in            Web-Tier-Pool-01 web-01a          default_https_monitor:L7OK
built-in            Web-Tier-Pool-01 web-02a          default_https_monitor:L7OK
```

Para el comando `show service load balancer monitor`, aparecen tres tipos de valores de supervisión de estado en la salida de la CLI:

- Integrado (Built-in): la comprobación de estado está habilitada y la realiza un motor de Capa 7 (proxy de HA).

- Servicio de supervisión (Monitor Service): la comprobación de estado está habilitada y la realiza un motor de servicio de supervisión (NAGIOS). Los comandos de la CLI `show service monitor` y `show service monitor service` pueden comprobar el estado de ejecución del servicio de supervisión. El campo **Estado** (Status) debe aparecer como CORRECTO (OK), ADVERTENCIA (WARNING) o CRÍTICO (CRITICAL).
- Sin definir (Not Defined): la comprobación de estado está deshabilitada.

La última columna de resultados se corresponde con el estado del miembro del grupo. Se muestran los siguientes estados:

Tabla 6-1. Estado y descripción

Estado	Descripción
Integrado (Built-in)	<ul style="list-style-type: none"> ■ UNK: desconocido ■ INI: inicializando ■ SOCKERR: error de socket ■ L4OK: comprobación de la capa 4 correcta, pero no están habilitadas las pruebas de capas superiores ■ L4TOUT: tiempo de espera de las capas 1 a la 4 ■ L4CON: problema de conexión de las capas 1 a la 4. Por ejemplo, "Conexión rechazada" (Connection refused), tcp rst, o "Sin ruta al host" (No route to host), icmp ■ L6OK: comprobación de la capa 6 correcta ■ L6TOUT: tiempo de espera de la capa 6 (SSL) ■ L6RSP: respuesta no válida de la capa 6: error de protocolo. Se pudo provocar ya que: <ul style="list-style-type: none"> ■ El servidor backend solo admite "SSLv3" o "TLSv1.0", ■ El certificado del servidor backend no es válido, o bien ■ Se produjo un error en la negociación del cifrado, etc. ■ L7OK: comprobación de la capa 7 correcta ■ L7OKC: comprobación de la capa 7 correcta de forma condicional. Por ejemplo, 404 con la opción deshabilitar-en-404 (disable-on-404) ■ L7TOUT: tiempo de espera de la capa 7 (HTTP/SMTP) ■ L7RSP: respuesta no válida de la capa 7: error de protocolo ■ L7STS: error de respuesta de la capa 7. Por ejemplo, HTTP 5xx
CRÍTICO (CRITICAL)	<ul style="list-style-type: none"> ■ La biblioteca SSL no admite la versión 2 del protocolo SSL ■ Versión del protocolo SSL no admitida ■ No se puede crear el contexto SSL ■ No se puede establecer la conexión SSL ■ No se puede iniciar el protocolo de enlace SSL ■ No se puede recuperar el certificado del servidor ■ No se puede recuperar el sujeto del certificado ■ Formato de hora incorrecto en el certificado ■ El certificado "<cn>" caducó el <fecha en la que caducó el certificado> ■ El certificado "<cn>" caducó hoy <fecha en la que caducó el certificado>
ADVERTENCIA/ CRÍTICO (WARNING/ CRITICAL)	El certificado "<cn>" caducará en <días_restantes/fecha en la que caducará el certificado> días

Tabla 6-1. Estado y descripción (continuación)

Estado	Descripción
ICMP	<ul style="list-style-type: none"> ■ Red no accesible ■ Host no accesible ■ Protocolo no accesible ■ Puerto no accesible ■ Error en la ruta de origen ■ Host de origen aislado ■ Red desconocida ■ Host desconocido ■ Red denegada ■ Host denegado ■ Tipo de servicio (ToS) incorrecto para la red ■ Tipo de servicio (ToS) incorrecto para el host ■ Prohibido por el filtro ■ Infracción de la prioridad de host ■ Límite de prioridad. La operación requiere el nivel mínimo de prioridad ■ Código no válido
UDP/TCP	<ul style="list-style-type: none"> ■ Error al crear el socket ■ Conectar a la dirección xxxx y al puerto xxx: [consulte el código de error de Linux] ■ No se recibió ningún dato del host ■ Respuesta inesperada del host/socket
HTTP/HTTPS	<ul style="list-style-type: none"> ■ HTTP DESCONOCIDO: error de asignación de memoria ■ HTTP CRÍTICO: no se puede abrir el socket TCP (error al crear el socket o al conectarse al servidor) ■ HTTP CRÍTICO: error al recibir datos ■ HTTP CRÍTICO: no se recibió ningún dato del host ■ HTTP CRÍTICO: se recibió una respuesta HTTP no válida desde el host: <línea de estado> (formato incorrecto de la línea de estado) ■ HTTP CRÍTICO: línea de estado no válida <línea de estado> (el código de estado no está compuesto por 3 dígitos: XXX) ■ HTTP CRÍTICO: estado no válido <línea de estado> (el código de estado es 600 o un valor superior, o bien menor a 100) ■ HTTP CRÍTICO: no se encuentra la cadena ■ HTTP CRÍTICO: no se encuentra el patrón ■ ADVERTENCIA DE HTTP: el tamaño <longitud_página> de la página es demasiado grande ■ ADVERTENCIA DE HTTP: el tamaño <longitud_página> de la página es demasiado pequeño

- 11 Si el código de error es L4TOUT/L4CON, normalmente se corresponde con problemas de conectividad en las redes subyacentes. Duplicate IP suele suceder como causa principal por dicha razón. Cuando se produce este error, solucione el problema de la siguiente manera:
 - a Consulte el estado Alta disponibilidad (High Availability, HA) de los Edge cuando se habilite la alta disponibilidad. Para ello, utilice el comando `show service highavailability` en ambos Edge. Compruebe si el vínculo de HA está INACTIVO (DOWN) y todos los Edge están Active para que no haya IP de Edge duplicadas en la red.
 - b Consulte la tabla ARP de Edge con el comando `show arp` y verifique si la entrada ARP del servidor backend cambia entre las dos direcciones MAC.
 - c Consulte la tabla ARP del servidor backend o utilice el comando `arp-ping` y compruebe si la IP de otro equipo es la misma que la IP de Edge.
- 12 Compruebe las estadísticas de los objetos del equilibrador de carga (VIPs, grupos o miembros). Consulte el grupo específico y verifique que los miembros estén activos y ejecutándose. Compruebe si el modo transparente está habilitado. Si es así, la puerta de enlace de servicios de Edge debe estar en línea entre el cliente y el servidor. Verifique si los servidores muestran incrementos en el contador de sesiones.

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01
```

TIMESTAMP	SESSIONS	BYTESIN	BYTESOUT	SESSIONRATE	HTTPREQS
2016-04-27 19:56:40	00	00	00	00	00
2016-04-27 19:55:00	00	32	100	00	00

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01 | MEMBER
+--> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-1, STATUS: UP
+--> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-2, STATUS: UP
```

- 13 Consulte ahora el servidor virtual, verifique si hay un grupo predeterminado y compruebe si el grupo está enlazado al servidor. Si utiliza los grupos a través de reglas de aplicaciones, debe consultar los grupos específicos que se muestran en el comando `#show service loadbalancer pool`. Especifique el nombre del servidor virtual.

```
nsxedge> show service loadbalancer virtual Web-Tier-VIP-01
```

Loadbalancer VirtualServer Statistics:

```
VIRTUAL Web-Tier-VIP-01
| ADDRESS [172.16.10.10]:443
| SESSION (cur, max, total) = (0, 0, 0)
| RATE (cur, max, limit) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
```

```

| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)

```

- 14** Si parece que todo está configurado correctamente y sigue apareciendo un error, debe capturar el tráfico para comprender lo que ocurre. Hay dos conexiones: la del cliente con el servidor virtual y la de la puerta de enlace de servicios de Edge con el grupo backend (con o sin configuración transparente en el grupo). El comando `#show ip forwarding` enumera las interfaces de vNic. Utilice esos datos.

Por ejemplo, suponga que el equipo cliente utiliza la interfaz `vNic_0` y el servidor usa la `vNic_1`. En ese caso, use una IP del cliente `192.168.1.2` y una IP VIP `192.168.2.2` en el puerto 80. La interfaz del equilibrador de carga tendrá la IP `192.168.3.1` y la IP del servidor backend será `192.168.3.3`. Hay dos comandos de captura de paquetes distintos. Uno muestra los paquetes, mientras que el otro los captura en archivos que se pueden descargar. Capture los paquetes para detectar errores del equilibrador de carga que no sean normales. Puede hacerlo desde dos direcciones:

- Capture los paquetes desde el cliente.
- Capture los paquetes enviados al servidor backend.

```

#debug packet capture interface interface-name [filter using _ for space]- creates a packet
capture file that you can download
#debug packet display interface interface-name [filter using _ for space]- outputs packet data to
the console
#debug show files - to see a list of packet capture
#debug copy scp user@url:path file-name/all - to download the packet capture

```

Por ejemplo:

- Captura en vNIC_0: `debug packet display interface vNic_0`
- Captura en todas las interfaces: `debug packet display interface any`
- Captura en vNIC_0 con un filtro: `debug packet display interface vNic_0 host_192.168.11.3_and_host_192.168.11.41`
- Una captura de paquetes del cliente para el tráfico del servidor virtual: `#debug packet display|capture interface vNic_0 host_192.168.1.2_and_host_192.168.2.2_and_port_80`
- Una captura de paquetes entre la puerta de enlace de servicios de Edge y el servidor en la que el grupo está en modo transparente: `#debug packet display|capture interface vNic_1 host 192.168.1.2_and_host_192.168.3.3_and_port_80`

- Una captura de paquetes entre la puerta de enlace de servicios de Edge y el servidor en la que el grupo no está en modo transparente: `#debug packet display|capture interface vNic_1 host 192.168.3.1_and_host_192.168.3.3_and_port_80`

Problemas frecuentes del equilibrador de carga

En esta sección se incluyen varios problemas y sus soluciones.

Los siguientes problemas son frecuentes al utilizar el equilibrio de carga de NSX:

- No funciona el equilibrio de carga en el puerto TCP (por ejemplo, el puerto 443).
 - Verifique la topología. Para obtener más información, consulte la *Guía de administración de NSX*.
 - Verifique que se pueda acceder a la dirección IP del servidor virtual haciendo ping o consulte el enrutador ascendente para comprobar que la tabla ARP está rellena.
 - [Verificación de configuración del equilibrador de carga y solución de problemas a través de la interfaz de usuario.](#)
 - [Resolución de problemas del equilibrador de carga a través de la CLI.](#)
 - Capture los paquetes.
- No se utilizó ningún miembro del grupo del equilibrio de carga.
 - Verifique que el servidor se encuentre en el grupo y esté habilitado y supervise su estado.
- El tráfico de Edge no tiene la carga equilibrada.
 - Verifique la configuración de la persistencia y el grupo. Si configuró la persistencia y utiliza un pequeño número de clientes, es posible que no observe una distribución uniforme de conexiones a los miembros del grupo backend.
- El motor del equilibrador de carga de Capa 7 se detuvo.
- El motor del monitor de estado se detuvo.
 - Habilite el servicio del equilibrador de carga. Consulte la *Guía de administración de NSX*.
- El estado del monitor de miembros del grupo es ADVERTENCIA/CRÍTICO (WARNING/CRITICAL).
 - Compruebe que se pueda acceder al servidor de la aplicación desde el equilibrador de carga.
 - Compruebe que el DFW o el firewall del servidor de la aplicación permita el tráfico.
 - Asegúrese de que el servidor de la aplicación puede responder al sondeo de estado.
- El miembro del grupo tiene el estado INACTIVO (INACTIVE).
 - Compruebe que el miembro del grupo esté habilitado en la configuración del grupo.
- La tabla estática de Capa 7 no está sincronizada con una instancia Edge en espera.
 - Compruebe que HA esté configurado.

- El cliente se puede conectar, pero no puede completar una transacción de aplicación.
 - Compruebe que se haya configurado la persistencia adecuada en el perfil de la aplicación.
 - Si la aplicación funciona únicamente con un servidor del grupo (en lugar de dos), es probable que se trate de un problema de persistencia.

Pasos básicos para solucionar problemas

- 1 Compruebe el estado de configuración del equilibrador de carga en vSphere Web Client:
 - a Haga clic en **Redes y seguridad > Instancias de NSX Edge** (Networking & Security > NSX Edges).
 - b Haga doble clic en un dispositivo NSX Edge.
 - c Haga clic en **Administrar** (Manage) y seleccione la pestaña **Equilibrador de carga** (Load Balancer).
 - d Compruebe el estado del equilibrador de carga y el nivel de inicio de sesión configurado.
- 2 Antes de solucionar los problemas relacionados con el servicio del equilibrador de carga, ejecute el siguiente comando en NSX Manager para garantizar que el servicio esté disponible y en ejecución:

```
nsxmgr> show edge edge-4 service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer      : running
-----
L7 Loadbalancer Statistics:
STATUS      PID      MAX_MEM_MB  MAX SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running     1580      0           2081       1024        0           0           0
0           0
-----
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN  TOTAL_CONN
0           0           0           0
-----
Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port      Forward Weight ActiveConn InActConn
```

Nota Puede ejecutar el comando `show edge all` para buscar los nombres de las instancias de NSX Edge.

Solucionar problemas relacionados con la configuración

Si la llamada de REST API o la interfaz de usuario de NSX rechazan la operación de configuración del equilibrador de carga, esto suele clasificarse como un problema de configuración.

Solucionar problemas relacionados con el plano de datos

NSX Manager acepta la configuración del equilibrador de carga, pero hay problemas relacionados con el rendimiento o la conectividad en el servidor del equilibrador de carga de Edge de cliente. Los problemas relacionados con el plano de datos también incluyen los problemas de la CLI del tiempo de ejecución del equilibrador de carga y los problemas del evento del sistema del equilibrador de carga.

- 1 Cambie el nivel de inicio de sesión de NSX Manager de INFO a TRACE o DEBUG utilizando esta llamada de REST API.

```
URL: https://NSX_Manager_IP/api/1.0/services/debug/loglevel/com.vmware.vshield.edge?level=TRACE
Method: POST
```

- 2 Compruebe el estado del miembro del grupo en vSphere Web Client.
 - a Haga clic en **Redes y seguridad > Instancias de NSX Edge** (Networking & Security > NSX Edges).
 - b Haga doble clic en un dispositivo NSX Edge.
 - c Haga clic en **Administrar** (Manage) y seleccione la pestaña **Equilibrador de carga** (Load Balancer).
 - d Haga clic en **Pools** (Grupos) para ver un resumen de los grupos del equilibrador de carga configurados.
 - e Seleccione su grupo del equilibrador de carga. Haga clic en **Mostrar estadísticas de grupo** (Show Pool Statistics) y compruebe que el estado del grupo sea ACTIVO (UP).
- 3 Puede obtener estadísticas más detalladas de la configuración del grupo del equilibrador de carga en NSX Manager. Para ello, utilice esta llamada de REST API:

```
URL: https://NSX_Manager_IP/api/4.0/edges/{edgeId}/loadbalancer/statistics
Method: GET
```

```
<?xml version="1.0" encoding="UTF-8"?>
<loadBalancerStatusAndStats>
  <timeStamp>1463507779</timeStamp>
  <pool>
    <poolId>pool-1</poolId>
    <name>Web-Tier-Pool-01</name>
    <member>
      <memberId>member-1</memberId>
      <name>web-01a</name>
      <ipAddress>172.16.10.11</ipAddress>
      <status>UP</status>
      <lastStateChangeTime>2016-05-16 07:02:00</lastStateChangeTime>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <httpReqTotal>0</httpReqTotal>
      <httpReqRate>0</httpReqRate>
```

```

        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <member>
        <memberId>member-2</memberId>
        <name>web-02a</name>
        <ipAddress>172.16.10.12</ipAddress>
        <status>UP</status>
        <lastStateChangeTime>2016-05-16 07:02:01</lastStateChangeTime>
        <bytesIn>0</bytesIn>
        <bytesOut>0</bytesOut>
        <curSessions>0</curSessions>
        <httpReqTotal>0</httpReqTotal>
        <httpReqRate>0</httpReqRate>
        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <status>UP</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</pool>
<virtualServer>
    <virtualServerId>virtualServer-1</virtualServerId>
    <name>Web-Tier-VIP-01</name>
    <ipAddress>172.16.10.10</ipAddress>
    <status>OPEN</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>

```

```
<rateMax>0</rateMax>  
<totalSessions>0</totalSessions>  
</virtualServer>  
</loadBalancerStatusAndStats>
```

- 4 Para comprobar las estadísticas del equilibrador de carga desde la línea de comandos, ejecute estos comandos en NSX Edge.

En un servidor virtual concreto: ejecute el comando `show service loadbalancer virtual` para obtener el nombre del servidor virtual. A continuación, ejecute el comando `show statistics loadbalancer virtual <virtual-server-name>`.

En un grupo de TCP concreto: ejecute el comando `show service loadbalancer pool` para obtener el nombre de la máquina virtual. A continuación, ejecute el comando `show statistics loadbalancer pool <pool-name>`.

- 5 Compruebe si existen signos de error en las estadísticas del equilibrador de carga.

Resolución de problemas de redes privadas virtuales (VPN)

7

NSX Edge admite varios tipos de VPN. Esta sección de solución de problemas indica cómo solucionar problemas relacionados con la SSL VPN y la VPN de Capa 2.

Este capítulo incluye los siguientes temas:

- [VPN de Capa 2](#)
- [SSL VPN](#)
- [IPsec VPN](#)

VPN de Capa 2

La VPN de Capa 2 permite ampliar varias redes lógicas de Capa 2 (VLAN y VXLAN) a los límites de Capa 3, que hacen de túnel dentro de SSL VPN. Además, puede configurar varios sitios en un servidor VPN de Capa 2. Las máquinas virtuales permanecen en la misma subred cuando se las traslada de un sitio a otro y sus direcciones IP no cambian. También puede implementar un Edge independiente en un sitio remoto sin que el sitio tenga "NSX habilitado" (NSX Enabled). La optimización del egreso permite a Edge enrutar cualquier paquete enviado hacia la dirección IP de optimización de egreso de forma local y conectar todo lo demás con un puente.

Por lo tanto, la VPN de Capa 2 permite a las empresas migrar sin problemas las cargas de trabajo respaldadas por VXLAN o VLAN entre ubicaciones separadas físicamente. 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 de las cargas de trabajo y las aplicaciones.

Problemas frecuentes relacionados con la configuración de la VPN de Capa 2

En este tema se analizan problemas de configuración comunes relacionados con la VPN de Capa 2.

Problema

A continuación se incluyen los problemas frecuentes de configuración:

- El cliente de VPN de Capa 2 está configurado, pero el firewall de Internet no permite el flujo de tráfico por el túnel a través del puerto de destino 443.

- El cliente de VPN de Capa 2 está configurado para validar el certificado del servidor, pero no con el FQDN o certificado de entidad de certificación correctos.
- El servidor de VPN de Capa 2 está configurado, pero no se creó la regla de firewall o NAT en el firewall de Internet.
- La interfaz de enlace troncal no está respaldada por un grupo de puertos estándar o distribuidos.

Nota El servidor de VPN de Capa 2 escucha en el puerto 443 de forma predeterminada. Este puerto se puede configurar desde los ajustes del servidor de VPN de Capa 2.

El cliente de VPN de Capa 2 realiza una conexión saliente con el puerto 443 de forma predeterminada. Este puerto se puede configurar en los ajustes del cliente de VPN de Capa 2.

Solución

- 1 Compruebe si se está ejecutando el proceso del servidor de VPN de Capa 2.
 - a Inicie sesión en la máquina virtual de NSX Edge.
 - b Ejecute el comando `show process monitor` y verifique que aparezca un proceso con el nombre *l2vpn*.
 - c Ejecute el comando `show service network-connections` y verifique si el proceso *l2vpn* realiza la escucha en el puerto 443.
- 2 Compruebe si se está ejecutando el proceso del cliente de VPN de Capa 2.
 - a Inicie sesión en la máquina virtual de NSX Edge.
 - b Ejecute el comando `show process monitor` y verifique que aparezca un proceso con el nombre *naclientd*.
 - c Ejecute el comando `show service network-connections` y verifique si el proceso *naclientd* realiza la escucha en el puerto 443.
- 3 Compruebe si se puede acceder al servidor de VPN de Capa 2 desde Internet.
 - a Abra el navegador y acceda a la página **`https://<l2vpn-public-ip>`**.
 - b Debería aparecer una página de inicio de sesión del portal. Si es así, significa que se puede acceder al servidor de VPN de Capa 2 a través de Internet.
- 4 Compruebe si la interfaz de enlace troncal cuenta con un grupo de puertos estándar o distribuidos.
 - a Si cuenta con un grupo de puertos distribuidos, se configurará automáticamente un puerto de recepción.
 - b Si cuenta con un grupo de puertos estándar, deberá configurar manualmente el conmutador distribuido de vSphere de la siguiente forma:
 - Defina el modo **promiscuo** para el puerto.
 - Seleccione **Aceptar** (Accept) en **Transmisiones falsificadas** (Forged Transmits).

5 Mitigue el problema relacionado con los bucles de la VPN de Capa 2.

- a Se observan dos problemas principales si la formación de equipos de NIC no se configura correctamente: cambio de MAC y paquetes duplicados. Verifique que la configuración se corresponda con lo descrito en [Opciones de VPN de Capa 2 para mitigar los bucles](#).

6 Compruebe si las máquinas virtuales de la VPN de Capa 2 pueden comunicarse entre sí.

- a Inicie sesión en la CLI del servidor de VPN de Capa 2 y capture el paquete en la interfaz TAP debug packet capture interface name correspondiente.
- b Inicie sesión en la CLI del cliente de VPN de Capa 2 y capture el paquete en la interfaz TAP debug packet capture interface name correspondiente.
- c Analice estas capturas para comprobar el flujo del tráfico de datos y si se solucionan los problemas de ARP.
- d Compruebe si la propiedad Allow Forged Transmits: dvSwitch está definida como *puerto de enlace de la VPN de Capa 2*.
- e Compruebe si el puerto de recepción está definido como *puerto de enlace de la VPN de Capa 2*. Para ello, inicie sesión en el host y ejecute el comando `net-dvs -l`. Busque la propiedad de recepción definida como puerto interno de Edge de la VPN de Capa 2 (`com.vmware.etherSwitch.port.extraEthFRP = SINK`). El puerto interno se refiere al puerto *dvPort* al que está conectado el enlace de NSX Edge.

net-dvs -l

ESXi

