Guía de actualización de NSX

VMware NSX for vSphere 6.2

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/es/support/pubs.

ES-001878-03

vmware®

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

http://www.vmware.com/es/support/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Guía de actualización de NSX

En este manual, la *Guía de actualización de NSX*, se describe cómo actualizar el sistema VMware® NSX™ mediante vSphere Web Client. La información incluye instrucciones de actualización paso a paso y prácticas recomendadas.

Público objetivo

Este manual está destinado a quienes deseen instalar o utilizar NSX 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 con operaciones de centros de datos. Este manual da por sentado que el usuario está familiarizado con VMware vSphere 5.5 o 6.0, 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.

Leer los documentos complementarios

Además de esta guía de actualización, VMware publica distintos documentos que complementan el proceso de actualización.

Notas de la versión	Antes de comenzar la actualización a NSX 6.2.X, revise las notas de la versión. En ellas se documentan problemas de actualización conocidos y las soluciones correspondientes. Conocer los problemas de actualización antes de comenzar el proceso puede ahorrarle tiempo y esfuerzo. Consulte https://www.vmware.com/support/pubs/nsx_pubs.html.
Matriz de interoperabilidad de productos	Compruebe la interoperabilidad con otros productos de VMware, como vCenter. Consulte la matriz de interoperabilidad de productos (Product Interoperability Matrix) de VMware en la pestaña **Interoperabilidad** (Interoperability) de la página http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Compruebe la compatibilidad de la ruta de acceso de actualización de su versión actual de NSX a la versión a la cual desea actualizar. En la pestaña **Ruta de acceso de actualización** (Upgrade Path), seleccione **VMware NSX** en el menú de productos.

Guía de compatibilidad	Compruebe la compatibilidad de las soluciones de los partners con NSX en la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.
Secuencia de actualización para productos VMware	Al actualizar otros productos de VMware junto con la actualización de NSX como por ejemplo, vCenter y ESXi, es importante seguir la secuencia de actualización correcta que se documenta en el ejemplo 5 de http://kb.vmware.com/kb/2109760.

Requisitos del sistema para NSX

Antes de instalar o actualizar NSX, tenga en cuenta los recursos y la configuración de red. Puede instalar un NSX Manager por cada vCenter Server, una instancia de Guest Introspection y Data Security por cada host ESX™ y varias instancias de NSX Edge por cada centro de datos.

Hardware

Tabla 1. Requisitos de hardware

Dispositivo	Memoria	vCPU	Espacio en disco
NSX Manager	16 GB (24 GB con ciertos tamaños de implementación de NSX*)	4 GB (8 GB con ciertos tamaños de implementación de NSX*)	60 GB
NSX Controller	4 GB	4	20 GB
NSX Edge	■ Compacto: 512 MB ■ Grande: 1 GB ■ Cuádruple: 1 GB ■ Extra grande: 8 GB	■ Compacto: 1 ■ Grande: 2 ■ Tamaño cuádruple: 4 ■ Extra grande: 6	■ Compacto: 1 disco de 500 MB ■ Grande: 1 disco de 500 MB + 1 disco de 512 MB ■ Cuádruple: 1 disco de 500 MB + 1 disco de 512 MB ■ Extra grande: 1 disco de 500 MB + 1 disco de 2 GB
Guest Introspection	1 GB	2	4 GB
NSX Data Security	512 MB	1	6 GB por host ESXi

*Como instrucción general, si el entorno administrado de NSX contiene más de 256 hipervisores, es recomendable aumentar los recursos de NSX Manager a 8 vCPU y 24 GB de RAM. Para conocer los detalles de tamaño específicos, póngase en contacto con el servicio de soporte técnico de VMware.

Para obtener información sobre el aumento de la memoria y la asignación de vCPU para los dispositivos virtuales, consulte las páginas de documentación de vSphere siguientes (o las páginas equivalentes para su versión de vSphere):

- vSphere 5.5:
  - Memoria---https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-49D7217C-DB6C-41A6-86B3-7AFEB8BF575F.html

    - vCPU---https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-76FC7E9F-8037-4C8E-BEB9-91C266C1EA9A.html

- vSphere 6.0:
    - Memoria---https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-49D7217C-DB6C-41A6-86B3-7AFEB8BF575F.html
    - vCPU---https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-76FC7E9F-8037-4C8E-BEB9-91C266C1EA9A.html

Software

Para ver la información de interoperabilidad más reciente, consulte la sección sobre matrices de interoperabilidad del producto en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Estas son las versiones recomendadas de los productos de VMware.

- VMware vCenter Server 5.5U3
- VMware vCenter Server 6.0U2

IMPORTANTE: VMware vCenter Server 6.x es necesario para cross-vCenter NSX.

Tenga en cuenta que para que una instancia de NSX Manager participe en una implementación de Cross-vCenter NSX, se deben dar las condiciones siguientes:

Componente	Versión
NSX Manager	6.2 o posterior
NSX Controller	6.2 o posterior
vCenter Server	6.0 o posterior
ESXi	■ ESXi 6.0 o versiones posteriores ■ Clústeres de host que cuentan con NSX 6.2 o VIB posteriores

Para administrar todas las instancias de NSX Manager en una implementación de Cross-vCenter NSX desde una sola instancia de vSphere Web Client, debe conectar vCenter Server en Enhanced Linked Mode. Consulte la *documentación de VMware vSphere 6* https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html.

Para comprobar la compatibilidad de las soluciones de partners con NSX, consulte la Guía de compatibilidad de VMware para Networking and Security en http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Acceso de clientes y usuarios

- Si agregó hosts ESXi por nombre al inventario de vSphere, compruebe que la resolución de nombres directa o inversa está funcionando. De lo contrario, NSX Manager no puede resolver las direcciones IP.
- Permisos para agregar y encender máquinas virtuales.
- Acceda al almacén de datos en el que almacena archivos de máquina virtual y a los permisos de cuenta para copiar los archivos en ese almacén de datos.
- Cookies habilitadas en el explorador web, para acceder a la interfaz de usuario de NSX Manager.

- En NSX Manager, compruebe que se puede acceder al puerto 443 desde el host ESXi, el servidor vCenter Server y los dispositivos NSX que se implementarán. Este puerto debe descargar el archivo OVF en el host ESXi para la implementación.
- Un navegador web que sea compatible con la versión de vSphere Web Client que está utilizando. Para obtener más información, consulte la documentación sobre la *administración de vCenter Server y hosts*:
  - vSphere 5.5: https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html
  - vSphere 6.0: https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html

Puertos y protocolos requeridos por NSX

Los puertos siguientes deben estar abiertos para que NSX funcione correctamente.

Tabla 2. Puertos y protocolos requeridos por NSX

Origen	Destino	Puerto	Protocolo	Propósito	Sensible	TLS	Autenticación
PC cliente	NSX Manager	443	TCP	Interfaz administrativa de NSX Manager	No	Sí	Autenticación PAM
PC cliente	NSX Manager	80	TCP	Acceso a VIB de NSX Manager	No	No	Autenticación PAM
Host ESXi	vCenter Server	80	TCP	Preparación del host ESXi	No	No	
vCenter Server	Host ESXi	80	TCP	Preparación del host ESXi	No	No	
Host ESXi	NSX Manager	5671	TCP	RabbitMQ	No	Sí	Usuario/contraseña de Rabbit MQ
Host ESXi	NSX Controller	1234	TCP	Conexión del agente del ámbito del usuario	No	Sí	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Clúster de controladoras, sincronización de estado	No	Sí	IPsec
NSX Controller	NSX Controller	7777	TCP	Puerto RPC entre controladoras	No	Sí	IPsec
NSX Controller	NSX Controller	30865	TCP	Clúster de controladoras, sincronización de estado	No	Sí	IPsec
NSX Controller	Servidor horario NTP	123	TCP	Conexión de cliente NTP	No	Sí	Sin autenticación
NSX Manager	NSX Controller	443	TCP	Comunicación de controladora a Manager	No	Sí	Usuario/contraseña
NSX Manager	vCenter Server	443	TCP	vSphere Web Access TCP	No	Sí	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	No	Sí	

Tabla 2. Puertos y protocolos requeridos por NSX (Continua)

Origen	Destino	Puerto	Protocolo	Propósito	Sensible	TLS	Autenticación
NSX Manager	Host ESXi	443	TCP	Conexión de aprovisionamiento y administración	No	Sí	
NSX Manager	Host ESXi	902	TCP	Conexión de aprovisionamiento y administración	No	Sí	
NSX Manager	Servidor DNS	53	TCP	Conexión de cliente DNS	No	No	
NSX Manager	Servidor syslog	514	TCP	Conexión de Syslog	No	Sí	
NSX Manager	Servidor horario NTP	123	TCP	Conexión de cliente NTP	No	Sí	
vCenter Server	NSX Manager	80	TCP	Preparación del host TCP	No	Sí	
Cliente REST	NSX Manager	443	TCP	API de REST de NSX Manager	No	Sí	Usuario/contraseña
NSX Controller	Servidor horario NTP	123	UDP	Conexión de cliente NTP	No	Sí	Sin autenticación
NSX Manager	Servidor DNS	53	UDP	Conexión de cliente DNS	No	No	
NSX Manager	Servidor de Syslog	514	UDP	Conexión de Syslog	No	Sí	
NSX Manager	Servidor horario NTP	123	UDP	Conexión de cliente NTP	No	Sí	
Terminal de túnel de VXLAN (VTEP)	Terminal de túnel de VXLAN (VTEP)	8472 o 4789*	UDP	Encapsulación de red de transporte entre VTEP	No	Sí	
Host ESXi	Host ESXi	6999	UDP	ARP en LIF de VLAN	No	Sí	
Host ESXi	NSX Manager	8301, 8302	UDP	Sincronización de DVS	No	Sí	
NSX Manager	Host ESXi	8301, 8302	UDP	Sincronización de DVS	No	Sí	

*En versiones de NSX anteriores a la versión 6.2.3, el puerto VTEP predeterminado para las instalaciones nuevas era el 8472. A partir de la versión 6.2.3 de NSX, el puerto VTEP predeterminado para las instalaciones nuevas es el 4789. Las implementaciones de NSX actualizadas de una versión anterior de NSX a NSX 6.2.3 siguen utilizando el mismo puerto de forma predeterminada. Además, puede configurar un puerto personalizado.

Actualización de vCloud Networking and Security a NSX 1

Este capítulo cubre los siguientes temas:

Prepararse para actualizar vCloud Networking and Security a NSX

Para garantizar que la actualización a NSX se realice correctamente, revise las notas de la versión para comprobar si existen problemas de actualización, utilice la secuencia de actualización correcta y compruebe que la infraestructura esté preparada correctamente para la actualización. Pueden usarse las siguientes instrucciones como lista de comprobación previa a la actualización.

ADVERTENCIA: Las versiones anteriores no son compatibles:

- Realice siempre una copia de seguridad de NSX Manager antes de realizar una actualización.
- Una vez que NSX Manager se actualiza correctamente, NSX no puede volver a una versión anterior.

VMware recomienda realizar actualizaciones en una ventana de mantenimiento tal y como indica su empresa.

Pueden usarse las siguientes instrucciones como lista de comprobación previa a la actualización.