```
port 939:
com.vmware.common.port.alias = , propType = CONFIG
com.vmware.common.port.connectid = 323234212 , propType = CONFIG
com.vmware.common.port.portgroupid = dvportgroup-181 , propType = CONFIG
com.vmware.common.port.block = false , propType = CONFIG
com.vmware.common.port.dvfilter = filters (num = 0):
propType = CONFIG
com.vmware.common.port.ptAllowed = 0x 0. 0. 0. 0
propType = CONFIG
com.vmware.etherSwitch.port.txUplink = normal , propType = CONFIG
com.vmware.common.port.volatile.persist = /vmfs/volumes/9ec6ae8b-38b8e621/.dvsData/1e ec 0e 50 02 9c a9 21-b6 d8
fc 73 e5 79 69/939 , propType = CONFIG
com.vmware.common.port.ptAllowedRT = 0x 0. 0. 0. 0
propType = RUNTIME
com.vmware.net.vxlan.trunkcfg = 0x63.6f.6e.66.69.67.56.65.72.73.69.6f.6e.3d.30.2e.31.3b.61.6c.6c.6f.77.47.75.65.7
74.56.6c.61.6e.3d.30.3b.6e.75.6d.54.72.75.6e.6b.4d.65.6d.62.65.72.73.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.43.70.45.6e.61.62.
.65.64.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.56.6e.69.3d.35.30.30.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.4d.63.61.73.74.49.70
d.30.2e.30.2e.30.2e.31.3b
propType = CONFIG POLICY
com.vmware.etherSwitch.port.extraEthFRP = SINK
propType = CONFIG POLICY
com.vmware.etherSwitch.port.teaming:
load balancing = first uplink (i.e. explicit)
link selection = link state up;
link behavior = notify switch; best effort on failure; shotgun on failure;
active = dvUplink1;
standby =
propType = CONFIG
com.vmware.etherSwitch.port.security = deny promiscuous; deny mac change; allow forged frames
propType = CONFIG
com.vmware.etherSwitch.port.vlan = Guest VLAN tagging
ranges = 0
propType = CONFIG
com.vmware.common.port.statistics:
pktsInUnicast = 0
bytesInUnicast = 0
pktsInMulticast = 6
bytesInMulticast = 620
```

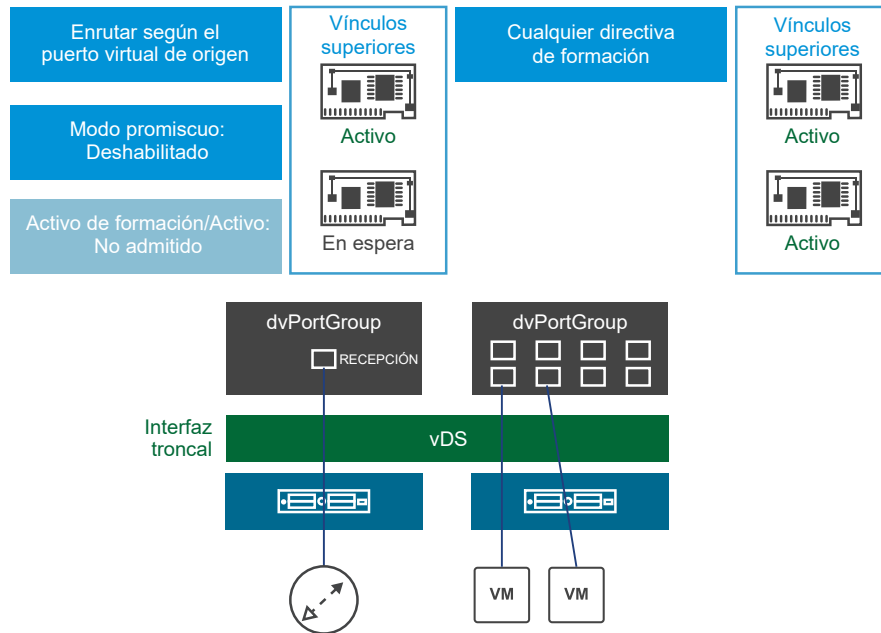
Sink port should be enabled for the dvPort where the Edge trunk is connected to

Opciones de VPN de Capa 2 para mitigar los bucles

Existen dos opciones para mitigar los bucles. Las instancias de NSX Edge y las máquinas virtuales pueden estar en hosts ESXi diferentes o en el mismo host ESXi.

Opción 1: separar los hosts ESXi para las instancias de Edge de VPN de Capa 2 y las máquinas virtuales

1. Implementar VM y edges L2VPN en hosts ESXi independientes



1. Implemente las instancias de Edge y las máquinas virtuales en hosts ESXi distintos.
2. Configure la directiva de formación de equipos y conmutación por error para el grupo de puertos distribuidos asociado con la vNic troncal de Edge de la siguiente forma:
 - a. Establezca el equilibrio de carga en "Enrutar según el puerto virtual de origen" (Route Based on originating virtual port).
 - b. Configure solo un vínculo superior como Activo (Active) y el otro como En espera (Standby).
3. Configure la directiva de formación de equipos y conmutación por error para el grupo de puertos distribuidos asociado con las máquinas virtuales de la siguiente forma:
 - a. Cualquier directiva de formación de equipos está bien.
 - b. Es posible configurar varios vínculos superiores.

- 4 Configure las instancias de Edge para que utilicen el modo de puerto de recepción y deshabilite el modo promiscuo en la vNic troncal.

Nota

- Deshabilite el modo promiscuo: si usa vSphere Distributed Switch.
- Habilite el modo promiscuo: si usa un conmutador virtual para configurar la interfaz de enlace troncal.

Si un conmutador virtual tiene habilitado el modo promiscuo, algunos de los paquetes procedentes de los vínculos superiores que no esté usando el puerto promiscuo en ese momento no se descartarán. Debe habilitar y, a continuación, deshabilitar `ReversePathFwdCheckPromisc`, lo que descartará explícitamente en el puerto promiscuo todos los paquetes procedentes de los vínculos superiores que no se estén usando en ese momento.

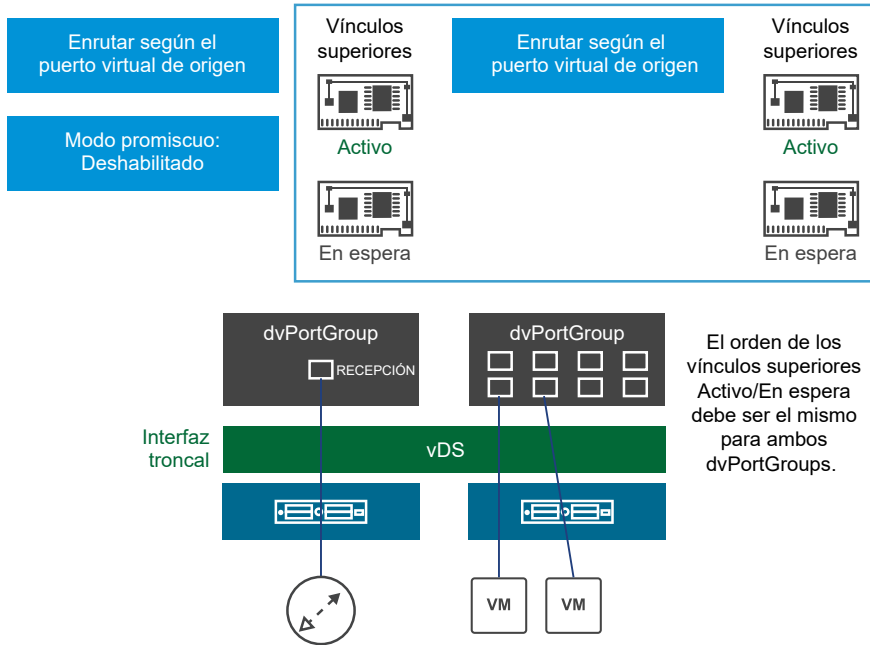
Para bloquear los paquetes duplicados, active la comprobación de RPF para el modo promiscuo desde la CLI de ESXi donde se encuentra NSX Edge:

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to
Promiscuous mode.
```

En la directiva de seguridad de **PortGroup**, cambie **Modo promiscuo** (PromiscuousMode) de **Aceptar** (Accept) a **Rechazar** (Reject) y vuelva a establecer **Aceptar** (Accept) para activar el cambio configurado.

- Opción 2: instancias de Edge y máquinas virtuales en el mismo host ESXi

2. Implementar VM y edges L2VPN en el mismo host



- a Configure la directiva de formación de equipos y conmutación por error para el grupo de puertos distribuidos asociado con la vNic troncal de Edge de la siguiente forma:
 - 1 Establezca el equilibrio de carga en "Enrutar según el puerto virtual de origen" (Route Based on originating virtual port).
 - 2 Configure solo un vínculo superior como activo y el otro como en espera.
- b Configure la directiva de formación de equipos y conmutación por error para el grupo de puertos distribuidos asociado con las máquinas virtuales de la siguiente forma:
 - 1 Cualquier directiva de formación de equipos está bien.
 - 2 Solo puede haber un vínculo superior activo.
 - 3 El orden de los vínculos superiores activo/en espera debe ser igual en el grupo de puertos distribuidos de las máquinas virtuales y el grupo de puertos distribuidos de la vNic troncal de Edge.
- c Configure la instancia de Edge independiente del lado del cliente para que utilice el modo de puerto de recepción y deshabilite el modo promiscuo en la vNic troncal.

Solución de problemas a través de la CLI

Puede utilizar la interfaz de línea de comandos (CLI) de NSX para solucionar problemas relacionados con la VPN de Capa 2.

Problema

La VPN de Capa 2 no funciona según lo esperado.

Solución

- 1 Utilice el siguiente comando de la CLI central para consultar los problemas de configuración:

`show edge <edgeID> configuration l2vpn.`

Por ejemplo, `show edge edge-1 configuration l2vpn.`

- 2 Utilice los siguientes comandos tanto en Edge de cliente como de servidor:

- `show configuration l2vpn`: compruebe estos cuatro valores de clave para verificar el servidor.

```

show configuration l2vpn

vShield Edge L2 VPN Config:
{
  "l2vpn" : {
    "cipher" : {
      "RC4-MD5"
    },
    "listenerPort" : 443,
    "clientVnicIndex" : null,
    "filters" : [],
    "serverPort" : null,
    "caCertificate" : null,
    "assumptionAlgorithm" : null,
    "listenerIp" : "192.168.100.3",
    "peerSites" : [
      {
        "vseVnicNames" : [
          "vNic_10"
        ],
        "name" : "L2VPN-Site1",
        "filters" : [],
        "l2vpnUser" : {
          "password" : "*****",
          "userId" : "vpnuser1"
        }
      }
    ],
    "clientProxySetting" : null,
    "enable" : true,
    "trunkedVnicIndexes" : [
      2
    ],
    "serverVnicIndex" : null,
    "l2vpnUsers" : [],
    "serverAddress" : null,
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "vseVnicNames" : null,
    "serverCertificate" : null
  }
}
  
```

- `show service l2vpn bridge`: el número de interfaces depende del número de clientes de VPN de Capa2. En el resultado que se muestra a continuación, hay un único cliente de VPN de Capa 2 (na1) configurado. Puerto 1 (Port1) se refiere a `vNic_2`. La dirección MAC 02:50:56:56:44:52 procede de la interfaz `vNic_2` y no es local de Edge (servidor de VPN de Capa 2). La fila 3 del siguiente ejemplo se refiere a la interfaz `na1`.

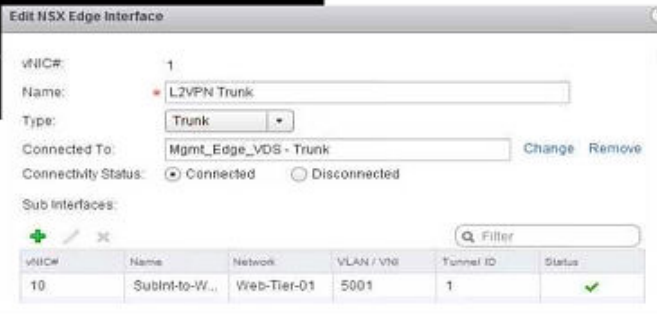
```
plr01-0> show service l2vpn bridge

bridge name      bridge id          STP enabled      interfaces
br-sub           8000.0050568e19fb  no               vNic_2
                                                         na1

List of learned MAC addresses for L2 VPN bridge br-sub
-----
port no mac addr          is local?      vlanid      ageing timer
1      00:50:56:8e:19:fb      yes            0            0.00
1      02:50:56:56:44:52      no             1            0.87
2      2a:56:30:31:7e:3b      yes            0            0.00
```

- show service l2vpn trunk table
- show service l2vpn conversion table: en el siguiente ejemplo, un marco de Ethernet procedente del túnel #1 convertirá su ID de VLAN #1 a VXLAN con el número de VLAN 5001 antes de que el paquete se transfiera a VDS.

```
plr01-0> show service l2vpn conversion-table
TunnelId  VLAN/VNI  Type
-----
1          5001     VXLAN
```



vNIC#	Name	Network	VLAN / VNI	Tunnel ID	Status
10	Subint-to-W...	Web-Tier-01	5001	1	✓

- show process monitor: identifique si se están ejecutando los procesos l2vpn (servidor) y naclntd (cliente).
- show service network-connections: compruebe si los procesos l2vpn (servidor) y naclntd (cliente) realizan la escucha en el puerto 443.

SSL VPN

Puede utilizar esta información para solucionar problemas en la configuración.

El portal web SSL VPN no se abre

Los usuarios de SSL VPN no pueden abrir la página de inicio de sesión del portal web SSL VPN y utilizar el paquete de instalación del cliente SSL VPN-Plus.

Problema

La página de inicio de sesión del portal web SSL VPN no se abre o la página no aparece correctamente en el navegador del sistema.

Causa

Este problema puede deberse a uno de los siguientes motivos:

- Su sistema utiliza una versión de explorador no admitida.
- Las cookies y JavaScript no están habilitadas en el explorador.

Solución

- 1 Asegúrese de que utiliza uno de los siguientes navegadores admitidos para abrir la página de inicio de sesión del portal web SSL VPN.

Explorador	Versiones mínimas admitidas
Internet Explorer	9.0.8112.16421
Chrome	67.03396
Safari	10.x

- 2 Abra la configuración del navegador y asegúrese de que las cookies y JavaScript están habilitados.
- 3 Si el idioma establecido en el navegador no es inglés, establézcalo y compruebe si el problema persiste.
- 4 Compruebe si seleccionó el cifrado AES en el servidor SSL VPN. Algunos navegadores no admiten el cifrado AES.

SSL VPN-Plus: errores de instalación

Utilice este tema para comprender los posibles problemas de instalación específicos del cliente SSL VPN-Plus, y para saber cómo puede solucionarlos.

Problema

A continuación, aparecen problemas comunes asociados a la instalación del cliente SSL VPN-Plus:

- El cliente SSL VPN-Plus se instaló correctamente, pero no funciona.
- En las máquinas Mac, aparecen mensajes de advertencia sobre extensión del kernel.
- En Mac OS High Sierra, aparecen los siguientes mensajes de error de instalación:

```
/opt/sslvpn-plus/naclient/signed_kext/tap.kext failed to load - (libkern/kext)system policy prevents loading; check the system/kernel logs for errors or try kextutil(8).
Error: Could not load /opt/sslvpn-plus/naclient/signed_kext/tap.kext
```

```
installer[4571] <Debug>: install:didFailWithError:Error Domain=
PKInstallErrorDomain Code=112 "An error occurred while running scripts from the package
"naclient.pkg".
" UserInfo={NSFilePath=./postinstall,NSURL=file:///<pathtofile>/
naclient.pkg,PKInstallPackageIdentifier=
com.vmware.sslvpn,NSLocalizedString=An error occurred while running scripts from the
package "naclient.pkg".}
```

```
installer[4571] <Error>: Install failed: The Installer encountered an error that caused the
installation to fail. Contact the software manufacturer for assistance.
installer: The install failed (The Installer encountered an error that caused the installation to
fail.
Contact the software manufacturer for assistance.)
```

- En las máquinas Windows aparece el siguiente mensaje de error: No se pudo instalar el controlador por el motivo E000024B. Por favor, pruebe a reiniciar la máquina (Driver installation failed for reason E000024B:Please try rebooting the machine).

Causa

Una de las siguientes razones puede provocar un error en el cliente SSL VPN-Plus, aunque se instalara correctamente en su equipo.

- Falta el archivo de configuración (naclient.cfg) o no es válido.
- Los permisos de directorio o de usuario son incorrectos.
- No se puede acceder al servidor SSL VPN.
- En las máquinas Linux y Mac, el controlador TAP no está cargado.

En las máquinas Mac, aparecen mensajes de advertencia de extensión del kernel porque su sistema bloquea la carga de dicha extensión.

En Mac OS High Sierra, los errores de instalación aparecen si la máquina Mac no admite kext ni le solicita que cargue el kext.