1. Compruebe que la versión de vCloud Networking and Security es la 5.5. Si no es así, consulte la *Guía de instalación y actualización de vShield* (vShield Installation and Upgrade Guide) versión 5.5 para obtener instrucciones sobre cómo realizar la actualización.
2. Compruebe que todos los puertos necesarios están abiertos. Consulte "Puertos y protocolos requeridos por NSX," página 8.
3. Compruebe que vCenter cumple los requisitos del sistema de NSX. Consulte "Requisitos del sistema para NSX," página 6.
4. Compruebe que puede recuperar la información del nombre de puerto del enlace de subida de los conmutadores distribuidos de vSphere. Consulte https://kb.vmware.com/kb/2129200.
5. Si se implementa un servicio de partners de vShield Endpoint, compruebe la compatibilidad antes de la actualización:
   - Consulte la Guía de compatibilidad de VMware para Networking and Security. Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

- Consulte la documentación del partner para obtener más detalles sobre compatibilidad y actualización.

6 Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar vShield Manager. Consulte "Desinstalar vShield Data Security," página 17.

7 Si utiliza Cisco Nexus 1000V como proveedor de conmutadores externo, debe migrar esas redes a vSphere Distributed Switch antes de realizar la actualización a NSX. Cuando NSX esté instalado, puede migrar los conmutadores distribuidos de vSphere a conmutadores lógicos.

8 Compruebe que cuenta con una copia de seguridad actualizada de Manager, vCenter y otros componentes de vCloud Networking and Security. Consulte "Copia de seguridad y restauración de vCloud Networking and Security," página 18.

9 Realice un snapshot de vShield Manager, incluida su memoria virtual. Consulte el artículo 2129224.

10 Cree un paquete de servicio técnico.

11 Asegúrese de que la resolución de nombres directa o inversa funcione utilizando el comando nslookup.

12 Si se utiliza VUM en el entorno, compruebe que a la marca bypassVumEnabled se le asigne el valor true en vCenter. Esta opción configura EAM para que instale los VIB directamente en los hosts ESXi aunque VUM esté instalado o no esté disponible. Acceda a la página http://kb.vmware.com/kb/2053782.

13 Descargue y organice el paquete de actualización, y valídelo con md5sum. Consulte "Descargar el paquete para actualizar vShield Manager a NSX y comprobar MD5," página 20.

14 Le recomendamos que desactive todas las operaciones del entorno hasta que todas las secciones de la actualización se completen.

15 No apague ni elimine ningún componente ni dispositivo de vCloud Networking and Security si no se le indica.

Necesidades de la licencia de evaluación antes de actualizar vCloud Networking and Security a NSX

Cuando actualice de vCloud Networking and Security a NSX, su licencia actual pasará a ser una licencia de NSX para vShield Endpoint.

Al iniciar NSX 6.2.3, la licencia predeterminada al completar la instalación será NSX para vShield Endpoint. Esta licencia habilita el uso de NSX para implementar y administrar vShield Endpoint solo para descarga de antivirus y tiene un cumplimiento forzado para restringir el uso de VXLAN, firewall y servicios Edge, bloqueando la preparación del host y la creación de instancias de NSX Edge.

Si ya implementó las funciones de vCloud Networking and Security, incluidos los hosts preparados, cables virtuales, vShield App o vShield Edge, estos continuarán funcionando, pero no podrá actualizarlos a NSX y no podrá realizar ningún cambio en ellos.

Si necesita otras funciones de NSX, incluidos conmutadores lógicos, enrutadores lógicos, firewall distribuido o NSX Edge, puede adquirir una licencia de NSX para utilizar dichas funciones o bien solicitar una licencia de evaluación para evaluar estas características a corto plazo.

Consulte las preguntas más recientes sobre la licencia de NSX en https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Impactos operativos de las actualizaciones de vCloud Networking and Security

El proceso de actualización de vCloud Networking and Security puede tardar algún tiempo, sobre todo al actualizar hosts ESXi, ya que se deben reiniciar los hosts. Es importante comprender el estado operativo de los componentes de vCloud Networking and Security durante una actualización, por ejemplo, cuando se han actualizado algunos hosts, pero no todos, o cuando no se han actualizado los dispositivos NSX Edge.

Para actualizar de vCloud Networking and Security a NSX 6.2.x, debe actualizar los componentes de NSX por el orden siguiente:

- vShield Manager
- Clústeres del host y cables virtuales
- vShield App
- vShield Edge
- vShield Endpoint

VMware recomienda ejecutar la actualización en una sola ventana de interrupción para minimizar el tiempo de inactividad y reducir la confusión entre los usuarios de vCloud Networking and Security que no pueden acceder a ciertas funciones de administración de vCloud Networking and Security durante la actualización. Sin embargo, si los requisitos del sitio no permiten completar la actualización en una sola ventana de interrupción, la información siguiente puede ayudar a los usuarios de vCloud Networking and Security a entender cuáles son las funciones disponibles durante la actualización.

Actualización de vCenter

Si utiliza el servicio SSO integrado de vCenter y está actualizando vCenter 5.5 a vCenter 6.0, es posible que vCenter pierda conectividad con vShield Manager. Esto ocurre si vCenter 5.5 se registró en vShield con el nombre de usuario raíz. A partir de NSX 6.2, ya no se utiliza el registro de vCenter con el nombre de usuario raíz. Como solución alternativa, vuelva a registrar vCenter en vShield con el nombre de administrator@vsphere.local en lugar de utilizar el nombre de usuario raíz.

Si utiliza un SSO externo, no es necesario realizar cambios. Puede mantener el mismo nombre de usuario, por ejemplo, admin@miempresa.midominio, y la conectividad de vCenter no se perderá.

Actualización de vShield Manager

Durante:

- La configuración de vShield Manager se bloquea. El servicio vShield API no está disponible. No pueden realizarse cambios en la configuración de vShield. La comunicación con las máquinas virtuales existentes sigue funcionando. El nuevo aprovisionamiento de máquinas virtuales continúa funcionando en vSphere, pero las nuevas máquinas virtuales no pueden conectarse con los cables virtuales de vShield durante la actualización de vShield Manager.

Después:

- Se permiten todos los cambios de configuración de vShield.

Actualización de clúster de host y cables virtuales

Como parte de la actualización del clúster de host, se instalan nuevos VIB en los hosts.

En NSX, los cables virtuales se redirigen a los conmutadores lógicos.

Durante:

- Los cambios de configuración no están bloqueados en NSX Manager.
- La actualización se realiza por clúster. Si DRS está habilitado en el clúster, se encarga de administrar el orden de actualización de los hosts.

Cuando se actualizan algunos hosts NSX en un clúster y otros no:

- No se bloquean los cambios en la configuración de NSX Manager. Se permiten cambios y modificaciones en las redes lógicas. El aprovisionamiento de máquinas virtuales sigue funcionando en los hosts que no están sometiéndose a una actualización. Los hosts que se están sometiendo a una actualización se colocan en modo de mantenimiento, por los que las máquinas virtuales deben apagarse o evacuarse a otros hosts. Esto puede realizarse con DRS o manualmente.

vShield App migró a NSX Distributed Firewall

Como parte de la actualización del clúster de host, la configuración de vShield App migra a Distributed Firewall.

Durante:

- Mientras la migración se está realizando, los filtros existentes siguen funcionando.
- No añada ni cambie filtros mientras se esté realizando la migración.

Después:

- Compruebe que todas las secciones migradas funcionan correctamente.
- Tras la migración, elimine vShield App a través de la página Implementación de servicio (Service Deployment) en NSX.

Actualización de vShield Edge

Las instancias de vShield Edge se pueden actualizar independientemente de las actualizaciones del host. Puede actualizar vShield Edge aunque aún no haya actualizado el host.

ADVERTENCIA: Si utiliza una versión de vCloud Director anterior a la 8.10, no actualice NSX Edge. Consulte "Determinar si actualizar Upgrade vShield Edge en un entorno de vCloud Director," página 52.

Durante:

- En el dispositivo de vShield Edge que se está actualizando se bloquean los cambios de configuración.
- El envío de paquetes se interrumpió temporalmente.
- Se permiten cambios y modificaciones en los conmutadores lógicos.
- El aprovisionamiento de máquinas virtuales nuevas sigue funcionando.

Después:

- No se bloquean los cambios de configuración. Todas las funciones nuevas introducidas en la actualización de NSX no se podrán configurar hasta que las instancias de NSX Controller estén instaladas y todos los clústeres del host estén actualizados a la versión 6.2.x de NSX.
- La VPN de Capa 2 se debe volver a configurar después de la actualización.
- Los clientes de VPN SSL se deben volver a instalar después de la actualización.

vShield Endpoint cambia a Guest Introspection

En NSX 6.x, vShield Endpoint se denomina Guest Introspection. Tras la actualización de NSX Manager, si se dirige a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Implementaciones de servicios (Service Deployments)** el servicio de Guest Introspection le mostrará un enlace de **Actualización** (Upgrade). Cuando se actualiza de vCloud Networking and Security a NSX, tanto el dispositivo virtual como el host de Guest Introspection se implementan en todos los hosts en el clúster en el que Guest Introspection esté habilitado.

Durante:

- Cuando se realiza un cambio en las máquinas virtuales, estas pierden protección en el clúster de NSX, por ejemplo, al realizar en ellas adiciones, vMotions o eliminaciones.

Después:

- Las máquinas virtuales están protegidas cuando se realiza en ellas adiciones, vMotions y eliminaciones.

Comprobar el estado de funcionamiento de vCloud Networking and Security

Antes de empezar la actualización, es importante probar el estado de funcionamiento de vCloud Networking and Security. De lo contrario, no podrá determinar si los problemas posteriores a la actualización ocurrieron debido al proceso de actualización o si ya existían.

No dé por sentado que todo funciona correctamente antes de empezar a actualizar la infraestructura de vCloud Networking and Security. Asegúrese de revisarla primero.

Puede usar el siguiente procedimiento para realizar una verificación antes de la actualización.

Procedimiento

1 Identifique las contraseñas y los identificadores de usuario administrador.

2 Compruebe que la resolución de nombres directa e inversa funciona en todos los componentes.

3 Compruebe que puede iniciar sesión en todos los componentes de vSphere y vShield.

4 Observe las versiones actuales de vShield Manager, vCenter Server, ESXi y vShield Edge.

5 Compruebe que los segmentos de la VXLAN funcionen.

   Asegúrese de establecer el tamaño del paquete correctamente y de incluir el bit "don't fragment" (no fragmentar).

   - Puede hacer ping entre dos máquinas virtuales que corresponden al mismo cable virtual pero están en dos hosts diferentes.
     - Desde una máquina virtual Windows: haga ping en -l 1472 –f <dest VM>
     - Desde una máquina virtual Linux: haga ping en -s 1472 –M do <dest VM>
   - Puede hacer ping entre las interfaces VTEP de dos hosts.
     - hacer ping en ++netstack=vxlan -d -s 1572 <dest VTEP IP>

     NOTA: Para obtener la dirección IP VTEP de un host, busque la dirección IP vmknicPG en la página **Administrar > Redes > Conmutadores virtuales** (Manage > Networking > Virtual Switches) del host.

6 Valide la conectividad Norte-Sur. Para ello, haga ping hacia afuera desde una máquina virtual.

7 Registre los estados de BGP y OSPF en los dispositivos NSX Edge.

8 Inspeccione visualmente el entorno de vShield para asegurarse de que todos los indicadores de estado estén en color verde, muestren una condición normal y estén implementados.

9 Compruebe que Syslog esté configurado.

10 Si es posible, en el entorno previo a la actualización, cree algunos componentes nuevos y pruebe que funcionen.

11 Valide las conexiones de agente del ámbito del usuario (UWA) netcpad y vsfwd.

   - En un host ESXi, ejecute `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` y revise el estado de conexión de la controladora.

- En vShield Manager, ejecute el comando `show tech-support save session` y busque el valor «5671» para garantizar que todos los hosts estén conectados a vShield Manager.

12 (Opcional) Si cuenta con un entorno de prueba, pruebe que funcionen las opciones de actualización y posteriores a la actualización antes de actualizar el entorno de un producto.

Migrar el usuario administrador local al usuario administrador de la interfaz de línea de comandos

Antes de la serie NSX 6.x, el usuario administrador era un usuario de base de datos local. A partir de NSX 6.0, el usuario administrador se convirtió en un usuario de la interfaz de línea de comandos. Para obtener compatibilidad con versiones anteriores, hay pasos que puede seguir para migrar el usuario administrador.

En la serie vCloud Networking and Security 5, el usuario administrador de la interfaz de línea de comandos y el usuario administrador de la interfaz de usuario (VSM) eran dos usuarios distintos. El sistema operativo administraba la contraseña del usuario administrador de la interfaz de línea de comandos, mientras que la base de datos local de usuarios administraba la contraseña del usuario de VSM. Al cambiar la contraseña del usuario administrador de la interfaz de línea de comandos, el cambio no afectaba la contraseña del usuario administrador de VSM. Del mismo modo, cuando cambiaba la contraseña del usuario administrador de VSM, el cambio no afectaba la contraseña del usuario administrador de la interfaz de línea de comandos.

En la serie NSX 6.x, se dejó de utilizar la base de datos de usuarios de VSM. El usuario de la interfaz de línea de comandos puede iniciar sesión directamente en NSX Manager.

En una situación de actualización, a fines de compatibilidad con versiones anteriores, el usuario administrador está presente en la base de datos de la interfaz de línea de comandos y en la base de datos de la interfaz de usuario web. En este caso, si se modifica la contraseña del usuario de la interfaz de línea de comandos, el cambio no se refleja en la interfaz de usuario ni en las llamadas API de REST. Antes de la serie NSX 6.x, el usuario de la interfaz de línea de comandos no podía iniciar sesión en la interfaz de usuario ni en la API REST.

En implementaciones nuevas (desde cero) de la serie NSX 6.x, el usuario de la interfaz de línea de comandos y NSX Manager (interfaz de usuario o REST) son lo mismo, y también lo son las credenciales.

Si desea que la implementación de NSX actualizada se comporte como una implementación nueva de NSX 6.x, tiene dos opciones.

- Opción 1: cambie la contraseña del usuario administrador de base de datos.

  Puede utilizar la siguiente API REST para cambiar la contraseña. Para esta opción, debe conocerse la contraseña anterior.

  PUT URI /api/2.0/services/usermgmt/user/local/<userId>

```
<userInfo>
      <userId></userId>
      <password></password>
      <fullname></fullname>
      <email></email>
      <accessControlEntry>
         <role></role>
         <resource>
             <resourceId></resourceId>
             ...
         </resource>
      </accessControlEntry>
</userInfo>
```

Por ejemplo, si se utiliza curl:

```
curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content–Type: application/xml' –X
PUT https://<vsm–ip>/api/2.0/services/usermgmt/user/local/admin –d
'<userInfo><userId>admin</userId><password>123</password><fullname>admin</fullname><email>adm
in@company.com</email><accessControlEntry><role>security_admin</role><resource><resourceId>da
tacenter–312</resourceId></resource></accessControlEntry></userInfo>'
```

Puede utilizarse la API para actualizar la cuenta de un usuario local, incluida la contraseña. Si no se proporciona una contraseña, se conserva la anterior. La variable userId en el URI debe ser igual a la especificada en XML.

- Opción 2: en lugar de conservar el usuario administrador de la interfaz de usuario web, puede eliminarlo y agregar un rol para el usuario administrador de la interfaz de línea de comandos. Después de este cambio, puede iniciar sesión en NSX Manager con las credenciales del usuario de la interfaz de línea de comandos, y un cambio en la contraseña del usuario de la interfaz de línea de comandos se reflejará en el usuario administrador de NSX Manager.

  Debido a que el usuario administrador de la interfaz de usuario web es super_user, debe agregar otro usuario con privilegios super_user para poder eliminar el usuario administrador de la interfaz de usuario web.

  - Agregue un nuevo usuario tempadmin con el rol super_user.

    Por ejemplo, si se utiliza curl:

    ```
    curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content–Type:
    application/xml' –X PUT https://<vsm–ip>/api/2.0/services/usermgmt/user/local/admin –d
    '<userInfo><userId>tempadmin</userId><password>123</password><fullname>tempadmin</fullnam
    e><email>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resourc
    e><resourceId>datacenter–312</resourceId></resource></accessControlEntry></userInfo>'
    ```

  - Utilice tempadmin para eliminar el usuario administrador de la interfaz de usuario web.

    Por ejemplo, si se utiliza curl:

    ```
    curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content–Type:
    application/xml' –X DELETE https://<vsm–ip>/api/2.0/services/usermgmt/user/admin
    ```

  - Agregue el rol super_user al usuario administrador de la interfaz de usuario web.

    Por ejemplo, si se utiliza curl:

    ```
    curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content–Type:
    application/xml' –X POST https://<nsx–ip>/api/2.0/services/usermgmt/role/admin?
    isCli=true –d '<accessControlEntry><role>super_user</role></accessControlEntry>'
    ```

Desinstalar vShield Data Security

Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar a NSX.

Desde la versión 6.2.3 de NSX, la función de seguridad de datos de NSX pasó a estar obsoleta. En la versión 6.2.3 de NSX puede seguir utilizando esta función como desee, pero tenga en cuenta que se eliminará de NSX en versiones futuras.

Procedimiento

1 En el panel del inventario de vShield Manager 5.5, expanda la carpeta de **Centros de datos** (Datacenters) y diríjase al host donde vShield Data Security está instalado.

2 En cada host en el que vShield Data Security esté instalado, complete los siguientes pasos para desinstalarlo.

   a Haga clic en el host y en la pestaña **Resumen** (Summary), en el panel Preparación del host de vShield (vShield Host Preparation), haga clic en el enlace **Desinstalar** (Uninstall) vShield Data Security.

   b En el panel Servicios que desea desinstalar (Select Services to Uninstall), compruebe que vShield Data Security está seleccionado y haga clic en el botón **Desinstalar** (Uninstall).

      vShield Data Security ya está desinstalado y el panel Preparación del host de vShield (vShield Host Preparation) aparece como `No instalado` (Not installed).

Copia de seguridad y restauración de vCloud Networking and Security

Realizar copias de seguridad apropiadas de todos los componentes de vCloud Networking and Security es crucial para restaurar el sistema a su estado de funcionamiento en caso de errores.

La copia de seguridad de vShield Manager contiene toda la configuración de vShield, incluidos los cables virtuales y las entidades de enrutamiento, la seguridad, las reglas de vApp y todo lo que configure dentro de la UPI o la API de vShield Manager. Se debe realizar una copia de seguridad por separado de la base de datos de vCenter y los elementos relacionados como por ejemplo, los conmutadores virtuales.

Recomendamos que como mínimo, realice copias de seguridad frecuentes de vShield Manager y vCenter. La frecuencia y la programación de las copias de seguridad pueden variar según las necesidades comerciales y los procedimientos operativos. Recomendamos realizar copias de seguridad de vCloud Networking and Security con frecuencia en momentos de cambios de configuración continuos.

Las copias de seguridad de vShield Manager pueden realizarse a petición o programadas a una hora, diariamente o semanalmente.

Recomendamos realizar copias de seguridad en las siguientes situaciones:

- Antes de actualizar vCloud Networking and Security o vCenter.
- Después de actualizar vCloud Networking and Security o vCenter.
- Después de una implementación desde cero y de la configuración inicial de los componentes de vCloud Networking and Security como por ejemplo, tras la creación de directivas de conmutadores virtuales, de instancias de Edge, de seguridad y de firewall.
- Después de cambios de infraestructura o topología.
- Después de cualquier cambio importante de día 2.

Para proporcionar el estado de todo un sistema al que se pueda revertir en un momento determinado, se recomienda sincronizar las copias de seguridad de los componentes de vCloud Networking and Security con la programación de copias de seguridad de otros componentes con los que exista interacción como por ejemplo, vCenter, sistemas de administración en la nube, herramientas operativas, etc.

Hacer copias de seguridad de los datos de vShield Manager a petición

Puede hacer copias de seguridad de los datos de vShield Manager en cualquier momento. Para ello, realice una copia de seguridad a petición.

Procedimiento

1 Haga clic en **Configuración e informes** (Settings & Reports) en el panel del inventario de vShield Manager.

2 Haga clic en la pestaña **Configuración** (Configuration).

3 Haga clic en **Copias de seguridad** (Backups).

4 (Opcional) Seleccione la casilla de verificación de **Excluir eventos del sistema** (Exclude System Events) si no desea hacer copias de seguridad de las tablas de eventos del sistema.

5 (Opcional) Seleccione la casilla de verificación de **Excluir registros de auditoría** (Exclude Audit Logs) si no desea hacer copias de seguridad de las tablas de registros de auditoría.

6 Escriba la **dirección IP del host** del sistema en el que se guardará la copia de seguridad.

7 Escriba el **nombre de host** del sistema de copia de seguridad.

8 Escriba el **nombre de usuario** que se solicita para iniciar sesión en el sistema de copia de seguridad.

9 Escriba la **contraseña** asociada al nombre de usuario del sistema de copia de seguridad.

10 En el campo **Directorio de copia de seguridad** (Backup Directory), escriba la ruta de acceso absoluta donde se almacenarán las copias de seguridad.

11 Escriba una cadena de texto en **Prefijo de nombre de archivo** (Filename Prefix).

Este texto se agrega antes del nombre de archivo de la copia de seguridad para que pueda reconocerlo fácilmente en el sistema de copia de seguridad. Por ejemplo, si escribe **`ppdb`**, la copia de seguridad resultante se denominará `ppdbHH_MM_SS_DayDDMonYYYY`.

12 Introduzca una **frase de contraseña** para proteger el archivo de la copia de seguridad.

En vCloud Networking and Security, la frase de contraseña es opcional. Sin embargo, en NSX es obligatoria.

13 En el menú desplegable **Protocolo de transferencia** (Transfer Protocol), seleccione **SFTP** o **FTP**.

14 Haga clic en **Copia de seguridad** (Backup).

Una vez se haya completado, la copia de seguridad aparecerá en una tabla situada debajo de estos formularios.

15 Haga clic en **Guardar configuración** (Save Settings) para guardar la configuración.

Tenga en cuenta que si todas las copias de seguridad se guardan en un solo directorio, es posible que tenga problemas al ver las copias de seguridad. Le recomendamos que mueva los archivos de las copias de seguridad a una carpeta de archivos ocasionalmente.

Hacer copias de seguridad de la configuración de CLI en ejecución de una vShield App

La opción **Configuración de CLI** (CLI Configuration) muestra la configuración que se está ejecutando de la vShield App. Puede hacer copias de seguridad de la configuración que se está ejecutando en vShield Manager para conservar la configuración.