En las máquinas Windows, aparece el error (E000024B) de instalación del controlador porque habilitó la opción **Ocultar el adaptador de red cliente SSL** (Hide SSL client network adapter) en el instalador SSL VPN-Plus cliente de Edge.

Solución

- 1 Asegúrese de instalar el cliente SSL VPN-Plus en sistemas operativos admitidos. Para obtener más información sobre los sistemas operativos admitidos, consulte el tema Descripción general de SSL VPN-Plus en *Guía de administración de NSX*.
- 2 En las máquinas Windows, compruebe que los usuarios que instalen el cliente SSL VPN-Plus tengan privilegios de **administrador**. En las máquinas Linux y Mac, los usuarios deben tener privilegios **raíz** para instalar el cliente SSL VPN-Plus. Además, para que el cliente SSL VPN-Plus se inicie y se ejecute correctamente en máquinas Mac, los usuarios deben tener permisos de **ejecución** en el directorio `usr/local/lib`.
- 3 En las máquinas Linux, compruebe que las siguientes bibliotecas estén instaladas. Estas bibliotecas son obligatorias para que funcione la interfaz de usuario.
 - TCL
 - TK
 - NSS

- 4 Si no se carga el controlador TAP en las máquinas Mac y linux, ejecute el script de shell para cargar el controlador.

Sistema operativo	Descripción
Mac	Ejecute el script de shell <code>Naclient.sh</code> desde el directorio <code>/opt/sslvpn-plus/naclient/</code> con privilegios sudo .
Linux	Ejecute el script de shell <code>naclient.sh</code> con privilegios sudo . Puede encontrar este script en el directorio <code>linux_phat_client/linux_phat_client</code> .

- 5 Para resolver los mensajes de advertencia de extensión del kernel en máquinas con macOS High Sierra o versiones posteriores, debe proporcionar una aprobación explícita de usuario para cargar una extensión del kernel (kext). Realice los pasos siguientes:
 - a En su máquina Mac, abra la ventana **Preferencias del Sistema > Seguridad y privacidad**.
 - b En la parte inferior de la ventana verá un mensaje similar a "Se bloqueó la descarga de algún software de sistema" ("Some system software was blocked from loading"). Haga clic en el botón "Permitir".
 - c Para continuar con la instalación, haga clic en **Permitir**.

Para obtener más información sobre cómo proporcionar la aprobación de usuario para cargar una extensión del kernel, consulte https://developer.apple.com/library/content/technotes/tn2459/_index.html.
 - d Mientras se carga la extensión del kernel, el proceso de instalación del cliente SSL VPN-Plus se ejecuta en segundo plano. Se instala el cliente SSL VPN-Plus, pero aparece el siguiente mensaje de error: Error en la instalación. El instalador encontró un error que provocó que la instalación no se realizara correctamente. Para obtener ayuda, póngase en contacto con el fabricante del software. (The installation failed. The installer encountered an error that cause the installation to fail. Contact the software manufacturer for assistance).
 - e Para solucionar este error, desinstale el cliente SSL VPN-Plus y vuelva a instalarlo.

- 6 Para resolver los mensajes de error de instalación en macOS High Sierra, realice los siguientes pasos.

- a Compruebe que las notificaciones estén habilitadas. Acceda a **Preferencias del Sistema > Seguridad y privacidad > Permitir notificaciones**.

Nota Al instalar el cliente SSL VPN-Plus por primera vez en Mac OS High Sierra, una ventana de notificación le solicitará que permita la instalación. Esta notificación suele durar 30 minutos. Si la notificación desaparece antes de hacer clic en **Permitir**, reinicie el equipo y vuelva a instalar el cliente SSL VPN-Plus SSL.

Si se siguen produciendo errores de instalación, esto significa que el sistema no permite la extensión del kernel (kext) ni le solicita que lo cargue. Complete el resto de los pasos secundarios para agregar tuntap kext team id a la lista de kext aprobados previamente.

- b Reinicie la máquina Mac en modo de recuperación.
- 1 Haga clic en el logotipo de Apple situado en la parte superior izquierda de la pantalla.
 - 2 Haga clic en **Reiniciar**.
 - 3 Pulse inmediatamente las teclas Comando y R hasta que vea un logotipo de Apple o un globo girando. El globo girando aparece cuando la máquina Mac intenta iniciar el modo de recuperación de macOS conectándose a Internet porque no puede iniciarlo mediante el sistema de recuperación integrado. A continuación, Mac se inicia en modo de recuperación.
- c En la barra superior, haga clic en **Utilidades > Terminal**.
- d Para agregar tuntap kext team id a la lista de kext preaprobados, ejecute el comando – `spctl kext-consent add KS8XL6T9FZ`.
- e Reinicie la máquina Mac en modo normal.
- f Para comprobar si team-id aparece en la lista de kext preaprobados, ejecute el comando – `spctl kext-consent list`.
- g Instale el paquete del cliente SSL VPN-Plus.
- 7 En las máquinas Windows, si aparece el error (E00024B) de instalación del controlador, deshabilite la opción **Ocultar el adaptador de red cliente SSL** (Hide SSL client network adapter) en el instalador SSL VPN-Plus cliente de Edge. Para obtener más instrucciones sobre cómo deshabilitar esta opción, consulte el artículo <https://kb.vmware.com/s/article/2108766> de la base de conocimientos de VMware.

SSL VPN-Plus: problemas de comunicación

Utilice este tema para comprender los posibles problemas de rutas de datos y de conectividad de SSL VPN, y para saber cómo puede solucionarlos.

Problema

A continuación, aparecen los problemas comunes asociados a la ruta de datos y a la conectividad SSL VPN:

- El cliente SSL VPN-Plus no puede conectarse al servidor SSL VPN.
- El cliente SSL VPN-Plus está instalado, pero los servicios SSL VPN-Plus no se están ejecutando.
- Se alcanzó el recuento máximo de usuarios que iniciaron sesión. Aparece el siguiente mensaje en el portal web SSL VPN o el cliente SSL VPN-Plus:

Se alcanzó el número máximo de usuarios/Se alcanzó el recuento máximo de sesiones iniciadas de acuerdo con la licencia de SSL VPN. Inténtelo de nuevo pasado un tiempo o Se produjo un error de lectura de SSL (Maximum users reached/Maximum count of logged in user reached as per SSL VPN license. Please try after some time or SSL read has failed).
- Los servicios SSL VPN se están ejecutando, pero la ruta de datos no funciona.
- Se establece la conexión SSL VPN, pero no se puede acceder a las aplicaciones de la red privada.

Solución

- 1 Si el cliente SSL VPN-Plus no puede conectarse al servidor SSL VPN, haga lo siguiente:
 - Asegúrese de que el usuario de SSL VPN inició sesión con la contraseña y el nombre de usuario correctos.
 - Compruebe si el usuario SSL VPN es válido.
 - Verifique si el usuario SSL VPN puede acceder al servidor SSL VPN usando el portal web.
- 2 En NSX Edge, siga estos pasos para verificar si el proceso SSL VPN se está ejecutando.
 - a Inicie sesión en NSX Edge desde la CLI. Para obtener más información sobre cómo iniciar sesión en la CLI de Edge, consulte *Referencia de la interfaz de línea de comandos de NSX*.
 - b Ejecute el comando `show process monitor` y busque el proceso `sslvpn`.
 - c Ejecute el comando `show service network-connections` y compruebe si el proceso `sslvpn` aparece en el puerto 443.

Nota De forma predeterminada, el sistema utiliza el puerto 443 para el tráfico SSL. Sin embargo, si configuró un puerto TCP diferente para el tráfico SSL, asegúrese de que el proceso `sslvpn` aparece en dicho número de puerto TCP.

3 En el cliente SSL VPN-Plus, compruebe que los servicios SSL VPN-Plus se estén ejecutando.

Sistema operativo	Descripción
Servidor	Abra el Administrador de tareas y compruebe si se inició el servicio del cliente SSL VPN-Plus.
Mac	<ul style="list-style-type: none"> ■ Asegúrese de que el proceso <code>naclntd</code> se inició para el daemon. ■ Asegúrese de que el proceso <code>naclnt</code> se inició para la GUI. <p>Para comprobar si los procesos se están ejecutando, ejecute el comando <code>ps -ef grep "naclnt"</code>.</p>
Linux	<ul style="list-style-type: none"> ■ Asegúrese de que se inician los procesos <code>naclntd</code> y <code>naclnt_poll</code>. ■ Para comprobar si los procesos se están ejecutando, ejecute el comando <code>ps -ef grep "naclnt"</code>.

Si los servicios no se están ejecutando, ejecute los siguientes comandos para iniciar los servicios.

Sistema operativo	Comando
Mac	Ejecute el comando <code>sudo launchctl load -w /Library/LaunchDaemons/com.vmware.naclntd.plist</code> .
Linux	Ejecute el comando <code>sudo service naclnt start</code> .

4 Si se alcanza el recuento máximo de usuarios SSL VPN con sesión iniciada, aumente el número de usuarios simultáneos (CCU) aumentando el formato de NSX Edge.

Para obtener más información, consulte la *Guía de administración de NSX*. Tenga en cuenta que los usuarios conectados se desconectan de la VPN al realizar esta operación.

5 Si los servicios SSL VPN se están ejecutando, pero la ruta de datos no funciona, realice los siguientes pasos:

- Compruebe si se asignó una IP virtual tras conectarse correctamente.
- Verifique si se agregaron las rutas.

- 6 Si no se puede acceder a las aplicaciones de red (back-end) privada, realice los siguientes pasos para solucionar el problema:
 - a Asegúrese de que la red privada y el grupo de IP no estén en la misma subred.
 - b Si el administrador no tiene ningún grupo de IP definido o si el grupo de IP se agotó, realice los siguientes pasos.
 - 1 Inicie sesión en vSphere Web Client.
 - 2 Haga clic en **Redes y seguridad** (Networking & Security) y, a continuación, en **NSX Edge** (NSX Edges).
 - 3 Haga doble clic en un NSX Edge y, a continuación, haga clic en la pestaña **SSL VPN-Plus**.
 - 4 Agregue un grupo de direcciones IP estático, tal y como se explica en el tema sobre cómo agregar un grupo de direcciones IP que aparece en *Guía de administración de NSX*. Asegúrese de agregar la dirección IP en el cuadro de texto **Puerta de enlace** (Gateway). La dirección IP de la puerta de enlace se asigna a la interfaz de *na0*. Todo el tráfico que no sea TCP fluye a través de un adaptador virtual denominado interfaz de *na0*. Puede crear varios grupos de direcciones IP con diferentes direcciones IP de puerta de enlace, pero asignadas a la misma interfaz de *na0*.
 - 5 Utilice el comando `show interface na0` para verificar la dirección IP proporcionada y comprobar si todos los grupos de direcciones IP están asignados a la misma interfaz de *na0*.
 - 6 Inicie sesión en el equipo cliente, acceda a la pantalla de **Cliente SSL VPN-Plus: Estadísticas** (SSL VPN-Plus Client - Statistics) y compruebe la dirección IP virtual asignada.
 - c Inicie sesión en la interfaz de línea de comandos (CLI) de NSX Edge y haga una captura de paquetes en la interfaz de *na0* ejecutando el comando `debug packet capture interface na0`. También puede capturar paquetes usando la herramienta de **captura de paquetes**. Para obtener más información, consulte *Guía de administración de NSX*.
-
- Nota** La captura de paquetes continúa ejecutándose en segundo plano hasta que detenga la captura al ejecutar el comando `no debug packet capture interface na0`.
-
- d Si la optimización de TCP no está habilitada, compruebe las reglas de firewall.
 - e En el tráfico que no sea TCP, asegúrese de que la red back-end tenga establecida la puerta de enlace predeterminada como interfaz interna de Edge.
 - f En los clientes Mac y Linux, inicie sesión en el sistema en el que está instalado el cliente SSL VPN y haga una captura de paquetes en la interfaz de *tap0* o el adaptador virtual ejecutando el comando `tcpdump -i tap0 -s 1500 -w filepath`. En clientes Windows, utilice una herramienta para analizar paquetes, como Wireshark, y capture paquetes en el adaptador del cliente SSL VPN-Plus.

- 7 Si los pasos anteriores no resuelven el problema, intente solucionarlo con los siguientes comandos de la CLI de NSX Edge.

Propósito	Comando
Compruebe el estado de SSL VPN.	<code>show service sslvpn-plus</code>
Compruebe las estadísticas de SSL VPN.	<code>show service sslvpn-plus stats</code>
Compruebe que los clientes VPN estén conectados.	<code>show service sslvpn-plus tunnels</code>
Compruebe las sesiones SSL VPN-Plus.	<code>show service sslvpn-plus sessions</code>

SSL VPN-Plus: problemas de autenticación

Tiene problemas con la autenticación en SSL VPN-Plus.

Problema

Se produce un error en la autenticación de SSL VPN-Plus.

Solución

- ◆ Si tiene problemas de autenticación, verifique las siguientes opciones:
 - a Asegúrese de que pueda acceder al servidor de autenticación externo desde NSX Edge. Desde NSX Edge, haga ping en el servidor de autenticación y compruebe que el servidor sea accesible.
 - b Consulte la configuración del servidor de autenticación externo con herramientas como el explorador de LDAP y compruebe si funciona la configuración. Los servidores de autenticación de LDAP y de AD solo se pueden comprobar mediante el explorador de LDAP.
 - c Asegúrese de que el servidor de autenticación local esté establecido en la prioridad más baja si se configuró en el proceso de autenticación.
 - d Si utiliza Active Directory (AD), establézcalo en modo de no-ssl y cree una captura de paquetes en la interfaz desde la cual se puede acceder al servidor de AD.
 - e Si la autenticación se realiza correctamente en el servidor syslog, aparecerá un mensaje similar a:


```
Log Output - SVP_LOG_NOTICE,
10-28-2013,09:28:39,Authentication,a,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2013,09:28:39,-,-,,,,,,,,-,-,
```
 - f Si se produce un error en la autenticación en el servidor syslog, aparecerá un mensaje similar a:


```
Log Output - SVP_LOG_NOTICE,
10-28-2013,09:28:39,Authentication,a,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2013,09:28:39,-,-,,,,,,,,-,-,
```

El cliente SSL VPN-Plus deja de responder

El cliente SSL VPN-Plus deja de responder cuando la optimización TCP está habilitada.

Problema

Configuró el servicio SSL VPN-Plus para ejecutarlo en un NSX Edge y habilitó la optimización TCP para enviar el tráfico a través del túnel. El cliente SSL VPN-Plus deja de responder cuando ejecuta cualquier medida de rendimiento de red y herramienta de ajuste (por ejemplo, iperf3) en el cliente SSL VPN-Plus.

Causa

Uno de los dos escenarios siguientes puede provocar que el túnel detecte un error cuando se envían datos desde el cliente SSL VPN-Plus:

- El servidor back-end cierra las conexiones TCP con el servidor VPN SSL cuando se envía una secuencia TCP FIN.
- Aparece un error en la operación para escribir en túneles mientras se envían datos al servidor back-end.

El error de lectura del túnel es ID de protocolo desconocido (unknown protocol ID). Este error elimina el túnel entre el servidor VPN SSL y el cliente SSL VPN-Plus, que provoca que fallen las operaciones de lectura y escritura de SSL en el cliente, y el cliente SSL VPN-Plus deja de responder.

Solución

- ◆ Para solucionar el problema, siga estos pasos en vSphere Web Client para deshabilitar la optimización de TCP para el tráfico de red privado mediante el túnel VPN SSL.
 - a Haga doble clic en la máquina virtual de NSX Edge en la que configuró el servicio de SSL VPN-Plus.
 - b Haga clic en la pestaña **SSL VPN-Plus** y seleccione la red privada.
 - c Desmarque la casilla de verificación **Habilitar optimización de TCP** (Enable TCP Optimization).

Análisis de registro básico

Los registros de la puerta de enlace de SSL VPN-Plus se envían al servidor syslog configurado en el dispositivo NSX Edge. Los registros del cliente SSL VPN-Plus se almacenan en el directorio siguiente del equipo del usuario remoto: C:\Users\nombredeusuario\AppData\Local\VMware\vpn\svp_client.log.

Análisis de registro básico: autenticación

Autenticación correcta

- El siguiente resultado del registro muestra que el usuario *a* se autenticó correctamente con Network Access Client el *28 de octubre de 2016* a las *0928* horas.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

Error de autenticación

- El siguiente resultado del registro muestra que el usuario *a* no se pudo autenticar con Network Access Client el *28 de octubre de 2016* a las *0928* horas.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILUR
E,,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

Para solucionar problemas de autenticación, consulte [SSL VPN-Plus: errores de instalación](#).

Análisis de registro básico: ruta de datos

Ruta de datos correcta

- El siguiente resultado del registro muestra que el usuario *a* se conectó correctamente con Network Access Client a través de TCP al servidor web backend *192.168.10.8* el *28 de octubre de 2016* a las *0941* horas.

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP
Connect,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,,10-28-2013,09:41:03,-,-,192.168.10.8,8
0,,,,,,,,,-,-,-
```

Error de ruta de datos

- El siguiente resultado del registro muestra que el usuario *a* no se pudo conectar con Network Access Client a través de TCP al servidor web backend *192.168.10.8* el *28 de octubre de 2016* a las *0941* horas.

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP
Connect,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,,10-28-2013,09:41:03,-,-,192.168.10.8,8
0,,,,,,,,,-,-,-
```

IPsec VPN

Utilice esta información para solucionar problemas de negociación en la configuración.

Negociación correcta (Fase 1 y Fase 2)

Los siguientes ejemplos muestran un resultado de negociación exitoso entre NSX Edge y un dispositivo Cisco.

NSX Edge

Desde la interfaz de línea de comandos NSX Edge (ipsec auto -status, part of show service ipsec command):

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

Cisco

```
ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

IKE Peer: 10.20.129.80
Type : L2L           Role   : responder
Rekey : no           State  : MM_ACTIVE
Encrypt : 3des       Hash   : SHA
Auth : preshared     Lifetime: 28800
Lifetime Remaining: 28379
```

No coincide la directiva de Fase 1

A continuación se incluyen los registros de error de la directiva de Fase 1 de no coincidencia.

NSX Edge

NSX Edge deja de responder en el estado STATE_MAIN_I1. En /var/log/messages, busque información donde se muestre que el elemento del mismo nivel envió de vuelta el mensaje IKE establecido en "NO_PROPOSAL_CHOSEN".

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
    expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    | Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
    "s1-c1" #1: ignoring informational payload,
    type NO_PROPOSAL_CHOSEN msgid=00000000
```

Cisco

Si se habilita el cifrado de depuración, se imprimirá un mensaje de error para mostrar que ninguna propuesta fue aceptada.

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
    IP = 10.20.129.80, IKE_DECODE RECEIVED
```

```

    Message (msgid=0) with payloads : HDR + SA (1)
    + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
    processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
    types for class Group Description: Rcv'd: Group 5
    Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
    types for class Group Description: Rcv'd: Group 5
    Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
    Message (msgid=0) with payloads : HDR + NOTIFY (11)
    + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
    All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
    payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
    FSM error history (struct &0xd8355a60) <state>, <event>:
    MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
    MM:9e0e4511 terminating: flags 0x01000002, refcnt 0,
    tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
    delete/delete with reason message

```

No coincide la Fase 2

A continuación se incluyen los registros de error de la directiva de Fase 2 de no coincidencia.

NSX Edge

NSX Edge deja de responder en STATE_QUICK_I1. Un mensaje del registro muestra que el elemento del mismo nivel envió el mensaje NO_PROPOSAL_CHOSEN.

```

000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
    QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
    idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
    0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
    ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     next payload
    type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |
    |     DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     Notify Message
    Type: NO_PROPOSAL_CHOSEN

```



```
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
    ignoring informational payload, type NO_PROPOSAL_CHOSEN
    msgid=00000000
```

Cisco

El mensaje de depuración muestra que la Fase 1 está completa, pero se produjo un error en la Fase 2 por un error en la negociación de la directiva.

```
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
    IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
    for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
    Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
    + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
    total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
    Session is being torn down. Reason: Phase 2 Mismatch
```

Falta de coincidencia con PFS

A continuación se incluyen los registros de error de falta de coincidencia con PFS.

NSX Edge

PFS se negocia como parte de la Fase 2. Si PFS no coincide, el comportamiento es similar al del caso de error descrito en [No coincide la Fase 2](#)

```
000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
    QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
    idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
    (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | next payload
    type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    | DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | Notify Message
    Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
    informational payload, type NO_PROPOSAL_CHOSEN
    msgid=00000000
```

```
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info: fa 16 b3 e5
          91 a9 b0 02 a3 30 e1 d9 6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info: 93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
          | processing informational NO_PROPOSAL_CHOSEN (14)
```

Cisco

```
<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
          IP = 10.20.129.80, sending delete/delete with
          reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
          IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
          IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
          IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
          IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
          Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
          + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
          Session is being torn down. Reason: Phase 2 Mismatch
```

No coincide con PSK

A continuación se incluyen los registros de error de la directiva PSK de no coincidencia.

NSX Edge

PSK se negocia en la última ronda de la Fase 1. Si se produce un error en la negociación de PSK, el estado de NSX Edge es STATE_MAIN_I4. El elemento del mismo nivel envía el mensaje INVALID_ID_INFORMATION.

```
Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
          "s1-c1" #1: transition from state STATE_MAIN_I3 to
          state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
          STATE_MAIN_I4: ISAKMP SA established
          {auth=OAKLEY_PRESHARED_KEY
          cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
          Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
          initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
          {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
          pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
```

```
ignoring informational payload, type INVALID_ID_INFORMATION
msgid=00000000
```

Cisco

```
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
+ NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, Received encrypted Oakley Main Mode
packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
Message (msgid=0) with payloads : HDR + NOTIFY (11)
+ NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, ERROR, had problems decrypting
packet, probably due to mismatched pre-shared key.
Aborting
```

Captura de paquetes para una negociación correcta

A continuación se incluye una sesión de captura de paquetes para lograr una negociación correcta entre NSX Edge y un dispositivo Cisco.

No.	Time	Source	Destination	Protocol	Info
9203	768.394800	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

Frame 9203 (190 bytes on wire, 190 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 0000000000000000
 Next payload: Security Association (1)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x00
 Message ID: 0x00000000
 Length: 148
 Security Association payload
 Next payload: Vendor ID (13)
 Payload length: 84
 Domain of interpretation: IPSEC (1)
 Situation: IDENTITY (1)
 Proposal payload # 0
 Next payload: NONE (0)
 Payload length: 72
 Proposal number: 0

```

Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms: 2
Transform payload # 0
  Next payload: Transform (3)
  Payload length: 32
  Transform number: 0
  Transform ID: KEY_IKE (1)
  Life-Type (11): Seconds (1)
  Life-Duration (12): Duration-Value (28800)
  Encryption-Algorithm (1): 3DES-CBC (5)
  Hash-Algorithm (2): SHA (2)
  Authentication-Method (3): PSK (1)
  Group-Description (4): 1536 bit MODP group (5)
Transform payload # 1
  Next payload: NONE (0)
  Payload length: 32
  Transform number: 1
  Transform ID: KEY_IKE (1)
  Life-Type (11): Seconds (1)
  Life-Duration (12): Duration-Value (28800)
  Encryption-Algorithm (1): 3DES-CBC (5)
  Hash-Algorithm (2): SHA (2)
  Authentication-Method (3): PSK (1)
  Group-Description (4): Alternate 1024-bit MODP group (2)
Vendor ID: 4F456C6A405D72544D42754D
  Next payload: Vendor ID (13)
  Payload length: 16
  Vendor ID: 4F456C6A405D72544D42754D
Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
  Next payload: NONE (0)
  Payload length: 20
  Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

```

No.	Time	Source	Destination	Protocol Info
9204	768.395550	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
  Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
  Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 104
  Security Association payload
    Next payload: Vendor ID (13)

```

```

Payload length: 52
Domain of interpretation: IPSEC (1)
Situation: IDENTITY (1)
Proposal payload # 1
  Next payload: NONE (0)
  Payload length: 40
  Proposal number: 1
  Protocol ID: ISAKMP (1)
  SPI Size: 0
  Proposal transforms: 1
  Transform payload # 1
    Next payload: NONE (0)
    Payload length: 32
    Transform number: 1
    Transform ID: KEY_IKE (1)
    Encryption-Algorithm (1): 3DES-CBC (5)
    Hash-Algorithm (2): SHA (2)
    Group-Description (4): Alternate 1024-bit MODP group (2)
    Authentication-Method (3): PSK (1)
    Life-Type (11): Seconds (1)
    Life-Duration (12): Duration-Value (28800)
Vendor ID: Microsoft L2TP/IPSec VPN Client
  Next payload: NONE (0)
  Payload length: 24
  Vendor ID: Microsoft L2TP/IPSec VPN Client

```

No.	Time	Source	Destination	Protocol Info
9205	768.399599	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

```

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
  Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
  Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data

```

No.	Time	Source	Destination	Protocol	Info
9206	768.401192	10.20.131.62	10.20.129.80	ISAKMP	Identity Protection (Main Mode)

Frame 9206 (298 bytes on wire, 298 bytes captured)
 Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Key Exchange (4)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x00
 Message ID: 0x00000000
 Length: 256
 Key Exchange payload
 Next payload: Nonce (10)
 Payload length: 132
 Key Exchange Data (128 bytes / 1024 bits)
 Nonce payload
 Next payload: Vendor ID (13)
 Payload length: 24
 Nonce Data
 Vendor ID: CISCO-UNITY-1.0
 Next payload: Vendor ID (13)
 Payload length: 20
 Vendor ID: CISCO-UNITY-1.0
 Vendor ID: draft-beaulieu-ike-xauth-02.txt
 Next payload: Vendor ID (13)
 Payload length: 12
 Vendor ID: draft-beaulieu-ike-xauth-02.txt
 Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
 Next payload: Vendor ID (13)
 Payload length: 20
 Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
 Vendor ID: CISCO-CONCENTRATOR
 Next payload: NONE (0)
 Payload length: 20
 Vendor ID: CISCO-CONCENTRATOR

No.	Time	Source	Destination	Protocol	Info
9207	768.404990	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

Frame 9207 (110 bytes on wire, 110 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52

Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x01
 Message ID: 0x00000000
 Length: 68
 Encrypted payload (40 bytes)

No.	Time	Source	Destination	Protocol	Info
9208	768.405921	10.20.131.62	10.20.129.80	ISAKMP	Identity Protection (Main Mode)

Frame 9208 (126 bytes on wire, 126 bytes captured)
 Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x01
 Message ID: 0x00000000
 Length: 84
 Encrypted payload (56 bytes)

No.	Time	Source	Destination	Protocol	Info
9209	768.409799	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

Frame 9209 (334 bytes on wire, 334 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

No.	Time	Source	Destination	Protocol	Info
9210	768.411797	10.20.131.62	10.20.129.80	ISAKMP	Quick Mode

Frame 9210 (334 bytes on wire, 334 bytes captured)
 Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)

```

Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
    Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 92585D2D797E9C52
    Responder cookie: 34704CFC8C8DBD09
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags: 0x01
    Message ID: 0x79a63fb1
    Length: 292
    Encrypted payload (264 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9211	768.437057	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```

Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
    Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
    Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 92585D2D797E9C52
    Responder cookie: 34704CFC8C8DBD09
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
    Flags: 0x01
    Message ID: 0x79a63fb1
    Length: 52
    Encrypted payload (24 bytes)

```


Resolución de problemas relacionados con NSX Controller

8

Esta sección proporciona información sobre cómo identificar la causa de los errores de NSX Controller y solucionar los problemas de los controladores.

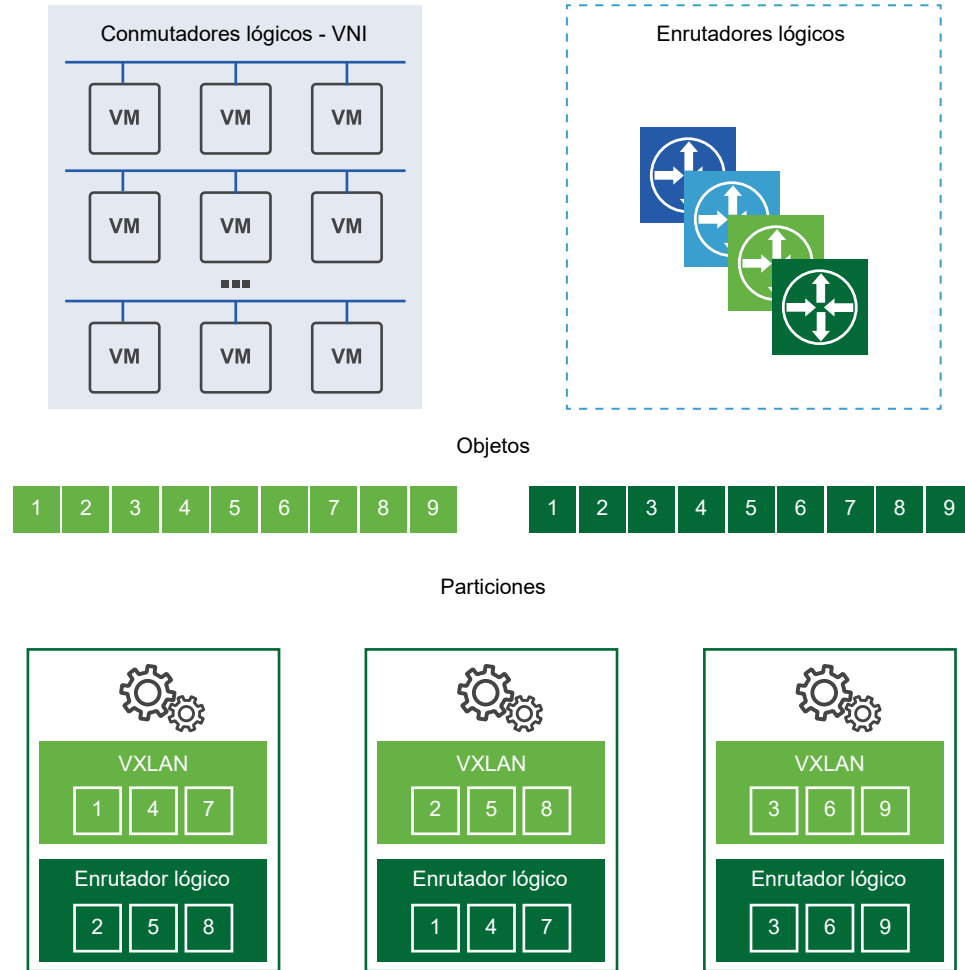
Este capítulo incluye los siguientes temas:

- [Comprender la arquitectura del clúster de controladores](#)
- [Problemas de implementación de NSX Controller](#)
- [Resolución de problemas de latencia del disco](#)
- [Errores de clústeres de NSX Controller](#)
- [NSX Controller está desconectado](#)
- [Problemas del agente de plano de control \(netcpa\)](#)

Comprender la arquitectura del clúster de controladores

El clúster de NSX Controller constituye un sistema distribuido horizontal en el que a cada nodo controlador se le asigna un conjunto de funciones que definen el tipo de tareas que puede implementar. Por motivos de resistencia y rendimiento, la implementación de máquinas virtuales de controladores debe hacerse en tres hosts distintos.

Se utilizan particiones para distribuir las cargas de trabajo entre los nodos del clúster de NSX Controller. Para ello, se dividen las cargas de trabajo de NSX Controller en diferentes particiones para que cada instancia de NSX Controller realice la misma cantidad de trabajo.



Esto demuestra cómo distintos nodos de controladores funcionan como principales en determinadas entidades, como los conmutadores lógicos, el enrutadores lógicos y otros servicios. Cuando se le asigna una función a una instancia de NSX Controller principal, NSX Controller divide los diferentes enrutadores y conmutadores lógicos entre todas las instancias de NSX Controller disponibles en el clúster.

Cada cuadro con un número representa una partición que la instancia principal utiliza para dividir las cargas de trabajo. El conmutador lógico principal divide los conmutadores lógicos en particiones y les asigna diferentes instancias de NSX Controller. El enrutador lógico principal también divide los enrutadores lógicos en particiones y les asigna diferentes instancias de NSX Controller.

Estas particiones se asignan a las distintas instancias de NSX Controller que hay en ese clúster. El conmutador o enrutador principal de una función decide qué instancias de NSX Controller se asignan a cada partición. Si la partición 3 de los enrutadores recibe una solicitud, esta debe conectarse a la tercera instancia de NSX Controller. Si la recibe la partición 2 de los conmutadores lógicos, la procesa la segunda instancia de NSX Controller.

Si se produce un error en una de las instancias de NSX Controller del clúster, los enrutadores o conmutadores principales de las funciones redistribuyen las particiones entre el resto de clústeres disponibles. Para cada función, se elige un nodo controlador principal. Este es responsable de asignar las particiones a nodos controladores individuales, determinar si se produce un error en un nodo y reasignar las particiones a otros nodos. También informa a los hosts ESXi de los errores que se producen en el nodo del clúster.

La elección del nodo principal de cada función requiere el voto de la mayoría de todos los nodos activos e inactivos del clúster. Este es el motivo principal por el que un clúster de controladores debe implementarse siempre con un número de nodos impar.

ZooKeeper

ZooKeeper es la arquitectura de servidor cliente responsable del mecanismo del clúster de NSX Controller. Se utiliza para descubrir y crear el clúster de controladores. Cuando aparece un clúster, esto significa que, literalmente, aparece ZooKeeper entre todos los nodos. Los nodos de ZooKeeper pasan un proceso de elección para formar el clúster de controladores, que debe tener un nodo de ZooKeeper principal. Este proceso se lleva a cabo mediante una elección entre nodos.

Cuando se crea un nuevo nodo controlador, NSX Manager propaga su información al clúster actual, con la IP y el ID del nodo. De este modo, cada nodo conoce el número total de nodos disponibles para formar el clúster. En el proceso de elección del nodo de ZooKeeper principal, cada nodo tiene un voto para elegir al principal. La votación se activa de nuevo hasta que un nodo cuenta con la mayoría de los votos. Por ejemplo, en un clúster de tres nodos, el principal debe recibir un mínimo de dos votos.

Nota Para evitar un escenario en el que no se pueda elegir un nodo de ZooKeeper principal, el clúster DEBE tener tres nodos.

- Cuando se implementa el primer controlador, se trata de un caso especial y este se convierte en el principal. Así, al implementar los controladores, el primer nodo debe completar la implementación antes de que se agreguen otros nodos.
- Al agregar el segundo controlador, también se trata de un caso especial, ya que el número de nodos es par en este momento.
- Cuando se agrega el tercero, el clúster adquiere un estado estable admitido.

ZooKeeper admite un único error cada vez. Esto quiere decir que, si un nodo controlador está inactivo, debe recuperarse antes de que se produzcan otros errores. De lo contrario, pueden producirse problemas que dañen el clúster.

Administrador de dominios del plano de control central (CCP)

Esta capa se encuentra por encima de ZooKeeper y proporciona la configuración de ZooKeeper a todos los nodos para iniciar el proceso. El administrador de dominios actualiza la configuración entre todos los nodos del clúster y, a continuación, lleva a cabo una llamada de procedimiento remota para que se inicie el proceso de ZooKeeper.

Además, es el responsable de iniciar todos los dominios. Para unir el clúster, el dominio del CCP se comunica con el dominio del CCP de otros equipos. *zk-cluster-bootstrap* es el componente del dominio del CCP que ayuda a iniciar el clúster.

Relación de los controladores con otros componentes

El clúster del controlador mantiene y proporciona información sobre los conmutadores lógicos, enrutadores lógicos y los VTEP a los hosts ESXi.

Al crear un conmutador lógico, los nodos de los controladores dentro del clúster determinan qué nodo será el *principal* (master) o *propietario* (owner) de ese conmutador lógico. Esto también ocurre al agregar un enrutador lógico.

Cuando se establece la propiedad de un conmutador o enrutador lógico, el nodo la envía a los hosts ESXi de la zona de transporte del conmutador o enrutador. El proceso de elección del propietario y el envío de esta información a los hosts es lo que se conoce como hacer particiones. Tenga en cuenta que el nodo propietario es el responsable de todas las operaciones relacionadas con NSX de ese conmutador o enrutador lógico. El resto de los nodos no realizarán ninguna operación de ese conmutador lógico.

Un único propietario debe ser la fuente de información veraz de un conmutador lógico y un enrutador lógico. Por lo tanto, si el clúster de controladores se daña y se eligen dos o más nodos propietarios, cada host de la red tendrá una información distinta procedente de esa fuente del conmutador o enrutador lógico. Si esto sucede, se interrumpirá la red porque las operaciones del plano de datos y control de esta solo pueden tener una fuente de información veraz.

Si un nodo controlador se encuentra inactivo, el resto de los nodos del clúster vuelven a realizar las particiones para determinar la propiedad del conmutador lógico y del enrutador lógico.

Problemas de implementación de NSX Controller

NSX Manager implementa las controladoras de NSX en formato OVA. Un clúster de controladoras proporciona una gran disponibilidad. Para implementar las controladoras, debe haber configurado los DNS y NTP en NSX Manager, vCenter Server y hosts ESXi. Se debe utilizar un grupo de IP estático para asignar las direcciones IP a cada controladora.

Le recomendamos que implemente las reglas de antiafinidad de DRS para mantener las instancias de NSX Controller en hosts distintos. Debe implementar TRES instancias de NSX Controller.

Problemas frecuentes relacionados con las controladoras

A continuación le mostramos los problemas más habituales que pueden aparecer durante la implementación de las instancias de NSX Controller:

- Errores de implementación de NSX Controller.
- NSX Controller no se puede unir al clúster.

- Al ejecutar el comando `show control-cluster status`, Estado de la mayoría (Majority status) cambia de Conectado a la mayoría del clúster (Connected to cluster majority) a Conexión interrumpida con la mayoría del clúster (Interrupted connection to cluster majority).
- El panel de control de NSX muestra un problema con el estado de conectividad.
- Se recomienda utilizar el comando `show control-cluster status` para ver si un controlador se ha unido a un clúster de control. Debe ejecutarlo en cada controlador para conocer el estado general del clúster.

controller # show control-cluster status		
Type	Status	Since
Join status:	Join complete	10/17 18:16:58
Majority status:	Connected to cluster majority	10/17 18:16:46
Restart status:	This controller can be safely restarted	10/17 18:16:51
Cluster ID:	af2e9dec-19b9-4530-8e68-944188584268	
Node UUID:	af2e9dec-19b9-4530-8e68-944188584268	
Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
dht_node	enabled	activated

Nota Cuando vea que el nodo controlador está desconectado, NO utilice los comandos `join cluster` ni `force join`. Este comando no está diseñado para unir el nodo al clúster. Si lo utiliza, es posible que el clúster adquiera un estado desconocido.

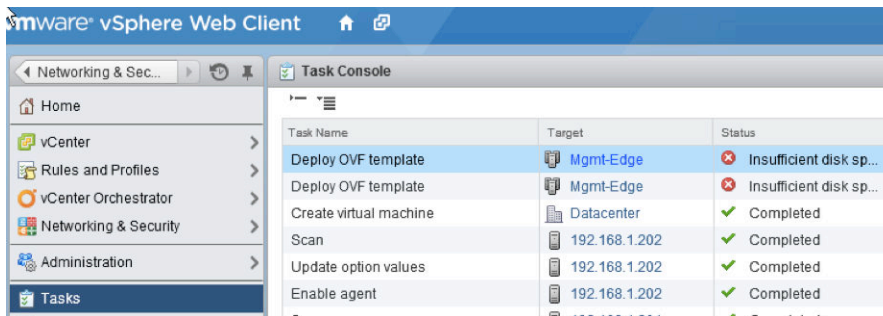
Los nodos de inicio del clúster sirven únicamente como pista a los miembros del clúster durante su inicio. No se preocupe si esta lista contiene miembros del clúster que están fuera de servicio. Esto no afectará a la función del clúster.

Todos los miembros deben tener el mismo ID de clúster. Si no es así, significa que el clúster está dañado y debe ponerse en contacto con el equipo de soporte técnico de VMware para repararlo.

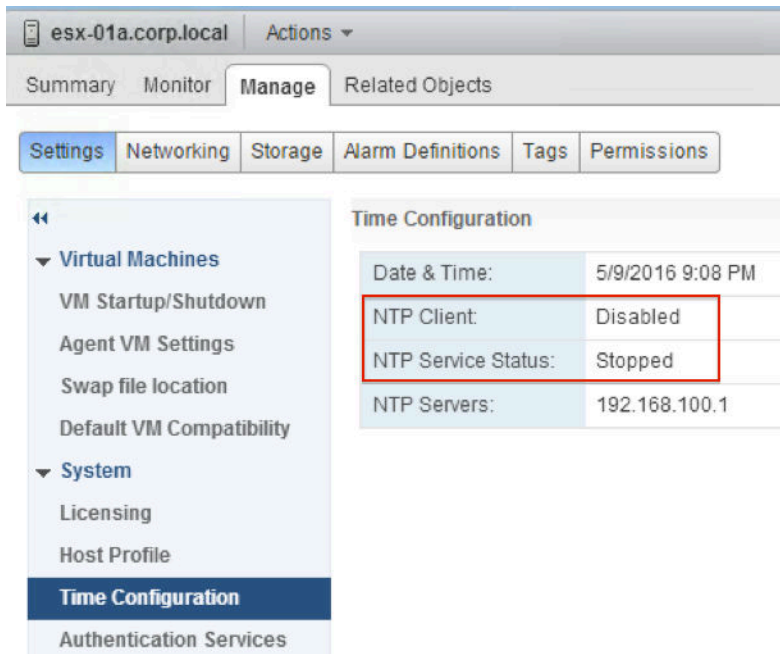
- El comando `show control-cluster startup-nodes` no está diseñado para mostrar todos los nodos actuales del clúster. En su lugar, muestra el resto de nodos controladores que utiliza este nodo para unirse al clúster cuando se reinicia el proceso del controlador. Por tanto, es posible que el resultado del comando muestre algunos nodos apagados o retirados del clúster.
- Además, el comando `show control-cluster network ipsec status` permite inspeccionar el estado del protocolo de seguridad de Internet (IPsec). Si observa que los controladores no se pueden comunicar entre sí durante unos minutos o unas horas, ejecute el comando `cat /var/log/syslog | egrep "sending DPD request|IKE_SA"` y compruebe si los mensajes de registro indican que no hay tráfico. También puede ejecutar el comando `ipsec`

`statusall | egrep "bytes_i|bytes_o"` y verificar que no hay túneles de IPsec establecidos. Proporcione el resultado de estos comandos y los registros del controlador cuando informe a su representante del equipo de soporte técnico de VMware sobre un posible problema del clúster de control.

- Problemas de conectividad entre NSX Manager y las controladoras de NSX. Este error suele deberse a problemas relacionados con la conectividad de la red física o a un firewall que bloquea la comunicación.
- No hay recursos suficientes (como almacenamiento disponible en vSphere para alojar las controladoras). Puede identificar estos problemas al consultar el registro de las tareas y los eventos de vCenter durante la implementación de la controladora.



- Una controladora que no funciona correctamente con un comportamiento "inadecuado" o una controladora actualizada con el estado **Disconnected** (Desconectada).
- El DNS no se configuró correctamente en los hosts ESXi ni en NSX Manager.
- El servidor NTP no está sincronizado en los hosts ESXi ni en NSX Manager.



- Cuando están recién conectadas, las máquinas virtuales no tienen acceso a la red. Es posible que esto se deba a un problema relacionado con el plano de control. Compruebe el estado de la controladora.

Asimismo, intente ejecutar el comando `esxcli network vswitch dvs vmware vxlan network list --vds-name <name>` en los hosts ESXi para comprobar el estado del plano de control. Tenga en cuenta que la conexión de la controladora está desactivada.