Procedimiento

1 Inicie sesión en la interfaz de usuario de vShield Manager.

2 Seleccione una vShield App del panel del inventario.

3 Haga clic en la pestaña **Configuración** (Configuration).

4 Haga clic en **Configuración de CLI** (CLI Configuration).

5 Haga clic en **Configuración de copias de seguridad** (Backup Configuration).

La configuración se completa en el campo **Configuración de copias de seguridad** (Backup Configuration). Puede cortar este texto y pegarlo en la CLI de vShield App en el mensaje del modo de configuración.

Hacer copias de seguridad de conmutadores distribuidos de vSphere

Puede exportar la configuración de un conmutador distribuido de vSphere y de un grupo de puertos distribuidos a un archivo.

El archivo conserva los valores de red válidos, lo que permite la distribución de estos valores a otras implementaciones.

Esta funcionalidad solo está disponible con vSphere Web Client 5.1 o posterior. La configuración de VDS y la configuración del grupo de puertos se incluyen en la importación.

La práctica recomendada consiste en importar la configuración de VDS antes de preparar el clúster para VXLAN. Para obtener instrucciones detalladas, consulte http://kb.vmware.com/kb/2034602.

Hacer una copia de seguridad de vCenter

Para proteger la implementación de NSX, es importante hacer una copia de seguridad de la base de datos de vCenter y crear instantáneas de las máquinas virtuales.

Consulte la documentación de su versión de vCenter para conocer los procedimientos y las prácticas recomendadas de copias de seguridad y restauraciones de vCenter.

Para las instantáneas de máquinas virtuales, consulte http://kb.vmware.com/kb/1015180.

Vínculos útiles para vCenter 5.5:

- http://kb.vmware.com/kb/2057353
- http://kb.vmware.com/kb/2034505
- http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf

Vínculos útiles para vCenter 6.0:

- https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
- http://kb.vmware.com/kb/2110294

Descargar el paquete para actualizar vShield Manager a NSX y comprobar MD5

El paquete de actualización de vShield Manager a NSX contiene todos los archivos necesarios para actualizar la infraestructura de NSX. Antes de actualizar vShield Manager, en primer lugar debe descargar el paquete de actualización de la versión a la que desea actualizar.

Prerequisitos

Una herramienta de suma de comprobación de MD5.

Procedimiento

1. Descargue el paquete de actualización de vShield Manager a NSX en una ubicación a la que vShield Manager pueda acceder. El nombre del archivo del paquete de actualización tiene un formato similar a `VMware-vShield-Manager-upgrade-bundle-to-NSX-releaseNumber-NSXbuildNumber.tar.gz`.
2. Compruebe que el nombre del archivo de la actualización acabe en tar.gz.

   Es posible que algunos exploradores alteren la extensión del archivo. Por ejemplo, si el nombre del archivo descargado es:

   VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz

   Cámbielo a:

   VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.tar.gz

En caso contrario, después de cargar el paquete de actualización, aparecerá el siguiente mensaje de error : "Archivo no válido de paquete de actualización VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx,gz, el nombre del archivo de actualización tiene la extensión tar.gz" (Invalid upgrade bundle file VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx,gz, el nombre de archivo de actualización tiene la extensión tar.gz).

3 Utilice una herramienta de suma de comprobación MD5 para comparar la suma MD5 oficial del paquete de actualización mostrada en el sitio web de VMware con la suma MD5 calculada por la herramienta de suma de comprobación.

   a En la herramienta de suma de comprobación MD5, desplácese hasta el paquete de actualización.

   b Utilice la herramienta para calcular la suma de comprobación del paquete.

   c Pegue la suma de comprobación indicada en el sitio web de VMware.

   d Utilice la herramienta para comparar las dos sumas de comprobación.

   Si las dos sumas de comprobación no coinciden, repita la descarga del paquete de actualización.

Pasos adicionales para preparar la actualización de entornos de vCloud Director

El aislamiento de redes de vCloud Director (VCDNI) es compatible con NSX. Sin embargo, esta tecnología está obsoleta.

Antes de que VXLAN obtuviera una adopción masiva, vCloud Director se basaba en la tecnología de aislamiento de redes de vCloud para proporcionar una superposición de redes lógicas. Esta tecnología de encapsulación de propietarios MAC en MAC es aún compatible, pero la asistencia para esta tecnología ya no está disponible. A diferencia de las redes lógicas VXLAN, las redes lógicas VCDNI las crea directamente vCloud Director, que se comunica con los hosts ESXi mediante el vCloud Agent que se ejecuta en VMkernel. Por lo tanto, la actualización de vCloud Networking and Security no afectará a las redes VCDNI y se podrá utilizar con NSX sin ningún tipo de limitación.

No obstante, le recomendamos que utilice la tecnología VXLAN ya que VCDNI es una tecnología obsoleta que solo es compatible con las implementaciones heredadas.

Actualizar de vCloud Networking and Security 5.5.x a NSX 6.2.x

Para actualizar a NSX 6.2.x, debe actualizar los componentes de vCloud Networking and Security en el orden documentado en esta guía.

Los componentes de vCloud Networking and Security deben actualizarse en el siguiente orden:

1 vShield Manager a NSX Manager

2 Implementar el clúster de NSX Controller - opcional, necesario para los enrutadores lógicos (distribuidos) y para cambiar el modo del plano de control a híbrido o unidifusión

3 Actualizar clústeres y hosts

4 Actualizar la zona de transporte - opcional, si se implementa el clúster de NSX Controller, puede cambiar el modo del plano de control a híbrido o unidifusión

5 De vShield App a NSX Distributed Firewall

6 vShield Edge a NSX Edge

7 vShield Endpoint a NSX Guest Instrospection

La administración del proceso de actualización está a cargo de vShield Manager. Si ocurre un error en la actualización de un componente o si se interrumpe y es necesario repetirla o reiniciarla, el proceso empieza por el punto donde se detuvo y no desde el principio.

El estado de la actualización se actualiza en cada nodo y en el nivel del clúster.

Actualizar vShield Manager a NSX Manager

El primer paso en el proceso de actualización de la infraestructura NSX es actualizar el dispositivo NSX Manager.

ADVERTENCIA: No desinstale ninguna instancia implementada de un dispositivo de vShield Manager.

Prerequisitos

- Compruebe que completó todas las tareas de preparación de la actualización descritas en "Prepararse para actualizar vCloud Networking and Security a NSX," página 11, incluida la comprobación de los requisitos del sistema y la realización de copias de seguridad.
- Compruebe que vShield Manager disponga de suficiente espacio en disco para realizar la actualización a NSX Manager. Consulte "Requisitos del sistema para NSX," página 6.
- Aumente la memoria reservada del dispositivo virtual de vShield Manager como mínimo a 16 GB y asigne 4 vCPU antes de realizar la actualización a NSX 6.2.x.

  Consulte "Requisitos del sistema para NSX," página 6.
- Asegúrese de que las instancias de vShield Edge anteriores a la versión 5.5 (si las hay) se actualizaron a la versión 5.5 de vShield.

  Las instancias anteriores a la versión 5.5 de vShield Edge no pueden administrarse ni eliminarse una vez que vShield Manager se actualice a NSX Manager.

Procedimiento

1. Descargue el paquete de actualización de NSX en una ubicación a la que vShield Manager pueda acceder. El nombre del paquete de actualización es similar a `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`release-buildNumber`*`.tar.gz`.
2. Haga clic en **Configuración e informes** (Setting & Reports) en el panel de inventario de vShield Manager 5.5.
3. Haga clic en la pestaña **Actualizaciones** (Updates) y, a continuación, en **Subir paquete de actualizaciones** (Upload Upgrade Bundle).
4. Haga clic en **Seleccionar archivo** (Choose File), seleccione el archivo `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`releasebuildNumber`*`.tar.gz` y haga clic en **Abrir** (Open).
5. Haga clic en **Subir archivo** (Upload File).

   La subida puede tardar unos minutos.
6. Haga clic en **Instalar** (Install) para comenzar la actualización.
7. Haga clic en **Confirmar instalación** (Confirm Install). El proceso de actualización reinicia vShield Manager, por lo que puede perder conexión a la interfaz de usuario de vShield Manager. No se reinician ninguno de los demás componentes de vShield.
8. Tras el reinicio, abra una ventana del navegador para iniciar sesión en el dispositivo virtual de NSX Manager e introduzca la dirección IP, por ejemplo, https://10.10.10.10. NSX Manager actualizado tiene la misma dirección IP que vShield Manager.

   La pestaña Resumen (Summary) muestra la versión de NSX Manager que tiene instalada.
9. Acceda a **Inicio (Home) > Administrar registro de Manage vCenter (Manage vCenter Registration)** y compruebe que el estado de vCenter Server sea `Conectado` (Connected).

10 Cierre el resto de navegadores que accedan a vSphere Web Client. Espere unos minutos y limpie la caché del navegador antes de volver a iniciar sesión en vSphere Web Client.

11 Si SSH estaba habilitado en vShield Manager, debe habilitarlo en NSX Manager tras la actualización. Inicie sesión en la aplicación virtual de NSX Manager y haga clic en **Ver resumen** (View Summary). En los componentes a nivel de sistema, haga clic en **Iniciar** (Start) para comenzar el servicio SSH.

IMPORTANTE: Tras actualizar desde vCloud Networking and Security 5 a NSX 6.x, deberá usar sus credenciales administrativas de inicio de sesión de CLI para iniciar sesión en NSX Manager. Previamente, en vCloud Networking and Security eran necesarias dos contraseñas: una para la CLI y otra para la interfaz de usuario. Para iniciar NSX 6.x, solo es necesaria una contraseña. Por ejemplo:

Contraseñas de vCloud Networking and Security

- micontraseña#123 para la CLI
- micontraseña#456 para la interfaz de usuario

Contraseñas tas la actualización de NSX

- micontraseña#123 para la CLI
- micontraseña#123 para la interfaz de usuario

Después de actualizar NSX Manager y de conectarlo a una instancia de vCenter Server existente, restablezca el servidor Web Client para permitir que también se actualicen los complementos de NSX.

- También puede hacer esto en vCenter 5.5. Para ello, abra https://<vcenter-ip>:5480 y reinicie el servidor Web Client.
- Para hacerlo en vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como raíz y ejecute los comandos siguientes.

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- En vCenter Server 6.0, puede ejecutar los siguientes comandos en Windows.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Se requiere reiniciar para evitar errores inesperados, como grupos de seguridad configurados que no aparecen en la pestaña **Grupos de seguridad** (Security Groups) de Service Composer.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su navegador.

Se recomienda utilizar diferentes servidores Web Client para administrar los servidores vCenter Server que ejecutan distintas versiones de NSX Manager a fin de evitar errores inesperados cuando diferentes versiones de complementos de NSX están en ejecución.

Una vez actualizado NSX Manager, cree un nuevo archivo de copia de seguridad de NSX Manager. Consulte "Copia de seguridad y restauración de NSX," página 62. La copia de seguridad anterior de NSX Manager solo es válida para la versión anterior.

Qué hacer a continuación

"Instalar y asignar una licencia de NSX," página 24.

Instalar y asignar una licencia de NSX

Una vez finalizada la actualización de NSX Manager se puede instalar y asignar una licencia NSX for vSphere mediante vSphere Web Client.