```
/etc/vmware/netcpa # esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS
VXLAN ID Multicast IP Control Plane Controller Connection
ARP Entry Count MTEP Count
-----
5000 N/A (headend replication) Enabled (multicast proxy, ARP proxy) 192.168.110.203 (down)
0 0
```

- Al ejecutar el comando de CLI `show log manager follow` de NSX Manager, se pueden identificar otros motivos por los que se producen fallos al implementar controladoras.

```
2014-02-26 10:09:44.931 GMT INFO taskScheduler-25 VcConnection$VimClient:1219 - Create stub for com.vmware.vim.binding
28c5157-abf3-718e-88c5-42209f389211
2014-02-26 10:09:44.932 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:301 - got prop collector up
ctReference: type = PropertyFilter, value = session[d46b86a2-7a10-c17e-6ebe-8ab252ee4efd]527420f2-bdd7-529b-8ab6-17d16
6E3-4A64-96D7-5833C287588F
2014-02-26 10:09:44.937 GMT ERROR taskScheduler-25 VCUtils:184 - Error while waiting for property collector updates.
com.vmware.vim.binding.vim.fault.NoDiskSpace:
datastore = datastore1 (1)
inherited from com.vmware.vim.binding.vim.fault.FileFault:
file = [datastore1 (1)] NSX_Controller_1c3dd18d-0cd3-4d7d-896b-51247176ae77/NSX_Controller_1c3dd18d-0cd3-4d7d-896b-512
inherited from com.vmware.vim.binding.vim.fault.VimFault:
inherited from com.vmware.vim.binding.vim.fault.NoDiskSpace: Insufficient disk space on datastore 'datastore1 (1)'.
```

Problemas de conectividad del host

Compruebe los errores de conectividad del host con los siguientes comandos. Ejecute estos comandos en cada nodo controlador.

- Busque estadísticas de error que no sean normales con el comando `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by host_IP`.
- Verifique la alta tasa de mensajes o las estadísticas de mensajes del enrutador o el conmutador lógicos con los siguientes comandos:
 - `show control-cluster core stats`: estadísticas generales
 - `show control-cluster core stats-sample`: muestras de las últimas estadísticas
 - `show control-cluster core connection-stats ip`: estadísticas por conexión
 - `show control-cluster logical-switches stats`
 - `show control-cluster logical-routers stats`
 - `show control-cluster logical-switches stats-sample`
 - `show control-cluster logical-routers stats-sample`
 - `show control-cluster logical-switches vni-stats vni`
 - `show control-cluster logical-switches vni-stats-sample vni`
 - `show control-cluster logical-switches connection-stats ip`

- `show control-cluster logical-routers connection-stats ip`
- Puede utilizar el comando `show host hostID health-status` para comprobar el estado de los hosts en sus clústeres preparados. Para solucionar los problemas del controlador, son compatibles las siguientes comprobaciones de estado:
 - Compruebe si `net-config-by-vsm.xml` está sincronizado con la lista de controladores.
 - Compruebe si hay una conexión de socket al controlador.
 - Compruebe si el identificador de red VXLAN (VNI) está creado y si la configuración es correcta.
 - Compruebe que el VNI pueda conectarse a los controladores principales (si está habilitado el plano de control).

Problemas de implementación e instalación

- Verifique que haya al menos tres nodos controladores implementados en un clúster. VMware recomienda utilizar las reglas de antiafinidad de vSphere nativas para evitar que se implemente más de un nodo controlador en el mismo host ESXi.
- Compruebe que todos los NSX Controller muestren el estado Conectado (Connected). Si algún nodo controlador muestra el estado Desconectado (Disconnected), compruebe que la siguiente información sea coherente. Para ello, ejecute el comando `show control-cluster status` en todos los nodos controladores:

Tipo	Estado
Estado de unión (Join status)	Unión completa (Join complete)
Estado de la mayoría (Majority status)	Conectado a la mayoría del clúster (Connected to cluster majority)
ID de clúster (Cluster ID)	Misma información en todos los nodos controladores (Same information on all controller nodes)

- Compruebe que todas las funciones sean consistentes en todos los nodos controladores:

Función	Estado configurado	Estado activo
<code>api_provider</code>	habilitado (enabled)	activado (activated)
<code>persistence_server</code>	habilitado (enabled)	activado (activated)
<code>switch_manager</code>	habilitado (enabled)	activado (activated)
<code>logical_manager</code>	habilitado (enabled)	activado (activated)
<code>directory_server</code>	habilitado (enabled)	activado (activated)

- Verifique que el proceso `vnet-controller` se esté ejecutando. Ejecute el comando `show process` en todos los nodos controladores y compruebe que el servicio `java-dir-server` se esté ejecutando.

- Verifique el historial del clúster y compruebe que la conexión del host no cambie y que no haya errores de unión de VNI ni cambios que no sean normales en los miembros del clúster. Para ello, ejecute el comando `show control-cluster history`. Los comandos también muestran si el nodo se reinicia frecuentemente. Compruebe que no haya muchos archivos de registro de tamaño cero (0) y con diferentes ID de proceso.
- Compruebe que el identificador de red VXLAN (VNI) esté configurado. Para obtener más información, consulte la sección sobre los pasos de preparación de VXLAN de la VMware VXLAN Deployment Guide.
- Compruebe que el protocolo SSL esté habilitado en el clúster de controladores. Ejecute el comando `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by sslEnabled` en cada nodo controlador.

Resolución de problemas de latencia del disco

Puede ver las alertas de latencia del disco en la pestaña **Administración** (Management). Las instancias de NSX Controller funcionan con discos de baja latencia.

Ver alertas de latencia del disco

Las alertas de latencia del disco supervisan la disponibilidad del disco y los problemas de latencia y generan informes sobre esto. Puede consultar información sobre la latencia del disco de cada NSX Controller. Los cálculos de latencia de lectura y escritura se obtienen de una media móvil de 5 segundos (predeterminada), lo que se utiliza para activar una alerta si se supera el límite de latencia. La alerta se desactiva cuando la media se reduce al límite mínimo. De forma predeterminada, se establecen 200 ms como límite máximo y 100 ms como límite mínimo. Las latencias altas afectan al funcionamiento de las aplicaciones de clústeres distribuidos de cada nodo controlador.

Para ver las alertas de latencia del disco de NSX Controller, siga este procedimiento:

Requisitos previos

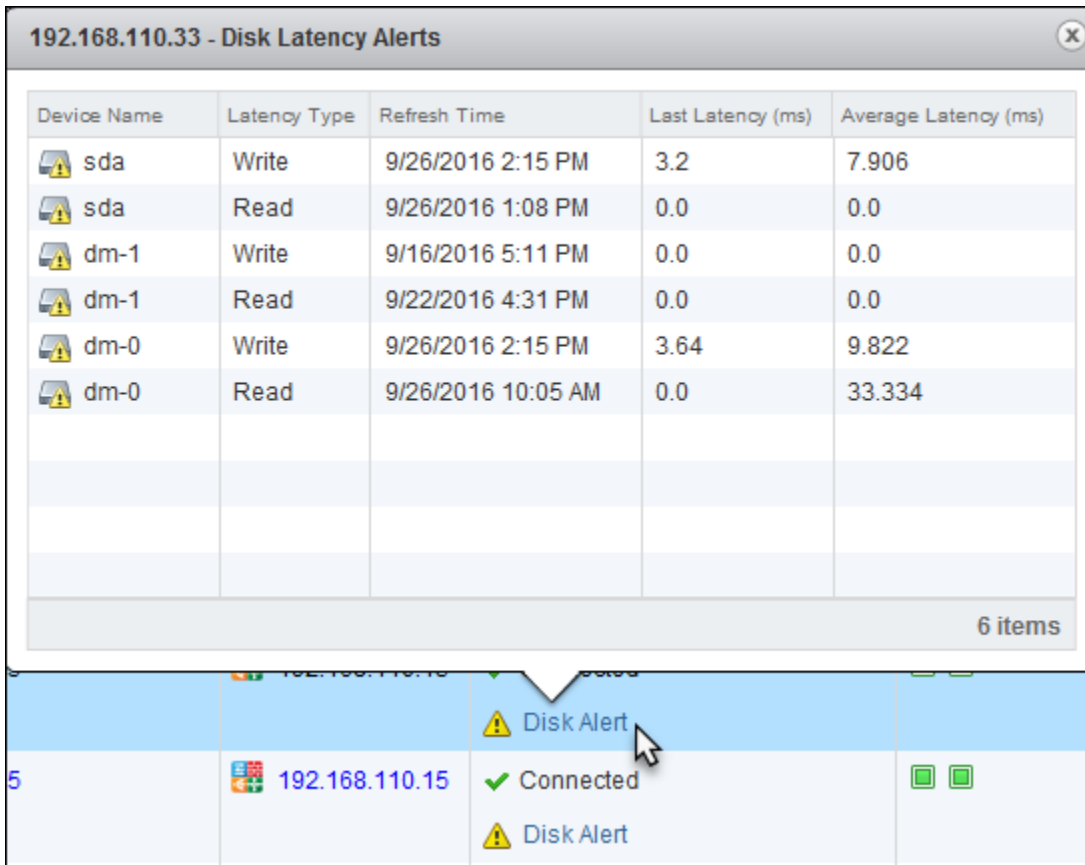
Se alcanzó el límite de latencia.

Procedimiento







- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).

- En **Administración** (Management), vaya al controlador que quiera consultar y haga clic en el vínculo **Alerta del disco** (Disk Alert).

Aparecerá la ventana Alertas de latencia del disco (Disk Latency Alerts).



The screenshot shows a window titled "192.168.110.33 - Disk Latency Alerts". Inside is a table with the following data:

Device Name	Latency Type	Refresh Time	Last Latency (ms)	Average Latency (ms)
 sda	Write	9/26/2016 2:15 PM	3.2	7.906
 sda	Read	9/26/2016 1:08 PM	0.0	0.0
 dm-1	Write	9/16/2016 5:11 PM	0.0	0.0
 dm-1	Read	9/22/2016 4:31 PM	0.0	0.0
 dm-0	Write	9/26/2016 2:15 PM	3.64	9.822
 dm-0	Read	9/26/2016 10:05 AM	0.0	33.334

At the bottom right of the table, it says "6 items". Below the table, there is a blue bar with a yellow warning icon and the text "Disk Alert". A mouse cursor is pointing at this button. Below the blue bar, there is a row with a green checkmark and the text "Connected", and another row with a yellow warning icon and the text "Disk Alert".

Resultados

En ella podrá consultar los detalles de latencia del controlador seleccionado. Los registros de alertas se almacenan durante siete días en el archivo `cloudnet/run/iostat/iostat_alert.log`. Puede utilizar el comando `show log cloudnet/run/iostat/iostat_alert.log` para abrir el archivo de registros.

Pasos siguientes

Para obtener más información sobre cómo solucionar problemas de latencia del disco, consulte [Problemas de latencia de disco](#).

Para obtener más información sobre los mensajes de registro, consulte la sección *Eventos del sistema y de registro de NSX*.

Problemas de latencia de disco

Los controladores funcionan con discos de baja latencia. El clúster necesita un sistema de almacenamiento en disco para que cada nodo tenga una latencia de escritura máxima de menos de 300 ms y mínima de 100 ms.

Problema

- Un NSX Controller se desconecta de un clúster de controladores.
- No se pueden recopilar registros del controlador porque la partición del disco está llena.
- Si el sistema de almacenamiento no cumple estos requisitos, el clúster puede volverse inestable y provocar un tiempo de inactividad del sistema.
- Los agentes de escucha de TCP aplicables a un NSX Controller que funciona ya no aparecen en los resultados del comando `show network connections of-type tcp`.
- El controlador desconectado intenta unirse al clúster utilizando un UUID compuesto únicamente de ceros que no es válido.
- El comando para mostrar el historial del clúster de control muestra un mensaje similar al siguiente:
INFO.20150530-000550.1774:D0530 13:25:29.452639 1983 zookeeper_client.cc:774] Zookeeper client disconnected!
- Al ejecutar el comando `show log cloudnet/cloudnet_java-zookeeper*.log` en la consola de NSX Controller aparecen entradas similares a las siguientes:

```
cloudnet_java-zookeeper.20150530-000550.1806.log-2015-05-30
13:25:07,382 47956539 [SyncThread:1] WARN
org.apache.zookeeper.server.persistence.FileTxnLog - fsync-ing the write ahead
log in SyncThread:1 took 3219ms which will adversely effect operation latency.
See the ZooKeeper troubleshooting guide
```

- Los registros de NSX Controller contienen entradas similares a las siguientes:

```
D0525 13:46:07.185200 31975
rpc-broker.cc:369] Registering address resolution for: 20.5.1.11:7777
D0525 13:46:07.185246 31975
rpc-tcp.cc:548] Handshake complete, both peers support the same
protocol
D0525 13:46:07.197654 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
D0525 13:46:07.222869 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
```

Causa

Este problema se debe a un rendimiento lento del disco que afecta negativamente al clúster de NSX Controller.

- Compruebe si el disco tiene un rendimiento lento. Para ello, busque mensajes de *fsync* en el archivo `/var/log/cloudnet/cloudnet_java-zookeeper.log`. Si *fsync* tarda más de un segundo,

ZooKeeper muestra un mensaje de advertencia de *fsync*, lo que quiere decir que el disco es demasiado lento. VMware recomienda dedicar un número de unidad lógica (LUN) específicamente al clúster de control, así como acercar la matriz de almacenamiento al clúster de control en términos de latencia.

- Puede consultar los cálculos de latencia de lectura y escritura obtenidos en una media móvil de 5 segundos (predeterminados), que se utiliza para activar una alerta si se supera el límite de latencia. La alerta se desactiva cuando la media se reduce al límite mínimo. De forma predeterminada, se establecen 200 ms como límite máximo y 100 ms como límite mínimo. Puede utilizar el comando `show disk-latency-alert config`. El resultado que se muestra es el siguiente:

```
enabled=True    low-wm=51      high-wm=150
nsx-controller # set disk-latency-alert enabled yes
nsx-controller # set disk-latency-alert low-wm 100
nsx-controller # set disk-latency-alert high-wm 200
```

- Utilice la REST API GET `/api/2.0/vdn/controller/<controller-id>/systemStats` para recuperar el estado de alerta de latencia de los nodos controladores.
- Utilice la REST API GET `/api/2.0/vdn/controller` para indicar si la alerta de latencia de disco se detecta en un nodo controlador.

Solución

- 1 Implemente NSX Controller en los discos con baja latencia.
- 2 Cada controlador debe utilizar su propio servidor de almacenamiento en disco. No utilice el mismo servidor de almacenamiento en disco en dos controladores.

Pasos siguientes

Para obtener más información sobre cómo ver las alertas, consulte [Ver alertas de latencia del disco](#).

Errores de clústeres de NSX Controller

Cuando se produce un error en uno de los nodos de NSX Controller del clúster, seguirá habiendo dos controladoras que funcionan. La mayoría del clúster se mantiene y el plano de control sigue funcionando.

Problema

El clúster de NSX Controller falla.

Solución

- 1 Inicie sesión en vSphere Web Client.
- 2 En **Redes y seguridad** (Networking & Security), haga clic en **Instalación > Administración** (Installation > Management).

- 3 En la sección de nodos de NSX Controller, observe la columna Del mismo nivel (Peers). Si esta muestra cuadros verdes, significa que no hay errores de conectividad del controlador del mismo nivel en el clúster. Por el contrario, los cuadros rojos indican que sí hay un error. Haga clic en el cuadro para ver los detalles.
- 4 Si la columna Del mismo nivel (Peers) indica que hay un problema en el clúster de controladores, inicie sesión en cada CLI de NSX Controller para obtener un diagnóstico detallado. Ejecute el comando `control-cluster status` para mostrar información y diagnosticar el estado de cada controlador. Todos los controladores del clúster deben tener el mismo UUID de clúster. Sin embargo, puede que este no coincida con el UUID del controlador principal. Puede obtener información sobre los problemas de implementación según lo descrito en [Problemas de implementación de NSX Controller](#).
- 5 Puede seguir estos pasos para solucionar el problema antes de volver a implementar el nodo de controlador o el clúster de controladores:
 - a Compruebe que el controlador esté encendido.
 - b Intente hacer ping al controlador afectado y, desde este, a otros nodos y al administrador para consultar las rutas de red. Si observa algún problema de red, solúcelo como se indica en [Problemas de implementación de NSX Controller](#).
 - c Consulte el estado del protocolo de seguridad de Internet (IPSec) utilizando los siguientes comandos de la CLI.
 - Verifique si el IPSec está habilitado con el comando `show control-cluster network ipsec status`.
 - Verifique el estado los túneles del IPSec con el comando `show control-cluster network ipsec tunnels`.

También puede utilizar los datos del estado del IPSec para abrir una incidencia con el servicio de soporte técnico de VMware.
 - d Si no se trata de un problema de red, decida si quiere reiniciarlo o volver a implementarlo.

Si quiere reiniciar un nodo, asegúrese de que solo reinicie un controlador cada vez. Sin embargo, si el estado del clúster de controladores muestra errores en más de un nodo de controlador, reinicie todos al mismo tiempo. Si reinicia un nodo de un clúster en buen estado, confirme siempre que el clúster se reformó correctamente al terminar y, a continuación, confirme que se volvió a hacer una partición del clúster correctamente.
- 6 Si decide volver a implementar los controladores, utilice uno de estos dos métodos:
 - Método 1: Eliminar el nodo de controlador dañado e implementar un nuevo nodo de controlador.
 - Método 2: Eliminar el clúster de controladores e implementar un nuevo clúster de controladores.

VMware recomienda seguir el segundo método.

Pasos siguientes

Elija uno de los dos métodos:

- [Método 1: Eliminar el controlador dañado e implementar un nuevo controlador](#)
- [Método 2: Volver a implementar el clúster de NSX Controller](#)

Método 1: Eliminar el controlador dañado e implementar un nuevo controlador

En primer lugar, puede intentar resolver el problema sin tener que implementar un nuevo clúster de NSX Controller. Este método consiste en eliminar primero el nodo de NSX Controller dañado y, a continuación, implemente un nuevo nodo de NSX Controller.

Procedimiento

1 [Eliminar un NSX Controller](#)

Puede eliminar un NSX Controller forzando la acción o sin forzarla. Sin forzarla, se comprueban las siguientes condiciones antes de eliminar el nodo:

2 [Volver a implementar un NSX Controller](#)

Después de eliminar el nodo de controlador dañado, implemente un nuevo nodo de controlador.

Eliminar un NSX Controller

Puede eliminar un NSX Controller forzando la acción o sin forzarla. Sin forzarla, se comprueban las siguientes condiciones antes de eliminar el nodo:

- Actualmente no hay ninguna operación de actualización del nodo de NSX Controller.
- El clúster de controladores está en buen estado y se puede procesar una solicitud de API del clúster de controladores.
- El estado del host, obtenido del inventario de vCenter Server indica que está conectado y encendido.
- No se trata del último nodo controlador.

Si se hace de manera forzada, no se comprobarán estas condiciones antes de eliminar el nodo controlador.

- Cuestiones que deben tenerse en cuenta al eliminar controladores:
 - No intente eliminar la máquina virtual del controlador antes hacerlo a través de la API o la interfaz de usuario de vSphere Web Client. Si no se puede usar la interfaz de usuario, utilice la API DELETE /2.0/vdn/controller/{controllerId} para eliminar el controlador.
 - Después de eliminar un nodo, compruebe que el clúster actual permanezca estable.
 - Al eliminar todos los nodos de un clúster, el último nodo que queda se debe eliminar con la opción **Eliminar el controlador de manera forzada** (Forcefully remove the controller). Verifique siempre que la VM del controlador se haya eliminado correctamente. Si no es así, desconecte manualmente la VM y elimine la VM del controlador mediante la interfaz de usuario.

- Si la operación no funciona, significa que no se pudo eliminar la máquina virtual. En ese caso, invoque la eliminación del controlador a través de la interfaz de usuario mediante la opción **Eliminar el controlador de manera forzada** (Forcefully remove the controller). En la API, asigne al parámetro `forceRemove` el valor `true`. Tras forzar la eliminación, desconecte manualmente la VM y elimine la VM del controlador mediante la interfaz de usuario.
 - Solo puede producirse un error en un clúster de varios nodos, por lo que la eliminación cuenta como error. El nodo eliminado se debe volver a implementar antes de que se produzca otro error.
 - En el entorno de Cross-vCenter NSX:
 - No se puede eliminar la máquina virtual del controlador ni desconectarla directamente en vCenter Server. La columna **Estado** (Status) muestra el estado **No sincronizado** (Out of sync).
 - Si se elimina únicamente una parte del controlador y queda una entrada en la base de datos de NSX Manager en un entorno de Cross-vCenter NSX, utilice la API DELETE `api/2.0/vdn/controller/external`.
 - Si se importa el controlador a través de la API de NSX Manager, utilice la API `removeExternalControllerReference` con la opción `forceRemove`.
 - Al eliminar un controlador, NSX solicita eliminar un controlador de la máquina virtual a través de vCenter Server con el identificador de objetos administrados (MOID) de la máquina virtual. Si vCenter Server no puede encontrar la máquina virtual por su identificador MOID, NSX informa de que se produjo un error en el controlador, elimina la solicitud y anula la operación.
- Si se selecciona la opción **Eliminar de manera forzada** (Forcefully Delete), NSX no se anulará la operación de eliminación del controlador y se borrará su información. NSX también actualiza todos los hosts para que no confíen en el controlador eliminado. Sin embargo, si la máquina virtual del controlador está todavía activa y en ejecución con un MOID diferente, todavía tiene las credenciales para participar como miembro del clúster del controlador. En este escenario, cualquier conmutador lógico o enrutador que estén asignados a este nodo controlador no funcionarán correctamente debido a que los hosts ESXi ya no confían en el controlador que se eliminó.

Para eliminar el NSX Controller, siga este procedimiento:

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
- 2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).
- 3 En **Administración** (Management), seleccione el controlador que quiera eliminar.
- 4 Haga clic en el icono **Eliminar (x)** (Delete).

5 Seleccione **Eliminar (Delete) o **Eliminar de manera forzada** (Forcefully Delete).**

- ◆ Si selecciona la opción **Eliminar de manera forzada** (Forcefully Delete), el controlador se eliminará de manera forzada. Esta opción ignora cualquier error y borra la información de la base de datos. Debe asegurarse de que cualquier posible error se solucione manualmente. Debe confirmar que la máquina virtual del controlador se eliminó correctamente. En caso contrario, deberá eliminarla a través de vCenter Server.

Nota Al eliminar el último controlador del clúster, debe seleccionar la opción **Eliminar de manera forzada** (Forcefully Delete) para eliminar el último nodo controlador. Cuando no hay controladores en el sistema, los hosts funcionan en lo que se denomina modo "sin periféricos". Las máquinas virtuales migradas con vMotion o las máquinas virtuales nuevas tendrán problemas de red hasta que se implementen los controladores nuevos y se complete la sincronización.

- ◆ Si no selecciona esta opción, el controlador se eliminará sin forzar la acción.

6 Haga clic en **Sí (Yes). Si no se fuerza la acción, el controlador se elimina siguiendo esta secuencia:**

- a Apague el nodo.
- b Compruebe el estado del clúster.
- c Si no está en buen estado, encienda el controlador y anule la solicitud de eliminación.
- d Si está en buen estado, elimine la máquina virtual del controlador y libere la dirección IP del nodo.
- e Elimine del clúster la identidad de la máquina virtual del controlador.

Se eliminará el controlador seleccionado.

7 Vuelva a sincronizar el estado del controlador. Para ello, haga clic en **Acciones > Actualizar estado del controlador (Actions > Update Controller State).**

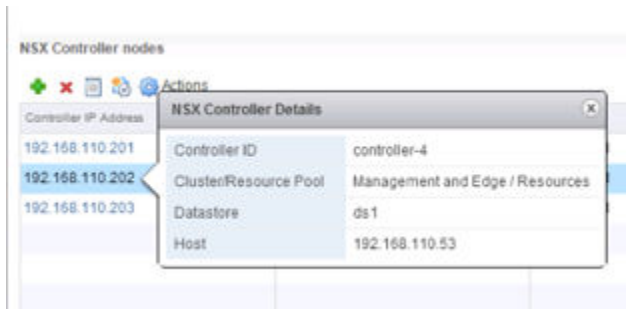
Volver a implementar un NSX Controller

Después de eliminar el nodo de controlador dañado, implemente un nuevo nodo de controlador.

Procedimiento

- 1** Inicie sesión en vSphere Web Client.
- 2** En **Redes y seguridad** (Networking & Security), haga clic en **Instalación > Administración** (Installation > Management).
- 3** En la sección **Nodos de NSX Controller** (NSX Controller nodes), haga clic en el controlador afectado. Haga capturas de pantalla o anote la información de la configuración de la pantalla **Detalles de NSX Controller** (NSX Controller Details) para poder consultarla en el futuro.

Por ejemplo:



- 4 Implemente un nuevo nodo de NSX Controller. Para ello, haga clic en el icono **Agregar nodo (+)** (Add Node).
- 5 En el cuadro de diálogo Agregar controlador (Add Controller), seleccione el centro de datos en el que agregará los nodos y configure las opciones del controlador.
 - a Seleccione el clúster adecuado.
 - b Seleccione un host en el clúster y el almacenamiento.
 - c Seleccione el grupo de puertos distribuidos.
 - d Seleccione el grupo de direcciones IP desde el cual se deben asignar las direcciones IP al nodo.
 - e Haga clic en **Aceptar** (OK), espere a que finalice la instalación y asegúrese de que el estado del nodo sea **Normal**.

Para obtener información detallada sobre cómo agregar un nodo de controlador, consulte "Implementar clúster de NSX Controller" en la *Guía de instalación de NSX*.

- 6 Vuelva a sincronizar el estado del controlador. Para ello, haga clic en **Acciones (Actions) > Actualizar estado del controlador (Update Controller State)**.

La opción Actualizar estado del controlador (Update Controller State) envía la configuración actual del enrutador lógico distribuido y de VXLAN (que incluye los objetos universales en una implementación de Cross-vCenter NSX) de NSX Manager al clúster de controladores.

Método 2: Volver a implementar el clúster de NSX Controller

Este método consiste en eliminar los tres nodos de controlador y agregar nuevos nodos de controlador para mantener un clúster de tres nodos completamente funcional.

VMware recomienda eliminar el clúster de NSX Controller cuando se cumpla cualquiera de las siguientes condiciones:

- Uno o varios nodos de controlador sufren errores catastróficos o irreversibles.
- No se puede acceder a las máquinas virtuales del controlador y no se pueden solucionar.

En estos casos, es preferible eliminar todos los nodos de controlador, aunque algunos parezcan estar en buen estado.

Vuelva a implementar un nuevo clúster de controladores y, a continuación, actualice el mecanismo de estado del controlador en NSX Manager. La actualización del estado del controlador hace que VXLAN se vuelva a sincronizar y que los enrutadores lógicos distribuidos se vuelvan a implementar.

Procedimiento

- 1 Inicie sesión en vSphere Web Client.
 - 2 Vaya a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Administración (Management)**.
 - 3 En la sección **Nodos de NSX Controller** (NSX Controller Nodes), elimine todos los nodos de controlador. Seleccione un nodo cada vez y haga clic en el icono **Eliminar** (Delete) (✖).
- Cuando no haya controladores en el sistema, los hosts funcionarán en modo "sin periféricos". Las máquinas virtuales nuevas o migradas tendrán problemas de red hasta que se implementen los controladores nuevos y se complete la sincronización.
- 4 Implemente tres nodos de controlador nuevos para crear un clúster de NSX Controller totalmente funcional.
- Para obtener información detallada sobre cómo agregar un clúster de controladores, consulte "Implementar clúster de NSX Controller" en la *Guía de instalación de NSX*.
- 5 Vuelva a sincronizar el estado del controlador. Para ello, haga clic en **Acciones (Actions) > Actualizar estado del controlador (Update Controller State)**.

Controlador fantasma

Un controlador fantasma puede ser la máquina virtual de un controlador activo o una máquina virtual que no existe y puede estar participando o no en el clúster. NSX Manager sincroniza la lista de todas las máquinas virtuales desde el inventario de vCenter Server. Un controlador fantasma se crea cuando vCenter Server o el host eliminan la máquina virtual de un controlador sin una solicitud de NSX Manager, o bien cuando el inventario de vCenter Server cambia el MOID de referencia de las máquinas virtuales del controlador.

Cuando el controlador se crea desde NSX, la información sobre la configuración se almacena en NSX Manager. NSX Manager implementa la nueva máquina virtual del controlador a través de vCenter Server.

El administrador de NSX proporciona a NSX Manager la configuración, incluido el grupo de direcciones IP, para crear un controlador. NSX Manager elimina una dirección IP del grupo y la envía a vCenter Server con el resto de la configuración del controlador como una solicitud de creación de máquina virtual. NSX Manager espera a que vCenter Server confirme el estado de la solicitud.

- The controller creation process was successful: si la máquina virtual del controlador se crea correctamente, vCenter Server la iniciará. NSX Manager almacena el identificador de objetos administrados (MOID) de la máquina virtual con el resto de la información de configuración del controlador. El MOID (o MO-REF) es un identificador único que vCenter asigna a cada objeto de su inventario. vCenter Server también usa este MOID para realizar un seguimiento de la máquina virtual si sigue formando parte del inventario de vCenter Server.
- The controller creation process was not successful: si las configuraciones de conexión de red e IP eran incorrectas, es posible que NSX Manager no pueda establecer conexión con vCenter Server.

NSX Manager espera una cantidad predeterminada de tiempo para crear un clúster de controladores de un solo nodo (si es el primero) o un nuevo controlador para agregarla al clúster activo. Si se agota este tiempo, NSX Manager solicita a vCenter Server que elimine la máquina virtual. La dirección IP se devuelve al grupo y NSX declara un error al crear el controlador.

Cómo se crean los controladores fantasma

Cuando NSX Manager solicita eliminar un controlador, vCenter Server busca la máquina virtual del controlador que utiliza ese MOID para su eliminación.

Sin embargo, si las actividades de vCenter tienen como resultado la eliminación de la máquina virtual del controlador desde el inventario de vCenter Server, vCenter elimina el MOID de su base de datos. Tenga en cuenta que la máquina virtual del controlador puede seguir estando activa y en funcionamiento en NSX Manager aunque se haya eliminado del inventario de vCenter. Pero para vCenter Server, la máquina virtual del controlador ya no existe. Aunque vCenter Server haya quitado la máquina virtual de su inventario, esta no se puede eliminar. Si la máquina virtual aún está activa, todavía estará participando o intentando participar en el clúster de controladores de NSX.

A continuación se muestra el ejemplo más común de cómo se crea un controlador fantasma:

- El administrador de vCenter Server elimina del inventario el host que contiene el controlador de la máquina virtual. Más tarde, vuelve a agregar el host. Cuando se elimina el host, vCenter Server elimina todos los MOID asociados al host y las máquinas virtuales que contiene. Cuando el host se vuelve a agregar, vCenter Server asigna un nuevo MOID al host y las máquinas virtuales. Para los usuarios de NSX, el host y la máquina virtual siguen siendo los mismos, pero vCenter Server considera a estos hosts y a estas máquinas virtuales objetos nuevos. Sin embargo, a efectos prácticos, los hosts y las máquinas virtuales siguen siendo los mismos. Las aplicaciones que se ejecutan en el host y en las máquinas virtuales no cambian.
- El administrador de vCenter Server elimina la máquina virtual del controlador a través de vCenter Server o mediante la administración de hosts. La eliminación no se inició en NSX Manager.
- En este caso, la *eliminación* incluye también cualquier error de almacenamiento o del host que tenga como resultado la pérdida de la máquina virtual. En este caso, la máquina virtual se pierde para vCenter Server y también para el clúster y NSX Manager. Pero como la eliminación no se inició en NSX Manager, tanto NSX Manager como el clúster de los controladores consideran que el controlador aún es válido. El estado del controlador devuelto a NSX Manager indica que este nodo controlador está inactivo, no forma parte del clúster y se muestra en la interfaz de usuario. NSX Manager también tiene registros que indican que ya no es posible acceder al controlador.

Qué hacer cuando se detecta un controlador fantasma

- 1 Sincronice los controladores como se describe en la sección [NSX Controller está desconectado](#).
- 2 Consulte las entradas de los registros. Si la máquina virtual del controlador se eliminó de forma accidental o resultó dañada, debe usar la opción **Eliminar de manera forzada** (Forcefully Delete) para borrar la entrada de la base de datos de NSX Manager. Para obtener más información, consulte [Eliminar un NSX Controller](#).

3 Después de eliminar el controlador, confirme que:

- La máquina virtual del controlador se eliminó.
- El comando `show controller-cluster startup-nodes` muestra solo controladores válidos.
- Las entradas de syslog de NSX Manager ya no muestran un controlador adicional.

A partir de la versión 6.2.7 de NSX, NSX Manager comprueba el MOID original de la máquina virtual del controlador en el inventario de vCenter para asegurarse de que aún existe. Si NSX Manager no encuentra la máquina virtual del controlador en el inventario, NSX Manager la busca mediante el UUID de instancia de la máquina virtual. El UUID de instancia se almacena en la máquina virtual, por lo que no cambia aunque la máquina virtual se vuelva a agregar al inventario de vCenter. Si NSX Manager encuentra la máquina virtual con el UUID de instancia, NSX Manager actualizará su base de datos con el nuevo MOID.

Sin embargo, si clona la máquina virtual del controlador, la máquina virtual clonada tendrá las mismas propiedades que la original, pero un nuevo UUID de instancia. NSX Manager no puede detectar el MOID de la máquina virtual clonada.

Entradas de registro de controladores fantasma

Las siguientes entradas de registro de errores se producen cuando se detecta un controlador fantasma:

- 2017-07-31 22:15:05.844 UTC ERROR NVPStatusCheck ControllerServiceImpl:2146 – Controller <#> does not exist, might be deleted already. Skip saving its connectivity info.
- 2017-07-31 22:15:05.769 UTC ERROR NVPStatusCheck ControllerServiceImpl:2580 – the node is created by this NSX Manager <#>, but database has no record and delete might be in progress.

NSX Controller está desconectado

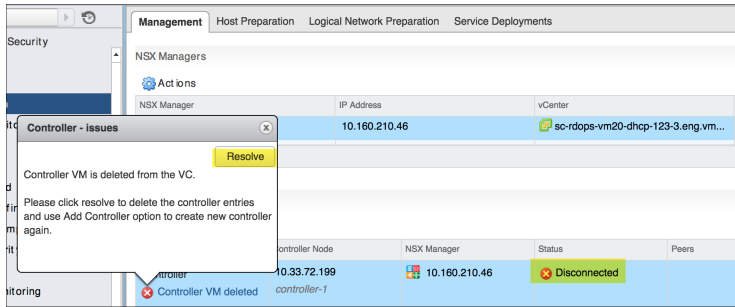
Si se desconectó la máquina virtual de NSX Controller desde vCenter Server o se eliminó una máquina virtual del controlador de vCenter Server, la columna **Estado** (Status) de la página **Instalación** (Installation) > **Administración** (Management) muestra el estado **No sincronizado** (Out of sync).

Requisitos previos

Máquina virtual del controlador desconectada o eliminada de vCenter Server.

Procedimiento

- 1 En vSphere Web Client, acceda a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Administración (Management)**.



- 2 Haga clic en el vínculo **Error** para consultar la razón detallada del estado sin sincronización.
- 3 Haga clic en el botón **Resolver** (Resolve) para solucionar el problema.

Resultados

Si la máquina virtual del controlador está desconectada, el plano de administración activa un comando power on para el controlador.

Si se elimina la máquina virtual del controlador, las entradas del controlador se eliminan del plano de administración y este lo comunica al plano de control central.

Pasos siguientes

Cree un controlador utilizando la opción **Agregar nodo** (Add node). Para obtener más información, consulte la *Guía de administración de NSX*.

Problemas del agente de plano de control (netcpa)

En NSX for vSphere, el plano de control (netcpa) actúa como demonio de agente local, que se comunica con NSX Manager y el clúster de controladores. La función **Estado del canal de comunicación** comprueba el estado de forma proactiva y genera informes periódicos sobre el estado del plano de control central, local y de NSX Manager. Muestra los resultados en la interfaz de usuario de NSX Manager. Estos informes también funcionan como latidos para que el canal del netcpa del host ESXi detecte el estado de funcionamiento de NSX Manager. Proporcionan información detallada durante los errores de comunicación, generan un evento cuando el canal tiene un estado incorrecto y envían mensajes de latidos desde NSX Manager a los hosts.

Problema

Problemas de conectividad entre el agente de plano de control y la controladora.

Causa

Si falta alguna conexión, es posible que el agente de plano de control no funcione correctamente.

Solución

- 1 Cuando el canal tenga un estado incorrecto, valide el estado de la conexión mediante el siguiente comando:

```
GET https://<NSX_Manager_IP>/api/2.0/vdn/inventory/host/{hostId}/connection/status
```

A continuación, se incluye un ejemplo del valor devuelto:

```
<?xml version="1.0" encoding="UTF-8"?>
<hostConnStatus>
<hostName>10.161.246.20</hostName>
<hostId>host-21</hostId>
<nsxMgrToFirewallAgentConn>UP</nsxMgrToFirewallAgentConn>
<nsxMgrToControlPlaneAgentConn>UP</nsxMgrToControlPlaneAgentConn>
<hostToControllerConn>DOWN</hostToControllerConn>
<fullSyncCount>-1</fullSyncCount>
<hostToControllerConnectionErrors>
<hostToControllerConnectionError>
<controllerIp>10.160.203.236</controllerIp>
<errorCode>1255604</errorCode>
<errorMessage>Connection Refused</errorMessage>
</hostToControllerConnectionError>
<hostToControllerConnectionError>
<controllerIp>10.160.203.237</controllerIp>
<errorCode>1255603</errorCode>
<errorMessage>SSL Handshake Failure</errorMessage>
</hostToControllerConnectionError>
</hostToControllerConnectionErrors>
</hostConnStatus>
```

Son compatibles los siguientes códigos de error:

```
1255602: Certificado del controlador incompleto (Incomplete Controller Certificate) 1255603:
Error del protocolo de enlace SSL (SSL Handshake Failure) 1255604: Conexión rechazada (Connection
Refused) 1255605: Tiempo de espera activo (Keep-alive Timeout) 1255606: Excepción de SSL (SSL
Exception) 1255607: Mensaje incorrecto (Bad Message) 1255620: Error desconocido (Unknown Error)
```

- 2 Determine el motivo por el que el agente de plano de control está inactivo como se indica a continuación:
 - a Compruebe el estado del agente de plano de control en los hosts. Para ello, ejecute el comando `/etc/init.d/netcpad status` en los hosts ESXi.

```
[root@esx-01a:~] /etc/init.d/netcpad status
netCP agent service is running
```

- b Compruebe las configuraciones del agente de plano de control con el comando `more /etc/vmware/netcpa/config-by-vsm.xml`. Las direcciones IP de las instancias de NSX Controller deben aparecer en la lista.

```
[root@esx-01a:~] more /etc/vmware/netcpa/config-by-vsm.xml
<config>
  <connectionList>
    <connection id="0000">
      <port>1234</port>
      <server>192.168.110.31</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>A5:C6:A2:B2:57:97:36:F0:7C:13:DB:64:9B:86:E6:EF:1A:7E:5C:36</thumbprint>
    </connection>
    <connection id="0001">
      <port>1234</port>
      <server>192.168.110.32</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>12:E0:25:B2:E0:35:D7:84:90:71:CF:C7:53:97:FD:96:EE:ED:7C:DD</thumbprint>
    </connection>
    <connection id="0002">
      <port>1234</port>
      <server>192.168.110.33</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>BD:DB:BA:B0:DC:61:AD:94:C6:0F:7E:F5:80:19:44:51:BA:90:2C:8D</thumbprint>
    </connection>
  </connectionList>
  ...
```

- 3 Valide las conexiones a los controladores desde el agente de panel de control con el siguiente comando. El resultado es una conexión para cada controlador.

```
>[root@esx-01a:~] esxcli network ip connection list | grep 1234
tcp      0  0  192.168.110.51:16594      192.168.110.31:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0  0  192.168.110.51:46917      192.168.110.33:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0  0  192.168.110.51:47891      192.168.110.32:1234      ESTABLISHED      36752  newreno
netcpa-worker
```

- 4 Valide las conexiones a los controladores desde el agente de panel de control para mostrar los estados CLOSED o CLOSE_WAIT. Para ello, utilice el siguiente comando:

```
esxcli network ip
  connection list |grep "1234.*netcpa*" | egrep "CLOSED|CLOSE_WAIT"
```

- 5 Si el agente de plano de control lleva inactivo mucho tiempo, es posible que las conexiones no aparezcan. Para validarlas, ejecute el siguiente comando. El resultado es una conexión para cada controlador.

```
esxcli network ip
connection list |grep "1234.*netcpa*" |grep ESTABLISHED
```

- 6 Mecanismo de recuperación automática del agente de plano de control (netcpa): el proceso de supervisión automático del agente de plano de control detecta que el estado es incorrecto. Cuando el estado del agente de plano de control es incorrecto, este deja de responder e intenta recuperarse automáticamente.

- a Si el agente de plano de control deja de responder, se genera un archivo de núcleo activo. Puede encontrar el archivo de núcleo de la siguiente forma:

```
ls /var/core
netcpa-worker-zdump.000
```

- b Se notifica un error de syslog en el archivo *vmkwarning.log*.

```
cat /var/run/log/vmkwarning.log | grep NETCPA
2017-08-11T06:32:17.994Z cpu1:1000044539)ALERT: Critical - NETCPA is hanged
Taking live-dump & restarting netcpa process!
```

Nota Si el mecanismo de supervisión del agente de panel de control experimenta un error temporal debido a un retraso en la respuesta a la comprobación de estado, es posible que se muestre un mensaje de advertencia parecido al siguiente en los registros de VMKernel.

Advertencia: Error de NETCPA al obtener el estado de netcpa.

Puede ignorar esta advertencia.

- 7 Si el problema no se soluciona automáticamente, reinicie el agente de panel de control de la siguiente forma:
 - a Inicie sesión como usuario raíz en el host ESXi a través de SSH o de la consola.
 - b Ejecute el comando `/etc/init.d/netcpad restart` para reiniciar el agente de panel de control en el host ESXi.

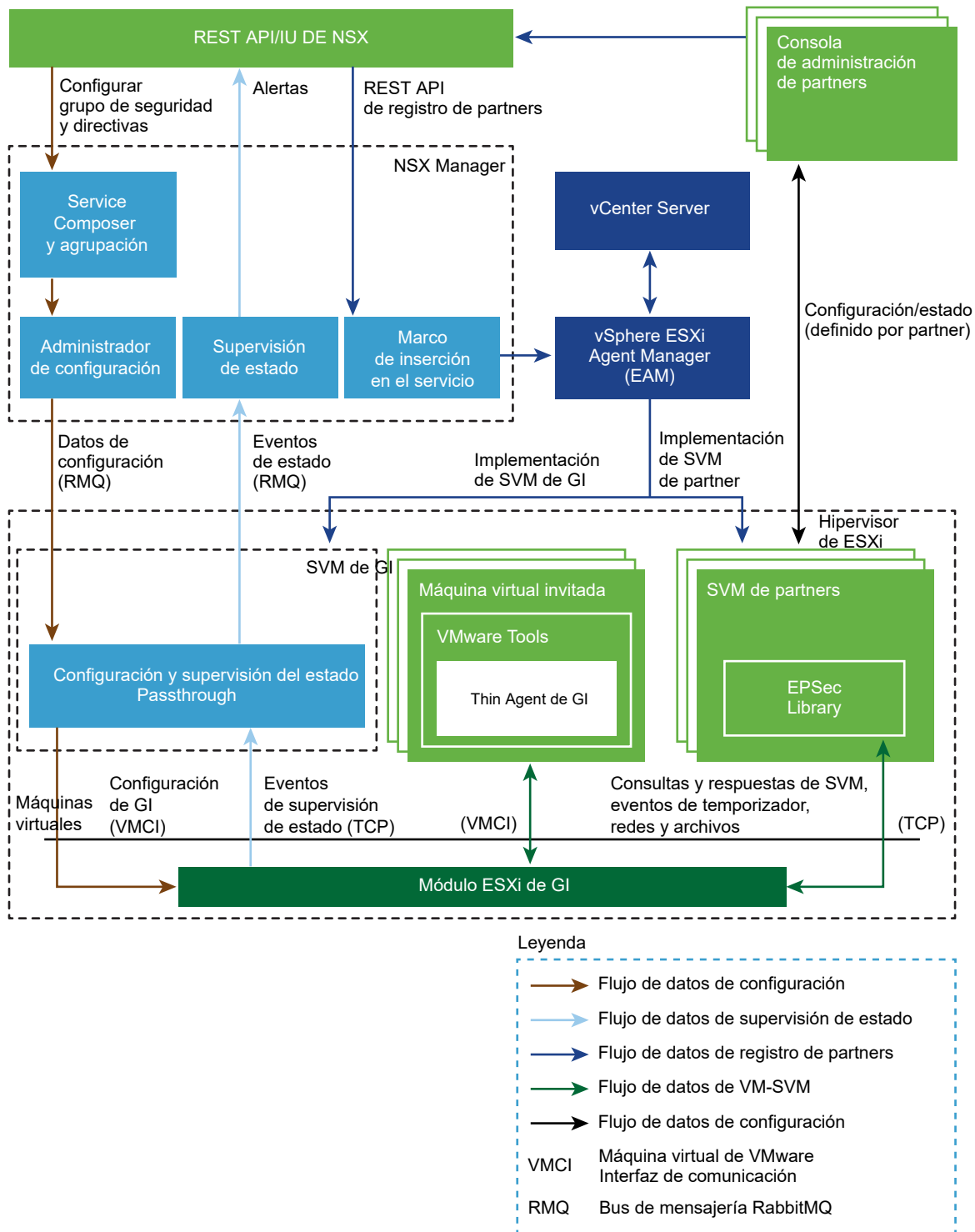
Solucionar problemas de Guest Introspection

9

Este capítulo incluye los siguientes temas:

- [Arquitectura de Guest Introspection](#)
- [Registros de Guest Introspection](#)
- [Recopilar información de trabajo y del entorno de Guest Introspection](#)
- [Solucionar problemas de Thin Agent en Linux o Windows](#)
- [Solucionar problemas del módulo GI de ESX \(MUX\)](#)
- [Solucionar problemas de EPSecLib](#)

Arquitectura de Guest Introspection



Registros de Guest Introspection

Existen diferentes registros que puede capturar para usarlos mientras soluciona problemas de Guest Introspection.

Registros del módulo de GI de ESX (MUX)

Si las máquinas virtuales de un host ESXi no funcionan con Guest Introspection o si existen alarmas en un host referentes a la comunicación con SVA, podría producirse un problema con el módulo GI de ESX en el host ESXi.

Ruta de acceso a registros y mensaje de muestra

Ruta de acceso a registros MUX

/var/log/syslog

var/run/syslog.log

Los mensajes del módulo GI de ESX (MUX) siguen el formato:

<marcadetiempo>EPsecMUX<[IDdesubproceso]>: <mensaje>

Por ejemplo:

```
2017-07-16T05:44:49Z EPsecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

En el ejemplo anterior,

- [ERROR] es el tipo de mensaje. Otros tipos pueden ser [DEPURACIÓN] (DEBUG) o [INFO].
- (EPSEC) significa que los mensajes son específicos para Endpoint Security.

Habilitar y consultar archivos de registro

Para consultar la versión del VIB instalado en el módulo GI de ESX, ejecute el comando `#esxcli software vib list | grep epsec-mux`.

Para activar el registro completo, realice estos pasos en el shell del comando del host ESXi:

- 1 Ejecute el comando de Mux `ps -c | grep` para encontrar los procesos del módulo GI de ESX que se están ejecutando en ese momento.

Por ejemplo:

```
~ # ps -c | grep Mux
192223 192223 sh /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t 1000000 /usr/lib/
vmware/vShield-Endpoint-Mux 900 -c 910
192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
```

- 2 Si el servicio no se está ejecutando, puede reiniciarlo con estos comandos: `/etc/init.d/vShield-Endpoint-Mux start` o `/etc//init.d/vShield-Endpoint-Mux restart`.
- 3 Para detener los procesos del módulo GI de ESX, incluido el proceso `watchdog.sh`, ejecute el comando `~ # kill -9 192223 192233 192236`.

Tenga en cuenta que se generan dos procesos del módulo GI de ESX.

- 4 Inicie un módulo GI de ESX con una nueva opción de `-d`. Tenga en cuenta que la opción `-d` no existe para las compilaciones de `epsec-mux 5.1.0-01255202` y `5.1.0-01814505` ~ # `/usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910`.
- 5 Consulte los mensajes de error del módulo GI de ESX en el archivo `/var/log/syslog.log` del host ESXi. Compruebe que las entradas correspondientes a las soluciones globales, al ID de la solución y al número de puerto estén especificadas correctamente.

Ejemplo: Archivo `muxconfig.xml` de ejemplo

```
<?xml version="1.0" encoding="UTF-8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371-3630-47b0-8796-f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/EndpointService (216)/EndpointService (216).vmx</vmxPath>

    </Solution>

    <Solution>

      <id>102</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48651</port>

      <uuid>423839c4-c7d6-e92e-b552-79870da05291</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/apoon/EndpointSVM-alpha-01/EndpointSVM-alpha-01.vmx</vmxPath>

    </Solution>

    <Solution>

      <id>6341068275337723904</id>
```

```

<ipAddress>xxx.xxx.xxx.xxx</ipAddress>

<listenOn>ip</listenOn>

<port>48655</port>

<uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>

<vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>

</Solution>

</InstalledSolutions>

<DefaultSolutions/>

<GlobalSolutions>

  <solution>

    <id>100</id>

    <tag></tag>

    <order>0</order>

  </solution>

  <solution>

    <id>102</id>

    <tag></tag>

    <order>10000</order>

  </solution>

  <solution>

    <id>6341068275337723904</id>

    <tag></tag>

    <order>10001</order>

  </solution>

</GlobalSolutions>

</EndpointConfig>

```

Registros de Thin Agent de GI

Thin Agent está instalado en el SO invitado de la máquina virtual y detecta la información de la sesión del usuario.

Ruta de acceso a registros y mensaje de muestra

Thin Agent consta de controladores de GI: vsepflt.sys, vnetflt.sys, vnetwfp.sys (Windows 10 y versiones posteriores).

Los registros de Thin Agent se encuentran en el host ESXi y forman parte del paquete de registros de vCenter. La ruta de acceso a los registros es /vmfs/volumes/<almacén de datos>/<nombre de máquina virtual>/vmware.log. Por ejemplo: /vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log.

Los mensajes de Thin Agent siguen el formato <marcador de tiempo> <Nombre de máquina virtual><Nombre de proceso>[<PID>]: <mensaje>.

En el ejemplo de registro que aparece a continuación, Guest: vnet or Guest:vsep indica los mensajes de registro relacionados con los respectivos controladores de GI, seguidos por los mensajes de depuración.

Por ejemplo:

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

Ejemplo: Habilitar el registro de los controladores de Thin Agent de vShield Guest Introspection

Como la opción de depuración puede saturar el archivo vmware.log hasta el punto de reducir el flujo de tráfico, le recomendamos que deshabilite el modo de depuración tras recopilar toda la información necesaria.

Este procedimiento requiere que modifique el Registro de Windows. Antes de modificar el registro, realice una copia de seguridad de este. Para obtener más información sobre cómo realizar la copia de seguridad de registro y restablecerlo, consulte el artículo [136393](#) de Microsoft Knowledge Base.

Siga estos pasos para habilitar el registro de depuración del controlador de Thin Agent:

- 1 Haga clic en **Inicio > Ejecutar** (Start > Run). Escriba `regedit` y haga clic en **Aceptar** (OK). Se abre la ventana Editor del Registro. Para obtener más información, consulte el artículo [256986](#) de Microsoft Knowledge Base.
- 2 Cree esta clave con el Editor del Registro: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt\parameters`.
- 3 En la clave de parámetros creada recientemente, cree estos DWORD. Asegúrese de que el formato hexadecimal esté seleccionado cuando introduzca estos valores:

```
Name: log_dest
Type: DWORD
Value: 0x2

Name: log_level
Type: DWORD
Value: 0x10
```

Otros valores para la clave del parámetro `log_level`:

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

- 4 Abra un símbolo del sistema como administrador. Ejecute estos comandos para descargar y volver a cargar el minicontrolador del sistema de archivos de vShield Endpoint:

- `fltmc unload vsepflt`
- `fltmc load vsepflt`

Puede encontrar las entradas de registro en el archivo `vmware.log` de la máquina virtual.

Habilitar el registro de los controladores de introspección de red de vShield GI

Como la opción de depuración puede saturar el archivo `vmware.log` hasta el punto de reducir el flujo de tráfico, le recomendamos que deshabilite el modo de depuración tras recopilar toda la información necesaria.

Este procedimiento requiere que modifique el Registro de Windows. Antes de modificar el registro, realice una copia de seguridad de este. Para obtener más información sobre cómo realizar la copia de seguridad de registro y restablecerlo, consulte el artículo [136393](#) de Microsoft Knowledge Base.

- 1 Haga clic en **Iniciar > Ejecutar** (Start > Run). Escriba `regedit` y haga clic en **Aceptar** (OK). Se abre la ventana Editor del Registro. Para obtener más información, consulte el artículo [256986](#) de Microsoft Knowledge Base.