Al iniciar NSX 6.2.3, la licencia predeterminada al completar la instalación será NSX para vShield Endpoint. Esta licencia habilita el uso de NSX para implementar y administrar vShield Endpoint solo para descarga de antivirus y tiene un cumplimiento forzado para restringir el uso de VXLAN, firewall y servicios Edge, bloqueando la preparación del host y la creación de instancias de NSX Edge.

Si necesita otras funciones de NSX, incluidos conmutadores lógicos, enrutadores lógicos, firewall distribuido o NSX Edge, puede adquirir una licencia de NSX para utilizar dichas funciones o bien solicitar una licencia de evaluación para evaluar estas características a corto plazo.

Consulte las preguntas más recientes sobre la licencia de NSX en https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Para obtener más información sobre las licencias de NSX, consulte http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

Procedimiento

- En vSphere 5.5, complete los siguientes pasos para agregar una licencia para NSX.
  a. Inicie sesión en vSphere Web Client.
  b. Haga clic en **Administración** (Administration) y, a continuación, en **Licencias** (Licenses).
  c. Haga clic en la pestaña **Soluciones** (Solutions).
  d. Seleccione NSX for vSphere en la lista Soluciones (Solutions). Haga clic en **Asignar una clave de licencia** (Assign a license key).
  e. Seleccione **Asignar una nueva clave de licencia** (Assign a new license key) en el menú desplegable.
  f. Escriba la clave de licencia y una etiqueta opcional para la nueva clave.
  g. Haga clic en **Descodificar** (Decode).

     Descodifique la clave de licencia para comprobar que tenga el formato correcto y suficiente capacidad para conceder una licencia a los activos.
  h. Haga clic en **Aceptar** (OK).
- En vSphere 6.0, complete los siguientes pasos para agregar una licencia para NSX.
  a. Inicie sesión en vSphere Web Client.
  b. Haga clic en **Administración** (Administration) y, a continuación, en **Licencias** (Licenses).
  c. Haga clic en la pestaña **Activos** (Assets) y luego en la pestaña **Soluciones** (Solutions).
  d. Seleccione NSX for vSphere en la lista Soluciones (Solutions). En el menú desplegable **Todas las acciones** (All Actions), seleccione **Asignar licencia...** (Assign license...).
  e. Haga clic en el icono **Agregar (**  **)** (Add). Introduzca la clave de licencia y haga clic en **Siguiente** (Next). Agregue un nombre para las licencias y haga clic en **Siguiente** (Next). Haga clic en **Finalizar** (Finish) para agregar la licencia.
  f. Seleccione la nueva licencia.
  g. (Opcional) Haga clic en el icono **Ver características** para ver qué características están habilitadas con esta licencia. Revise la columna de **Capacidad** para comprobar la capacidad de la licencia.
  h. Haga clic en **Aceptar** (OK) para asignar la nueva licencia a NSX.

Qué hacer a continuación

"Implementar clúster de NSX Controller," página 25.

En caso de no implementar controladoras, "Actualizar los clústeres del host," página 27

Implementar clúster de NSX Controller

NSX Controller es un sistema de administración de estado avanzado distribuido que proporciona funciones del plano de control para funciones de enrutamiento y conmutación lógicos de NSX. Sirve como punto de control central para todos los conmutadores lógicos de una red y mantiene información sobre todos los hosts, conmutadores lógicos (VXLAN) y enrutadores lógicos distribuidos. Las controladoras se requieren cuando se planean implementar 1) enrutadores lógicos distribuidos o 2) VXLAN en modo híbrido o de unidifusión.

Más allá del tamaño de la implementación de NSX, VMware requiere que cada clúster de NSX Controller tenga tres nodos de controladora. No se admite otra cantidad de nodos de controladora.

El clúster requiere que el sistema de almacenamiento en disco de cada controladora tenga una latencia de escritura máxima de menos de 300 ms y una latencia de escritura media menor a 100 ms. Si el sistema de almacenamiento no cumple estos requisitos, el clúster puede volverse inestable y provocar un tiempo de inactividad del sistema.

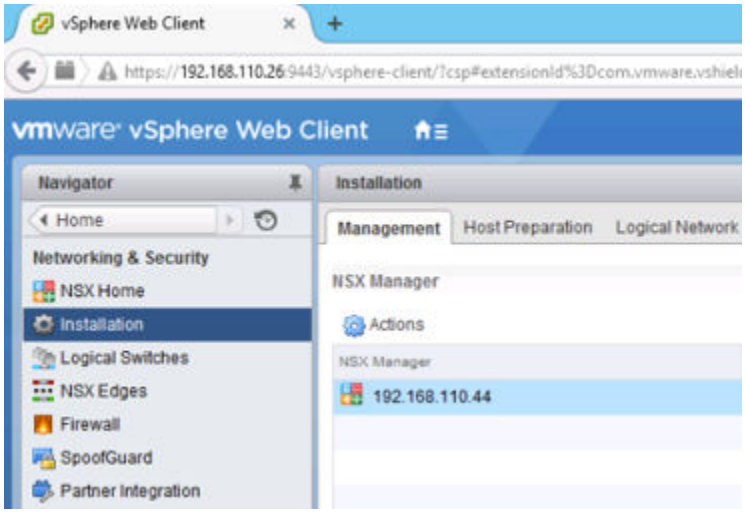
Prerequisitos

- Antes de implementar las instancias de NSX Controller, debe implementar un dispositivo NSX Manager y registrar vCenter con NSX Manager.
- Determine la configuración del grupo de direcciones IP del clúster de controladoras, incluidos la puerta de enlace y el rango de direcciones IP. La configuración de DNS es opcional. La red IP de NSX Controller debe tener conexión a NSX Manager y a las interfaces de administración de los hosts ESXi.

Procedimiento

1 En vCenter, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Administración** (Management).

Por ejemplo:

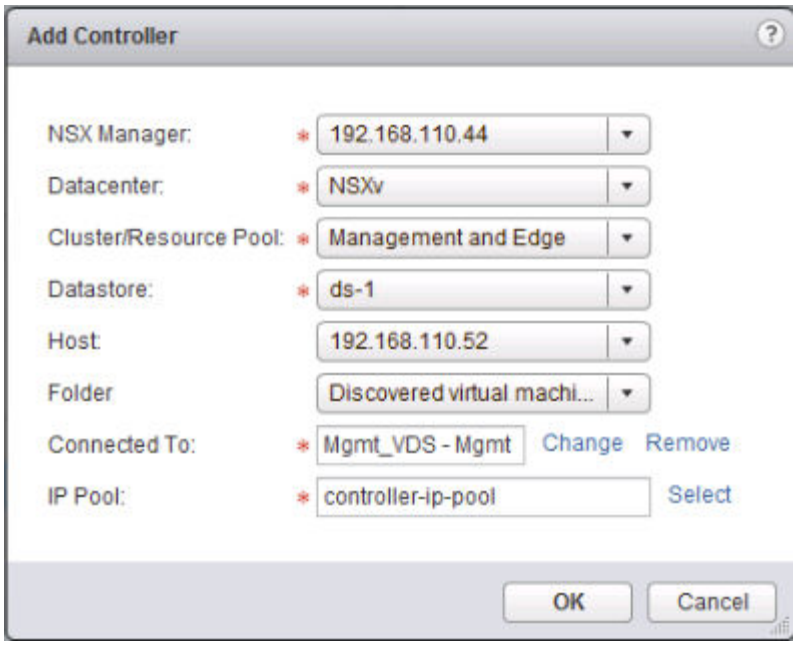


2 En la sección de nodos de NSX Controller, haga clic en el icono **Agregar nodo** (Add Node) ( ).

3 Introduzca la configuración de NSX Controller adecuada para el entorno.

Las instancias de NSX Controller deben implementarse en un grupo del puerto de vSphere Distributed Switch o de vSphere Standard Switch que no esté basado en VXLAN y que tenga conexión a NSX Manager, a otros controladores y a hosts a través de IPv4.

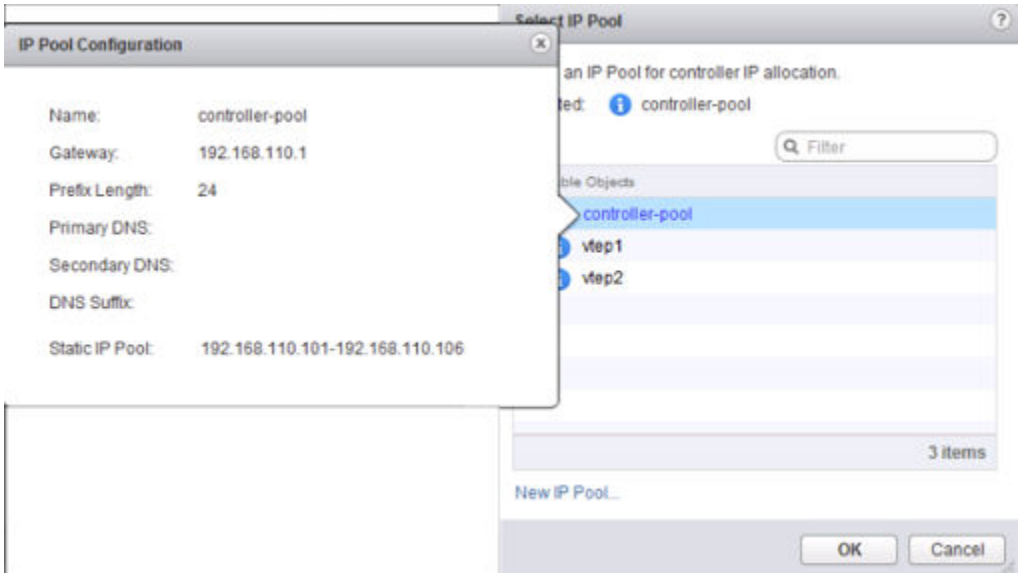
Por ejemplo:



4 Si todavía no configuró un grupo de direcciones IP para el clúster de controladoras, haga clic en **Nuevo grupo de direcciones IP** (New IP Pool) para hacerlo.

De ser necesario, las controladoras individuales pueden estar en subredes de IP distintas.

Por ejemplo:



5 Introduzca y vuelva a introducir una contraseña para la controladora.

NOTA: La contraseña no debe contener el nombre de usuario como subcadena. Los caracteres no deben repetirse 3 o más veces consecutivas.

La contraseña debe tener al menos 12 caracteres y cumplir con al menos 3 de las siguientes 4 reglas:

- Al menos una letra en mayúscula
- Al menos una letra en minúscula
- Al menos un número
- Al menos un carácter especial

6 Una vez implementada la primera controladora, implemente otras dos más.

Es obligatorio tener tres controladoras. Le recomendamos que configure una regla antiafinidad DRS para evitar que las controladoras residan en el mismo host.

Qué hacer a continuación

"Actualizar los clústeres del host," página 27

Actualizar los clústeres del host

Debe preparar su entorno para la virtualización de la red mediante la instalación de los componentes de la infraestructura de red a nivel de clúster para cada servidor vCenter. De esta forma se implementa el software necesario en todos los hosts del clúster y se vuelve a nombrar a los cables virtuales como conmutadores lógicos de NSX. Durante este proceso, se actualiza el software de cada host del clúster y, a continuación, el host se reinicia.

Se recomienda actualizar a conmutadores lógicos en una ventana de mantenimiento del centro de datos.

Si DRS está habilitado, supervise en el host el progreso de evacuación, cómo entra en el modo de mantenimiento y su reinicio. Si DRS está deshabilitada o en modo manual, las evacuaciones y los reinicios del host se deben realizar de forma manual. Durante la preparación del host, pueden aparecer advertencias que solo se verán si hace clic en el icono de advertencias, haga clic en **Resolver** (Resolve) cuando sea necesario.

Mientras se esté realizando la actualización, no implemente, actualice ni desinstale ningún servicio ni componente.

NOTA: Los VTEP que se crearon en vCloud Networking and Security no utilizan grupos de IP, sino un DHCP o direcciones IP asignadas de forma manual.

Prerequisitos

- Compruebe que vShield Manager está actualizado a NSX Manager.
- Compruebe que la columna VXLAN de la pestaña Preparación del host (Host Preparation) aparece **Habilitada** (Enabled).
- Compruebe que puedan resolverse los nombres de dominio completos (FQDN) de todos los hosts.
- Si DRS está deshabilitado, apague o transfiera por vMotion las máquinas virtuales manualmente antes de empezar la actualización.
- Si DRS está habilitado, las máquinas virtuales en ejecución se moverán automáticamente durante la actualización del clúster de hosts. Antes de iniciar la actualización, asegúrese de que DRS funcione en el entorno.
  - Compruebe que DRS esté habilitado en los clústeres del host.
  - Compruebe que vMotion funcione correctamente.

- Compruebe el estado de la conexión del host con vCenter.
- Compruebe si cuenta con tres hosts ESXi como mínimo en cada clúster de host. Durante una actualización de NSX, hay más probabilidades de que un clúster de hosts con solo uno o dos hosts presente problemas con el control de admisión de DRS. Para que la actualización de NSX funcione, VMware recomienda que cada clúster de hosts tenga al menos tres hosts. Si un clúster contiene menos de tres hosts, se recomienda evacuarlos manualmente.

Procedimiento

1 Inicie sesión en vSphere Web Client.

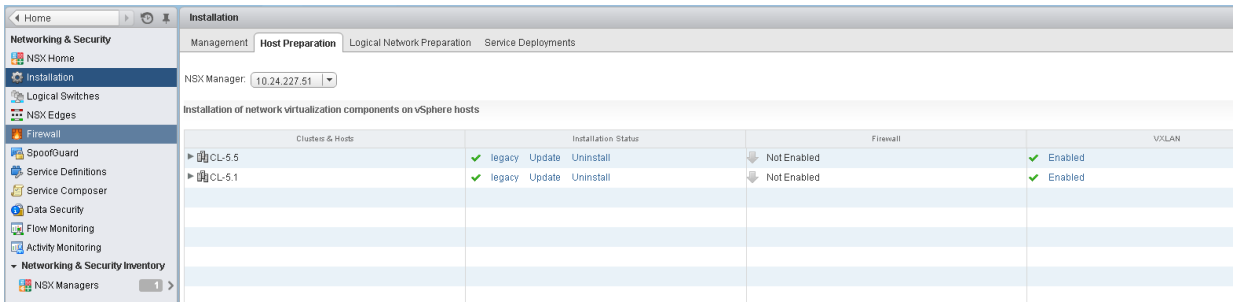
2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).

3 Haga clic en la pestaña **Preparación de host** (Host Preparation).

Se muestran todos los clústeres que se encuentren en su infraestructura.

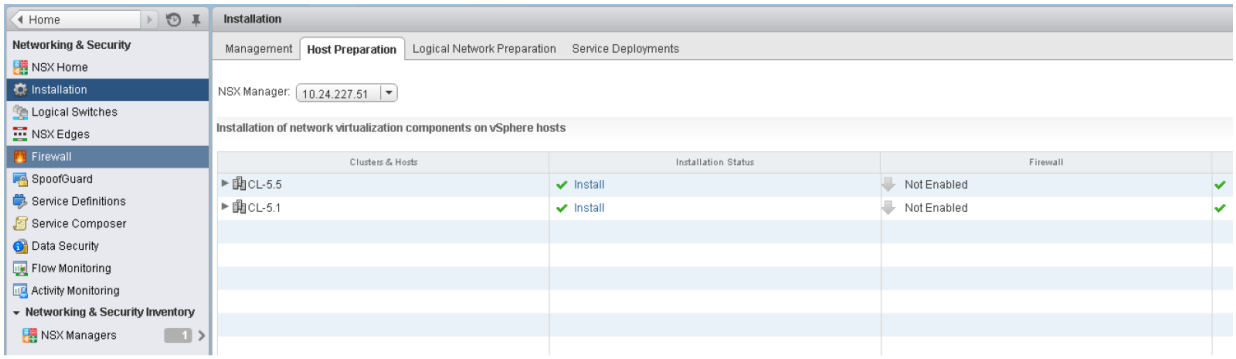
Si cuenta con Virtual Wires en su entorno 5.5, la columna **Estado de instalación** (Installation Status) muestra **heredado** (legacy), **Actualizar** (Update) y **Desinstalar** (Uninstall).

Figura 1-1. La columna Estado de instalación (Installation Status) muestra Actualizar (Update) si cuenta con Virtual Wires en su entorno 5.5



Si no cuenta con Virtual Wires en su entorno 5.5, en la columna **Estado de instalación** (Installation Status) aparece **Instalar** (Install).

Figura 1-2. En Estado de instalación (Installation Status) aparece Instalar (Install) si no tiene Virtual Wires en su entorno 5.5.



4 En cada clúster, haga clic en **Actualizar** (Update) o **Instalar** (Install) en la columna Estado de Instalación (Installation Status).

Cada host del clúster recibe el nuevo software de conmutador lógico.

La actualización del host inicia un análisis del host. Los VIB anteriores se eliminan (aunque no desaparecen por completo hasta después del reinicio). Los nuevos VIB se instalan en la partición altboot. Para ver los nuevos VIB en un host que aún no se reinició, se puede ejecutar el comando `esxcli software vib list --rebooting-image | grep esx`.

5 Supervise la instalación hasta que la columna **Estado de instalación** (Installation Status) muestre una marca de verificación de color verde.

   Si el clúster tiene DRS habilitado, DRS intenta reiniciar los hosts de una forma controlada que permite que las máquinas virtuales continúen en ejecución. vMotion mueve las máquinas virtuales en ejecución a otros hosts del clúster y coloca al host en el modo de mantenimiento.

   Si es necesario colocar los hosts manualmente en el modo de mantenimiento (por ejemplo, debido a requisitos de HA o a reglas de DRS), el proceso de actualización se detiene y el clúster **Estado de instalación** (Installation Status) muestra la opción **No está listo** (Not Ready). Haga clic en para mostrar los errores.

   Tras evacuar manualmente los hosts, seleccione el clúster y haga clic en la acción **Resolver** (Resolve). La acción **Resolver** (Resolve) intenta completar la actualización y reinicia todos los hosts del clúster. Si se produce un error en el reinicio del host por alguna razón, la acción **Resolver** (Resolve) se detiene. Compruebe el estado de los hosts en la vista **Hosts y clústeres** (Hosts and Clusters) y asegúrese de que estén encendidos, conectados y que no contengan máquinas virtuales en ejecución. A continuación, vuelva a intentar ejecutar la acción **Resolver** (Resolve).

Los nombres de todas las conexiones virtuales de la infraestructura de la versión 5.5 se cambian a los conmutadores lógicos de NSX y la columna VXLAN del clúster aparece **Habilitada** (Enabled).

Asegúrese de que la columna VXLAN de la pestaña Preparación del host (Host Preparation) aparece **Habilitada** (Enabled).

Cuando el clúster está actualizado, la columna **Estado de instalación** (Installation Status) muestra la versión de software a la que se actualizó.

Para confirmar la actualización del host, inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list | grep esx`. Asegúrese de que los siguientes VIB estén actualizados a la versión prevista.

- esx-vsip
- esx-vxlan

NOTA: En NSX 6.2, el VIB esx-dvfilter-switch-security se incluye dentro del VIB esx-vxlan.

Si la actualización de un host tiene errores, soluciónelos con los siguientes pasos:

- Revise ESX Agent Manager en vCenter y busque alertas y errores.
- Inicie sesión en el host, compruebe el archivo de registro `/var/log/esxupdate.log` y, a continuación, busque alertas y errores.
- Asegúrese de que DNS y NTP estén configurados en el host.

Qué hacer a continuación

"Cambiar el puerto de VXLAN," página 29

Cambiar el puerto de VXLAN

Es posible cambiar el puerto utilizado para el tráfico de VXLAN.

En NSX 6.2.3., el puerto VXLAN predeterminado es el 4789, el puerto estándar que asigna la IANA. Antes de NSX 6.2.3, el número de puerto UDP de VXLAN predeterminado era el 8472.

Las instalaciones nuevas de NSX utilizarán el puerto UDP 4789 para VXLAN.

Si en la actualización a NSX 6.2.3 y en la instalación se utilizó el puerto antiguo predeterminado (8472) o un número de puerto personalizado predeterminado (por ejemplo, el 8888) antes de la actualización, dicho puerto seguirá utilizándose tras la actualización a menos que realice los pasos necesarios para cambiarlo.

Si la instalación que actualizó utiliza o utilizará puertas de enlace de VTEP de hardware (puertas de enlace ToR), debe cambiar al puerto 4789 de VXLAN.

No es necesario que utilice el puerto 4789 para el puerto VXLAN en Cross-vCenter NSX; sin embargo, todos los hosts de un entorno de Cross-vCenter NSX deben estar configurados para usar el mismo puerto VXLAN. Si cambia al puerto 4789, garantiza que las nuevas instalaciones de NSX agregadas al entorno de Cross-vCenter NSX utilizan el mismo puerto que las implementaciones de NSX.

El cambio del puerto de VXLAN se realiza en un proceso de tres fases y no interrumpirá el tráfico de VXLAN. En un entorno de Cross-vCenter NSX, el cambio se propagará a todos los dispositivos de NSX Manager y a todos los hosts del entorno de Cross-vCenter NSX.

Prerequisitos

- Compruebe que un firewall no bloquee el puerto que desea utilizar para VXLAN.
- Compruebe que la preparación del host no se esté ejecutando a la vez que cambia el puerto de VXLAN.

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).

3 Haga clic en la pestaña **Preparación de red lógica** (Logical Network Preparation) y, a continuación, haga clic en **Transporte de VXLAN** (VXLAN Transport).

4 Haga clic en el botón **Cambiar** (Change) en el panel del puerto de VXLAN. Introduzca el puerto al que desee cambiar. El puerto 4789 es el que asigna la IANA para VXLAN.

   El cambio de puerto tardará un breve periodo de tiempo en propagarse a todos los hosts.