2 Editar el registro:

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest" = DWORD: 0x00000001
```

3 Reinicie la máquina virtual.

Ubicación de los archivos de registro vsepflt.sys y vnetflt.sys

Si se establece la configuración de registro `log_dest` en `DWORD: 0x00000001`, el controlador Thin Agent de Endpoint inicia sesión en el depurador. Ejecute el depurador (DbgView desde SysInternals o windbg) para capturar la salida del proceso.

También puede establecer la configuración de registro `log_dest` en `DWORD:0x000000002`. En este caso, los registros del controlador se escribirán en un archivo `vmware.log`, que se encuentra en la carpeta de la máquina virtual correspondiente del host ESXi.

Habilitar el registro UMC

El componente del modo de usuario (UMC) de Guest Introspection se ejecuta en el servicio VMware Tools de la máquina virtual protegida.

- 1 En Windows XP y Windows Server 2003, cree un archivo `tools config` si no existe en la siguiente ruta: `C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf`.
- 2 En Windows Vista, Windows 7 y Windows Server 2008, cree un archivo `tools config` si no existe en la siguiente ruta: `C:\ProgramData\VMware\VMware Tools\tools.conf`.
- 3 Agregue estas líneas en el archivo `tools.conf` para habilitar el registro del componente UMC.

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

Con la opción `vsep.handler = vmx`, el componente UMC se registra en el archivo `vmware.log`, que se encuentra en la carpeta correspondiente de la máquina virtual del host ESXi.

Con los siguientes registros de la configuración, los registros del componente UMC se escribirán en el archivo de registro especificado.

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

Registros de SVM y de EPSecLib de GI

EPSecLib recibe eventos del módulo GI de ESX (MUX) del host ESXi.

Ruta de acceso a registros y mensaje de muestra

Ruta de acceso a los registros de EPSecLib

/var/log/syslog

var/run/syslog

Los mensajes de EPSecLib siguen el formato <marcadetiempo> <Nombre de máquina virtual><Nombre de proceso><[PID]>: <mensaje>.

En el siguiente ejemplo, [ERROR] es el tipo de mensaje y (EPSEC) representa los mensajes específicos para Guest Introspection.

Por ejemplo:

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
[7203] Initializing EPSec library build: build-000000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

Recopilar registros

Siga estos pasos si desea habilitar el registro de depuración de EPSec Library, que se trata de un componente de la SVM de GI:

- 1 Inicie sesión en la SVM de GI con la contraseña de la consola que proporciona NSX Manager.
- 2 Cree el archivo /etc/epseclib.conf y agregue:

```
ENABLE_DEBUG=TRUE
```

```
ENABLE_SUPPORT=TRUE
```

- 3 Cambie los permisos ejecutando el comando `chmod 644 /etc/epseclib.conf`.
- 4 Reinicie el proceso GI-SVM ejecutando el comando `/usr/local/sbin/rcusvm restart`.

Esta acción habilita el registro de depuración para EPSecLib en la SVM de GI y dichos registros se almacenan en /var/log/messages. Estos registros se aplican a NSX for vSphere 6.2.x y 6.3.x. Como la opción de depuración puede saturar el archivo vmware.log hasta el punto de reducir el flujo de tráfico, le recomendamos que deshabilite el modo de depuración tras recopilar toda la información necesaria.

Registros de SVM de GI

Antes de capturar los registros, determine el ID o el MOID del host:

- Ejecute los comandos `show cluster all` y `show cluster <cluster ID>` en NSX Manager.

Por ejemplo:

```
nsxmgr-01a> show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	RegionA01-COMP01	domain-c26	RegionA01	Enabled
2	RegionA01-MGMT01	domain-c71	RegionA01	Enabled

```
nsxmgr-01a> show cluster domain-c26
```

Datacenter: RegionA01
Cluster: RegionA01-COMP01

No.	Host Name	Host Id	Installation Status
1	esx-01a.corp.local	host-29	Ready
2	esx-02a.corp.local	host-31	Ready

- 1 Para determinar el estado actual del registro, ejecute este comando:

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm
```

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/root
```

- 2 Para cambiar el estado actual del registro, ejecute este comando:

```
POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel
```

```
## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>
```

- 3 Para generar registros, ejecute este comando:

```
GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs
```

Seleccione Send y Download.

Tenga en cuenta que este comando genera registros de SVM de GI y guarda el archivo como techsupportlogs.log.gz. Como la opción de depuración puede saturar el archivo vmware.log hasta el punto de reducir el flujo de tráfico, le recomendamos que deshabilite el modo de depuración tras recopilar toda la información necesaria.

Recopilar información de trabajo y del entorno de Guest Introspection

Recopilar la información del entorno es de utilidad cuando se comprueba la compatibilidad de los componentes.

- 1 Determine si se usa NSX Guest Introspection en el entorno del cliente. Si no es así, elimine el servicio de Guest Introspection de la máquina virtual y confirme que el problema está resuelto.
- 2 Recopile información sobre el entorno:
 - a Versión de compilación de ESXi: ejecute el comando `uname -a` en el host ESXi o haga clic en un host de vSphere Web Client y busque el número de compilación situado en la parte superior del panel derecho.
 - b Número de compilación y versión del producto de Linux
 - c `/usr/sbin/vsep -v` proporcionará la versión de producción

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

- 3 Versión de VMware NSX ® for vSphere ® y lo siguiente:
 - Número de la versión y nombre de la solución del partner
 - Número de la versión de EPsec Library que usa la solución del partner. Inicie sesión en la SVM de GI y ejecute la ruta `#strings a EPsec library/libEPsec.so | grep BUILD`
 - Sistema operativo invitado en la máquina virtual
 - Cualquier otra aplicación externa o controladores del sistema de archivo
- 4 Versión del módulo de GI de ESX (MUX). Ejecute el software `vib list | grep epsec-mux` del comando `esxcli`.
- 5 Recopile la información sobre la carga de trabajo, como el tipo de servidor.
- 6 Recopile los registros del host ESXi. Para obtener más información, consulte [cómo recopilar información de diagnóstico para VMware ESX/ESXi \(653\)](#).
- 7 Recopile registros de la máquina virtual de servicio (SVM de GI) desde la solución del partner. Póngase en contacto con su partner para obtener más información sobre la recopilación de registros de SVM de GI.
- 8 Recopile un archivo de estado suspendido mientras se produce el problema y consulte el artículo sobre [cómo suspender una máquina virtual en ESX/ESXi \(2005831\)](#) para recopilar información de diagnóstico.

- Después de recopilar la fecha, compare la compatibilidad de los componentes de vSphere. Para obtener más información, consulte las [Matrices de interoperabilidad de productos de VMware](#).

Solucionar problemas de Thin Agent en Linux o Windows

Thin Agent de Guest Introspection se instala con VMware Tools™ en cada máquina virtual invitada.

Solucionar problemas de Thin Agent en Linux

Si una máquina virtual tarda en leer y escribir operaciones, así como al descomprimir o guardar archivos, es posible que exista algún problema con Thin Agent.

- Compruebe la compatibilidad de todos los componentes involucrados. La compatibilidad es uno de los problemas principales de Endpoint. Necesita los números de compilación de ESXi, vCenter Server, NSX Manager y la solución de seguridad que eligió (Trend Micro, McAfee, Kaspersky y Symantec, entre otros). Después de recopilar estos datos, compare la compatibilidad de los componentes de vSphere. Para obtener más información, consulte las [Matrices de interoperabilidad de productos de VMware](#).
- Asegúrese de que la introspección de archivos esté instalada en el sistema.
- Utilice el comando `service vsep status` para comprobar que Thin Agent se esté ejecutando. Después de ejecutar este comando, el servicio vsep debe aparecer en ejecución.
- Si cree que Thin Agent está causando un problema de rendimiento en el sistema, detenga el servicio ejecutando el comando `service vsep stop`.
- A continuación, realice una prueba para obtener un valor de referencia. Después, podrá iniciar el servicio vsep y ejecutar otra prueba con el comando `service vsep start`.
- Habilite la depuración de Thin Agent de Linux:
 - Abra el archivo `/etc/vsep/vsep.conf`
 - Cambie `DEBUG_LEVEL=4` a `DEBUG_LEVEL=7` en todos los registros
 - Se puede establecer en `DEBUG_LEVEL=6` para registros moderados
 - El destino de registro predeterminado (`DEBUG_DEST=2`) es `vmware.log` (en el host), para cambiarlo a invitado (es decir, `/var/log/message` o `/var/log/syslog`) establezca `DEBUG_DEST=1`

Nota Habilitar el registro completo puede provocar que una elevada actividad de registro sature el archivo `vmware.log`, lo cual hace que crezca hasta alcanzar un gran tamaño. Deshabilite el registro cuanto antes.

Solucionar problemas de Thin Agent en Windows

- 1 Compruebe la compatibilidad de todos los componentes involucrados. Necesita los números de compilación de ESXi, vCenter Server, NSX Manager y la solución de seguridad que eligió (Trend Micro, McAfee, Kaspersky y Symantec, entre otros). Después de recopilar todos los datos, puede comparar la compatibilidad de los componentes de vSphere. Para obtener más información, consulte las [Matrices de interoperabilidad de productos de VMware](#).
- 2 Asegúrese de que la utilidad VMware Tools™ esté actualizada. Si observa que únicamente está afectada una máquina virtual en particular, consulte el [artículo 2004754 sobre cómo instalar y actualizar VMware Tools en vSphere](#).
- 3 Verifique que Thin Agent se carga al ejecutar el comando `fltmc` de Powershell.

Después de ejecutar este comando, debe aparecer el nombre `vsepflt` en la lista de controladores. Si el controlador no se carga, debe hacerlo con el comando `fltmc load vsepflt`.
- 4 Si Thin Agent está causando un problema de rendimiento en el sistema, descargue el controlador con este comando: `fltmc unload vsepflt`.

A continuación, realice una prueba para obtener un valor de referencia. Luego puede cargar el controlador y realizar otra prueba con este comando:

`fltmc load vsepflt`.

Si existe un problema de rendimiento con Thin Agent, consulte el [artículo 2144236 sobre máquinas virtuales lentas tras actualizar VMware Tools en NSX y vCloud Networking and Security](#).
- 5 Si no está utilizando la introspección de red, elimine o deshabilite este controlador.

También la puede eliminar mediante el instalador para modificar VMware Tools:
 - a Monte el instalador de VMware Tools.
 - b Acceda a **Panel de control > Programas y características**.
 - c Haga clic con el botón secundario en **VMware Tools > Cambiar**.
 - d Seleccione **Instalación completa**.
 - e Busque la introspección de archivos de NSX. Debe haber una carpeta secundaria para la introspección de red.
 - f Deshabilite **Introspección de red** (Network Introspection).
 - g Reinicie la máquina virtual para completar la desinstalación del controlador.
- 6 Habilite el registro de depuración de Thin Agent. Para obtener más información, consulte [Registros de Guest Introspection](#). Toda la información de depuración está configurada para que se registre en el archivo `vmware.log` de esa máquina virtual.
- 7 Revise los análisis de los archivos de Thin Agent consultando los registros `procmon`. Para obtener más información, consulte el [artículo 2094239 sobre cómo solucionar problemas de rendimiento de vShield Endpoint con un software antivirus](#).

Recopilar información de la carga de trabajo y del entorno

- 1 Determine si se usa NSX Guest Introspection en el entorno del cliente. Si no es así, elimine el servicio de Guest Introspection de la máquina virtual y confirme que el problema está resuelto. Solucione el problema de Guest Introspection solo si esta función es necesaria.
- 2 Recopile información sobre el entorno:
 - a Versión de compilación de ESXi: ejecute el comando `uname -a` en el host ESXi o haga clic en un host de vSphere Web Client y busque el número de compilación situado en la parte superior del panel derecho.
 - b Número de compilación y versión del producto de Linux
 - c `/usr/sbin/vsep -v` proporcionará la versión de producción

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

- 3 Versión de VMware NSX® for vSphere® y lo siguiente:
 - Número de la versión y nombre de la solución del partner
 - Número de la versión de EPsec Library que usa la solución del partner. Inicie sesión en la SVM y ejecute la ruta `#strings a EPsec library/libEPsec.so | grep BUILD`
 - Sistema operativo invitado en la máquina virtual
 - Cualquier otra aplicación externa o controladores del sistema de archivo
- 4 Versión del módulo GI de ESX (MUX): ejecute el comando `esxcli software vib list | grep epsec-mux`.
- 5 Recopile la información sobre la carga de trabajo, como el tipo de servidor.
- 6 Recopile los registros del host ESXi. Para obtener más información, consulte [cómo recopilar información de diagnóstico para VMware ESX/ESXi \(653\)](#).
- 7 Recopile los registros de la máquina virtual de servicio (SVM) desde la solución del partner. Póngase en contacto con su partner para obtener más información sobre la recopilación de registros de SVM.
- 8 Recopile un archivo de estado suspendido mientras se produce el problema y consulte el artículo sobre [cómo suspender una máquina virtual en ESX/ESXi \(2005831\)](#) para recopilar información de diagnóstico.

Solucionar bloqueos de Thin Agent

Si se bloquea Thin Agent, se genera el archivo de núcleo en `/directory`. Recopile el archivo (núcleo) del volcado de núcleo de `location / directory`. Utilice el comando `file` para comprobar si `vsep` genera el núcleo. Por ejemplo:

```
# file core
core: ELF 64-bit LSB core file x86-64, version 1 (SYSV), SVR4-style, from '/usr/sbin/vsep'
```

La máquina virtual se bloquea

Recopile el archivo `vmss` de VMware de la máquina virtual en estado de suspensión, consulte el [artículo 2005831 sobre cómo suspender una máquina virtual en ESX/ESXi para recopilar información de diagnóstico](#) o bloquee la máquina virtual y recopile el archivo de volcado de memoria completo. VMware ofrece una utilidad para convertir un archivo `vmss` de ESXi en un archivo de volcado de núcleo. Consulte [Vmss2core fling](#) para obtener más información.

Solucionar problemas del módulo GI de ESX (MUX)

Módulo GI de ESX (MUX)

Si las máquinas virtuales de un host ESXi no funcionan con Guest Introspection o si existen alarmas en un host concreto en cuanto a la comunicación con SVA de GI, podría existir un problema con el módulo GI de ESX en el host ESXi.

- 1 Compruebe que el servicio se esté ejecutando en el host ESXi con el comando `# /etc/init.d/vShield-Endpoint-Mux status`:

Por ejemplo:

```
# /etc/init.d/vShield-Endpoint-Mux status
vShield-Endpoint-Mux is running
```

- 2 Si el servicio no se está ejecutando, puede iniciarlo o reiniciarlo con este comando:

```
/etc/init.d/vShield-Endpoint-Mux start
```

o

```
/etc/init.d/vShield-Endpoint-Mux restart
```

Tenga en cuenta que es más seguro reiniciar este servicio durante las horas de producción, ya que su impacto será menor y se reinicia en unos segundos.

- 3 Para saber los procesos del módulo GI de ESX que se están llevando a cabo o para comprobar el estado de la comunicación, puede consultar los registros del host ESXi. Los registros del módulo GI de ESX se escriben en el archivo `/var/log/syslog`. Esto también se incluye en los registros del soporte técnico del host ESXi.

Para obtener más información, consulte el [artículo 2032892 sobre cómo recopilar la información de diagnóstico para los hosts ESXi/ESX y vCenter Server usando vSphere Web Client](#).

- 4 La opción de registro predeterminada para el módulo GI de ESX es info y se puede utilizar como método de depuración para obtener más información:

Para obtener más información, consulte [Registros de Guest Introspection](#).

- 5 También se pueden solucionar muchos problemas reinstalando el módulo GI de ESX, especialmente si está instalada una versión errónea o se utiliza el host ESXi en un entorno que ya tenía instalado Endpoint. Debe eliminarlo y volverlo a instalar.

Para eliminar VIB, ejecute este comando: `esxcli software vib remove -n epsec-mux`

- 6 Si aparecen problemas con la instalación del VIB, consulte el archivo `/var/log/esxupdate.log` del host ESXi. Este registro explica claramente por qué el controlador no se instaló correctamente. Este es un problema común de la instalación del módulo GI de ESX. Para obtener más información, consulte el [artículo 2135278 sobre los errores al instalar los servicios de NSX Guest Introspection \(VIB del módulo GI de ESX\) del host ESXi en VMware NSX for vSphere 6.x](#).

- 7 Para comprobar si existe una imagen dañada de ESXi, busque un mensaje similar al siguiente:

```
esxupdate: esxupdate: ERROR: Installation Error:
(None, 'No image profile is found on the host or image profile is empty.
An image profile is required to install or remove VIBs. To install an image profile,
use the esxcli image profile install command.')
```

- 8 Para verificar que la imagen esté dañada, ejecute el comando `cd /vmfs/volumes` en el host ESXi.

- a Busque el archivo `imgdb.tgz` con el siguiente comando: `find * | grep imgdb.tgz`.

Este comando suele dar como resultado dos coincidencias. Por ejemplo:

```
0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz o edbf587b-da2add08-3185-3113649d5262/
imgdb.tgz
```

- b En cada coincidencia, ejecute el siguiente comando: `ls -l match_result`

Por ejemplo:

```
> ls -l 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz -rwx-----
1 root root 26393 Jul 20 19:28 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz
> ls -l edbf587b-da2add08-3185-3113649d5262/imgdb.tgz -rwx-----
1 root root 93 Jul 19 17:32 edbf587b-da2add08-3185-3113649d5262/imgdb.tgz
```

El tamaño predeterminado del archivo `imgdb.tgz` es mucho mayor que el otro archivo. Si uno de los archivos tiene pocos bytes, esto indica que el archivo está dañado. La única forma admitida de solucionar esta situación es volver a instalar ESXi en ese host ESXi en concreto.

Solucionar problemas de EPSecLib

NSX Manager controla la implementación de esta máquina virtual.

EPSecLib

Antes (con vShield), la solución SVA de terceros controlaba la implementación. Esa solución se conecta ahora a NSX Manager. NSX Manager controla la implementación de esta SVA. Si existen alarmas de las SVA del entorno, vuelva a implementarlas mediante NSX Manager.

- Todas las configuraciones se pierden, ya que se almacenan en NSX Manager.
- Es mejor volver a implementar las máquinas virtuales de SVA que reiniciarlas.
- NSX se basa en EAM para implementar y supervisar los VIB y las SVM del host, como SVA.
- EAM es la fuente de información veraz para determinar el estado de instalación.
- El estado de instalación en la interfaz de usuario (IU) de NSX solo puede notificar si los VIB están instalados o si la SVM está encendida.
- El estado del servicio en la IU de NSX indica si la funcionalidad de la máquina virtual es correcta.

Relación e implementación de SVA entre NSX y el proceso de vCenter Server

- 1 Cuando se selecciona el clúster que se preparará para Endpoint, se crea una agencia en EAM para implementar la SVA.
- 2 A continuación, EAM implementa OVF en el host ESXi con la información de la agencia que creó.
- 3 NSX Manager comprueba si EAM implementó OVF.
- 4 NSX Manager comprueba si EAM encendió la máquina virtual.
- 5 NSX Manager se comunica con el administrador de la solución SVA del partner que registró y encendió la máquina virtual.
- 6 EAM envía un evento a NSX para indicar que se completó la instalación.
- 7 El administrador de la solución SVA del partner envía un evento a NSX para indicar que el servicio que se encuentra en la máquina virtual SVA está activo y en ejecución.
- 8 Si tiene algún problema con la SVA, puede consultar dos apartados de los registros. Puede comprobar los registros de EAM, ya que EAM controla la implementación de estas máquinas virtuales. Para obtener más información, consulte el [artículo 1011641 sobre cómo recopilar información de diagnóstico para VMware vCenter Server 4.x, 5.x y 6.0](#). También puede consultar los registros de SVA.

Para obtener más información, consulte [Registros de Guest Introspection](#).

- 9 Si existe algún problema con la implementación de SVA, es posible que se produzca un problema con EAM y la comunicación con NSX Manager. Puede comprobar los registros de EAM; el proceso más sencillo que puede hacer es reiniciar el servicio EAM. Para obtener más información, consulte [Preparación del host](#).
- 10 Si todo lo anterior parece funcionar correctamente, pero prefiere probar la funcionalidad de Endpoint, hágalo con un archivo de prueba Eicar:
 - Cree un archivo de texto con cualquier etiqueta. Por ejemplo: eicar.test.

- El contenido del archivo solo debe ser la siguiente cadena:
`X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
- Guarde el archivo. Después de guardar, debería ver que el archivo se eliminó. Esto verifica que la solución Endpoint esté funcionando.