5 (Opcional) Compruebe el progreso del cambio de puerto con la solicitud API de `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus`.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>PHASE_TWO</taskPhase>
    <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

```
...
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>FINISHED</taskPhase>
    <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

Qué hacer a continuación

"Actualizar las zonas de transporte y los conmutadores lógicos," página 31.

Actualizar las zonas de transporte y los conmutadores lógicos

Si se implementa un clúster de NSX Controller, no se debe confiar en la multidifusión para redes lógicas. Puede actualizar a unidifusión o a híbrido el modo del plano de control de sus zonas de transporte y conmutadores lógicos.

El cambio del modo del plano de control y la migración de los conmutadores lógicos existentes no afecta al tráfico del plano de datos de la red.

Procedimiento

1 En el vSphere Web Client, diríjase a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de la red lógica (Logical Network Preparation) > Zona de Transporte (Transport Zones)**.

2 Seleccione su zona de transporte y haga clic en **Acciones (Actions) > Editar configuración (Edit Settings)**. Seleccione el modo de replicación que desee:

- **Multidifusión** (Multicast): para el plano de control se utilizan las direcciones IP de multidifusión de la red física. Este modo se recomienda únicamente para actualizar a partir de implementaciones de VXLAN anteriores. Se requiere PIM/IGMP en la red física.
- **Unidifusión** (Unicast): el plano de control es operado por NSX Controller. El tráfico de unidifusión aprovecha la replicación de cabecera optimizada. No se requieren direcciones IP de multidifusión ni ninguna configuración de red especial.
- **Híbrido** (Hybrid): descarga la replicación de tráfico local en la red física (multidifusión de Capa 2). Para esto se requiere la intromisión de IGMP en el conmutador del primer salto y el acceso a un solicitante de IGMP en cada subred de VTEP, pero no se requiere tecnología PIM. El conmutador del primer salto administra la replicación de tráfico de la subred.

3 Seleccione la casilla **Migrar conmutadores lógicos existentes al nuevo modo de plano de control** (Migrate existing Logical Switches to the new control plane method) y haga clic en **Aceptar** (OK).

Qué hacer a continuación

"Actualizar vShield App a Distributed Firewall," página 31.

Actualizar vShield App a Distributed Firewall

Se puede actualizar a Distributed Firewall únicamente desde la versión 5.5 de vShield App. Si tiene una versión anterior de vShield App en su infraestructura, debe actualizar a la versión 5.5 antes de actualizar a la versión 6.2.x. Para más información sobre cómo actualizar a la versión 5.5, consulte la *Guía de instalación y actualización de vShield* (vShield Installation and Upgrade Guide) versión 5.5.

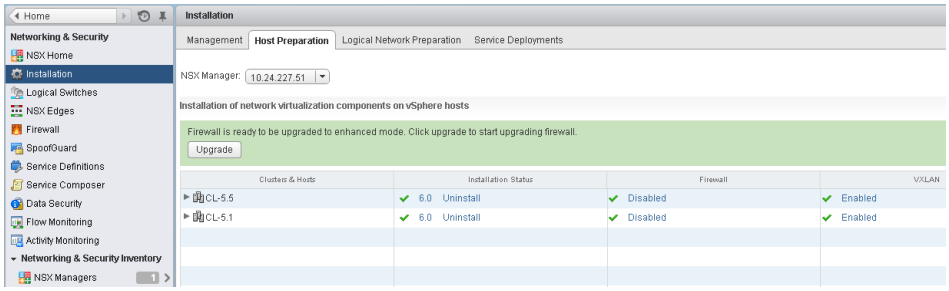
La duración del procedimiento siguiente depende del número de reglas que se encuentren en su entorno. Cuando se migra de vShield App a NSX Distributed Firewall (modo mejorado), se realiza una migración y un envío push de las reglas. Esto interrumpe el tráfico. Esta función se debe realizar durante un periodo de mantenimiento.

Prerequisitos

- vShield Manager se actualizó a NSX Manager.
- Los cables virtuales se actualizaron a conmutadores lógicos de NSX. Los usuarios que no utilicen VXLAN deben tener instalados los componentes de virtualización de la red.
- Si quiere migrar las reglas de vShield App 5.5 a Distributed firewall, no elimine los dispositivos de vShield App antes de actualizar a Distributed firewall.

Procedimiento

1 Tras preparar todos los clústeres de su entorno para los componentes de virtualización de la red, un mensaje informa de que el firewall se puede actualizar.



2 Haga clic en **Actualizar** (Upgrade).

Las reglas de vShield App 5.5 migran a NSX siguiendo este procedimiento:

a Se creará una nueva sección en la tabla de firewall para cada espacio de nombre (centro de datos y cables virtuales) que se configuran en la versión 5.5 de vShield App. Cada sección incluye las reglas correspondientes para el firewall.

b Todas las reglas de cada sección tienen el mismo valor en el campo **Aplicado a** (AppliedTo): ID del centro de datos para el espacio de nombres del centro de datos, ID de cables virtuales para el espacio de nombres de cables virtuales e ID de grupo de puertos para el espacio de nombres basado en el grupo de puertos.

c Los contenedores que se creen en niveles diferentes de espacios de nombres se trasladan a un nivel global.

d El orden de la sección debe ser el siguiente para asegurar que el firewall sigue cumpliendo su función tras la actualización:

Section_Namespace_Portgroup-1

.....

Section_Namespace_Portgroup-N

Section_Namespace_VirtualWire-1

.....

Section_Namespace_VirtualWire-N

Section_Namespace_Datacenter_1

.....

Section_Namespace_Datacenter_N

Default_Section_DefaultRule

Cuando la actualización finaliza, en la columna Firewall aparece **Habilitado** (Enabled).

3 Haga clic en **Inicio > Hosts y clústeres** (Home > Hosts and Clusters) y diríjase a los hosts en los que se ejecutan las máquinas virtuales del servicio de vShield App. Desconecte las máquinas virtuales del servicio de vShield App heredado.

4 Diríjase a **Redes y seguridad > Firewall** (Networking & Security > Firewall) y revise cada sección y regla actualizadas para comprobar que funcionan correctamente.

5 Acceda a **Instalación (Installation) > pestaña Implementación de servicios** (Service Deployment) y compruebe que se han solucionado todas las situaciones de alarma y que el estado del servicio de vShield App heredado sea **Correcto** (Succeeded).

6 Si las reglas funcionan correctamente, en la pestaña **Implementaciones de servicios** (Service Deployments), seleccione vShield App y haga clic en **Eliminar implementación de servicio (** ✖ **)** (Delete Service Deployment) para eliminar las máquinas virtuales del servicio de vShield App heredado.

Qué hacer a continuación

"Actualizar vShield Edge a NSX Edge," página 33

Actualizar vShield Edge a NSX Edge

Solo se puede actualizar desde la versión de vShield 5.5 a NSX Edge 6.2.x. Si tiene una versión anterior de vShield Edge en su infraestructura, debe actualizar a la versión 5.5 antes de actualizar a la versión 6.2.x. Para más información sobre cómo actualizar a la versión 5.5, consulte la *Guía de instalación y actualización de vShield* (vShield Installation and Upgrade Guide) versión 5.5.

Durante el proceso de actualización, se implementa un nuevo dispositivo virtual Edge junto con el existente. Cuando el nuevo dispositivo Edge está listo, las vNIC del dispositivo Edge anterior se desconectan y se conectan las del nuevo Edge. A continuación, el nuevo Edge envía paquetes gratuitos de ARP (GARP) para actualizar la caché de ARP de los conmutadores conectados. Cuando se implementa HA, el proceso de actualización se realiza dos veces.

Este proceso puede afectar de forma temporal el reenvío de paquetes. Para minimizar el impacto, configure el dispositivo Edge para que funcione en modo ECMP.

Las adyacencias de OSPF se retiran durante la actualización si el reinicio estable no está habilitado.

Prerequisitos

- Compruebe que vShield Manager está actualizado a NSX Manager.
- Tenga en cuenta el impacto operativo que produce la actualización de NSX Edge cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de vCloud Networking and Security," página 13.
- Compruebe que cuenta con un grupo de identificadores de segmento local aunque no tenga previsto crear conmutadores lógicos de NSX.
- Compruebe que los hosts tienen recursos suficientes para implementar dispositivos de puerta de enlace de servicios NSX Edge durante la actualización, sobre todo si está actualizando varios dispositivos NSX Edge en paralelo. Consulte "Requisitos del sistema para NSX," página 6 para los recursos que sean necesarios según el tamaño de NSX Edge.
  - Para una instancia sencilla de NSX Edge son necesarios dos dispositivos NSX Edge del tamaño adecuado que se mantengan encendidos durante la actualización.
  - A partir de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, se implementarán los dos dispositivos de sustitución antes de reemplazar los dispositivos anteriores. Esto significa que habrá cuatro dispositivos NSX Edge de tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualice de nuevo, cualquiera de los dispositivos con HA podrá activarse.
  - Antes de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, solo se implementaba un dispositivo de sustitución a la vez cuando se sustituían los dispositivos antiguos. Esto significa que habrá tres dispositivos NSX Edge del tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualiza, el dispositivo NSX Edge con HA con índice 0 se suele activar.
- Si tiene habilitada la VPN de Capa 2 en NSX Edge, debe eliminar su configuración antes de iniciar la actualización. Después de la actualización, puede volver a configurar la VPN de Capa 2.

Procedimiento

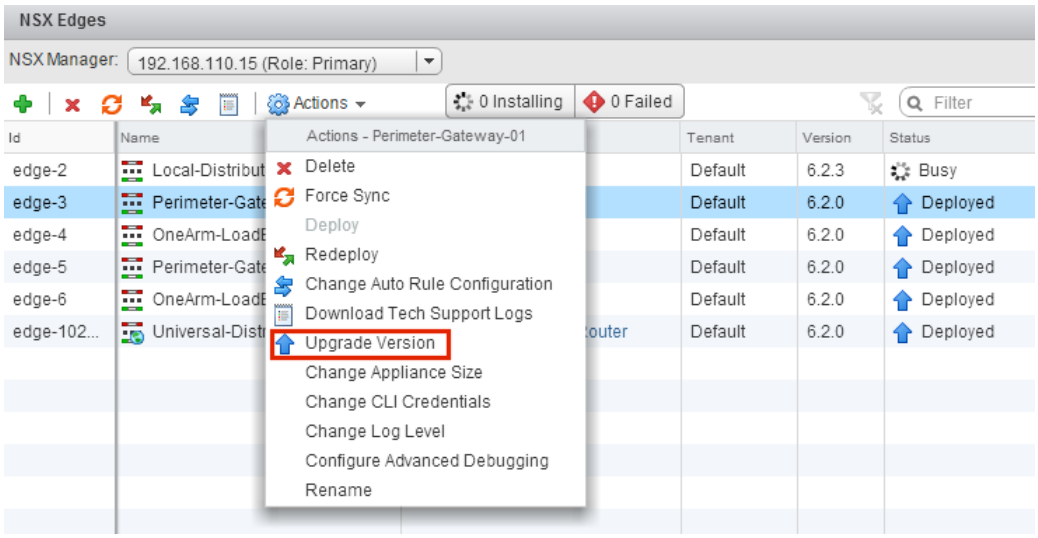
1 En vSphere Web Client, seleccione **Redes y seguridad (Networking & Security) > NSX Edge**.

2 Haga doble clic en cada instancia de NSX Edge y, antes de actualizar, compruebe que tiene establecida la siguiente configuración.

   a Haga clic en **Administrar > VPN > VPN de Capa 2** (Manage > VPN > L2 VPN) y compruebe si la VPN de Capa 2 está habilitada. Si es así, elimine la configuración de la VPN de Capa 2 después de apuntar los detalles de dicha configuración.

   b Haga clic en **Administrar > Enrutamiento > Rutas estáticas** y compruebe si alguna de las rutas estáticas no tiene la configuración del siguiente salto. Si alguna no la tiene, agregue el siguiente salto antes de actualizar NSX Edge.

3 Para cada instancia de NSX Edge, seleccione la opción **Versión de actualización** (Upgrade Version) en el menú **Acciones** (Actions).



   Si en la actualización aparece el mensaje de error "No se pudo implementar el dispositivo Edge" (Failed to deploy edge appliance), asegúrese de que el host donde se implementa el dispositivo NSX Edge esté conectado y no esté en modo de mantenimiento.

Una vez que NSX Edge se actualiza correctamente, el **Estado** (Status) se implementa (Deployed) y la columna **Versión** (Version) muestra la nueva versión de NSX.

Si un dispositivo Edge no se puede actualizar y tampoco hay una reversión a la versión anterior, haga clic en el icono **Volver a implementar NSX Edge** (Redeploy NSX Edge) e intente actualizar nuevamente.

Las reglas del firewall de NSX Edge no admiten sourcePort, por eso las reglas de la versión 5.5 de vShield Edge que contienen sourcePort se modifican durante la actualización tal y como se especifica a continuación:

- Si no existen aplicaciones que se usen en la regla, se crea un servicio con protocol=any, port=any y sourcePort=asDefinedInTheRule.
- Si en la regla se usan aplicaciones o grupos de aplicaciones, estos objetos agrupados se duplican al agregarles el sourcePort. Debido a esto, el identificador groupingObjectIds utilizado en la regla del firewall cambia tras la actualización.

Las reglas de firewall de usuario en NSX Edge 6.x no generan IPSets ni applicationSets internos basados en entradas procedentes de API de REST. En su lugar, se mantendrán en el formato sin procesar. Durante la actualización, el IPSet y los applicationSets generados internamente se utilizan para crear reglas con datos sin procesar. El identificador interno groupingObjects ya no aparecerá en las reglas de firewall (firewallRules) del usuario.

Qué hacer a continuación

Vuelva a configurar la VPN de Capa 2. Consulte la Descripción general de la VPN de Capa 2 en la *Guía de instalación de NSX*.

"Actualizar Guest Introspection," página 78

Actualizar vShield Endpoint a NSX Guest Instrospection

Es importante que actualice Guest Introspection para que coincida con la versión de NSX Manager.

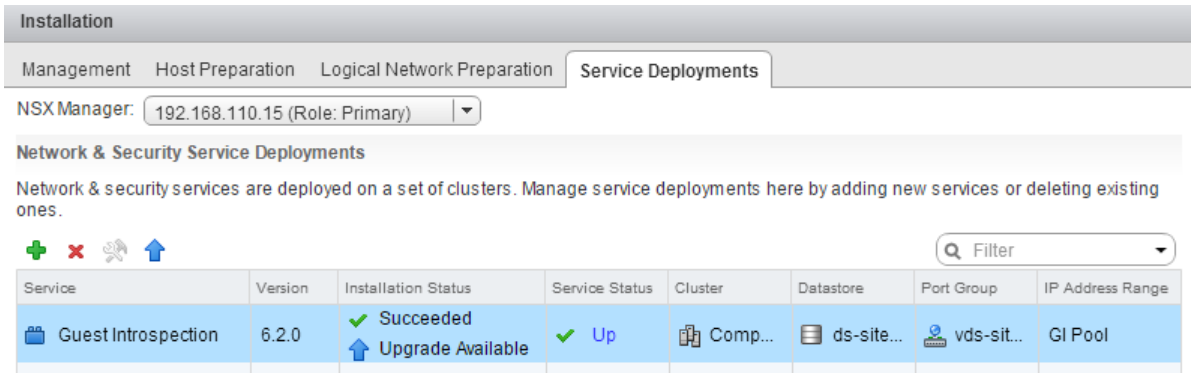
NOTA: Las máquinas virtuales de servicio de Guest Introspection se pueden actualizar desde vSphere Web Client. No es necesario eliminar la máquina virtual de servicio después de la actualización de NSX Manager para que se actualice. Si elimina la máquina virtual de servicio, el estado del servicio (Service Status) aparecerá como `Error` (Failed) ya que falta la máquina virtual agente. Haga clic en **Resolver** (Resolve) para implementar una nueva máquina virtual de servicio y, a continuación, haga clic en **Actualización disponible** (Upgrade Available) para implementar la máquina virtual de servicio de Guest Introspection más reciente.

Prerequisitos

NSX Manager, las controladoras, los clústeres del host preparados y NSX Edge deben estar actualizados a la versión 6.2.x.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

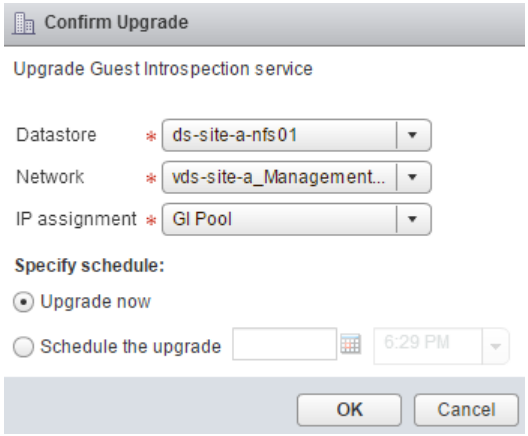


La columna **Estado de instalación** (Installation Status) indica **Actualización disponible** (Upgrade Available).

2 Seleccione la implementación de Guest Introspection que desea actualizar.

Se habilita el icono **Actualizar** (↑) (Upgrade) en la barra de herramientas ubicada encima de la tabla de servicios.

3 Haga clic en el icono **Actualizar** (⬆) (Upgrade) y siga las indicaciones de la interfaz de usuario.



Tras la actualización de Guest Introspection, el estado de la instalación es `Correcto` (Succeeded) y el estado del servicio aparece como `Listo` (Up). Las máquinas de servicio virtual de Guest Introspection están visibles en el inventario de vCenter Server.

Qué hacer a continuación

Después de actualizar Guest Introspection en un clúster concreto, puede actualizar las soluciones de los partners. Si las soluciones de los partners están habilitadas, consulte la documentación sobre la actualización que ellos mismos proporcionan. Aunque no se actualice la solución del partner, se mantiene la protección.

Si actualiza una solución de un partner a una versión que esté certificada por NSX, debe utilizar Service Composer para crear directivas basadas en las soluciones de los partners para mantener la protección. Consulte cómo utilizar Service Composer en la *Guía de administración de NSX*.

Servicios NSX Services que no admiten actualización directa

Algunas instancias de NSX Services como por ejemplo, los dispositivos virtuales de seguridad de VMware Partner, no admiten actualizaciones directas. En estos casos, debe desinstalar los servicios y volver a instalarlos.

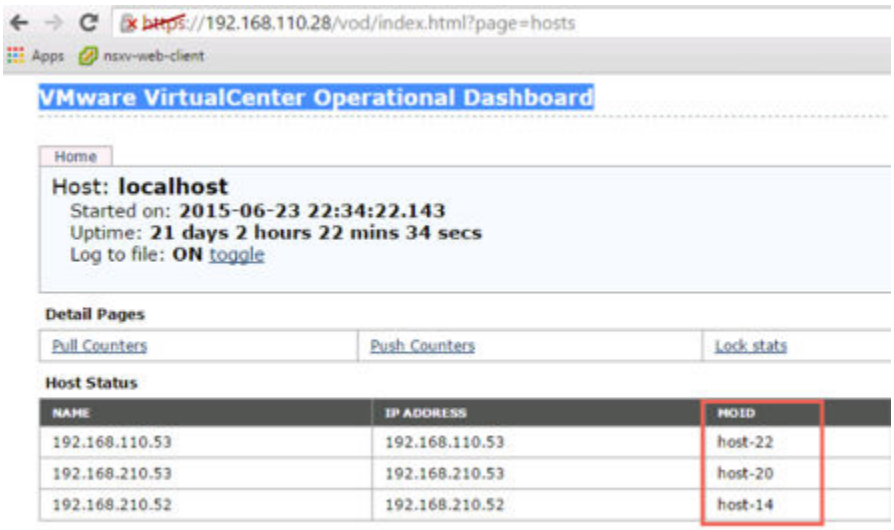
NSX Data Security

Lo ideal es desinstalar NSX Data Security antes de actualizar NSX, para volver a instalarlo después de completar la actualización de NSX. Si actualizó NSX sin desinstalar primero NSX Data Security, debe desinstalarlo con una llamada API de REST.

Emita la siguiente llamada API:

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

El identificador del host es el MOID del host ESXi. Para recuperar el MOID, abra el panel operativo de VMware VirtualCenter: https://<vcenter-ip>/vod/index.html?page=hosts.



Para el host ESXi con el MOID "host-22" en vCenter Server 192.168.110.28, la llamada API debería tener el siguiente formato:

```
DELETE https://192.168.110.28/api/1.0/vshield/host-22/vsds
```

Asegúrese de emitir la llamada API en todos los hosts ESXi.

Después de desinstalar Data Security, puede instalar la versión nueva. Consulte "Instalar NSX Data Security," página 37.

VPN SSL de NSX

A partir de NSX 6.2, la puerta de enlace de la VPN SSL solo acepta el protocolo TLS. A partir de NSX 6.2.3, el protocolo TLS 1.0 está obsoleto. Los dispositivos virtuales de seguridad de VMware Partner no admiten actualizaciones directas. Sin embargo, después de actualizar a NSX 6.2.x, todos los clientes nuevos de NSX 6.2.x creados utilizan automáticamente el protocolo TLS al establecer la conexión.

Cuando un cliente de NSX 6.0.x intenta conectarse con una puerta de enlace de NSX 6.2.x, se produce un error en el paso del enlace SSL al establecer la conexión. Este error se debe al cambio de protocolo.

Después de la actualización a NSX 6.2.x, desinstale los clientes de VPN SSL anteriores e instale la versión 6.2.x de NSX de los clientes de VPN SSL. Consulte "Instalar cliente SSL en un sitio remoto" en la *Guía de administración de NSX*.

VPN de Capa 2 de NSX

La configuración de una VPN de Capa 2 en una instancia de NSX Edge se debe eliminar para poder actualizar NSX Edge a NSX 6.2.x.

Instalar NSX Data Security

NOTA: Desde la versión 6.2.3 de NSX, la función de seguridad de datos de NSX pasó a estar obsoleta. En la versión 6.2.3 de NSX puede seguir utilizando esta función como desee, pero tenga en cuenta que se eliminará de NSX en versiones futuras.

Prerequisitos

NSX Guest Introspection debe instalarse en el clúster donde se va a instalar Data Security.

Si desea asignar una dirección IP a la máquina virtual del servicio Data Security desde un grupo de direcciones IP, cree el grupo de direcciones IP antes de instalar Data Security. Consulte Agrupar objetos en la *Guía de administración de NSX*.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

2 Haga clic en el icono **Nueva implementación de servicios** (New Service Deployment) ( ).

3 En el cuadro de diálogo Implementar servicios de red y seguridad (Deploy Network and Security Services), seleccione **Data Security** y haga clic en **Siguiente** (Next).

4 En **Especificar programación** (Specify schedule), en la parte inferior del cuadro de diálogo, seleccione **Implementar ahora** (Deploy now) para implementar Data Security apenas se instale, o bien seleccione una fecha y una hora de implementación.

5 Haga clic en **Siguiente** (Next).

6 Seleccione el centro de datos y los clústeres donde desea instalar Data Security y, a continuación, haga clic en **Siguiente** (Next).

7 En la página Seleccionar red de almacenamiento y administración (Select storage and Management Network), seleccione el almacén de datos en el que desea agregar las máquinas virtuales de servicio, o bien seleccione **Especificado en el host** (Specified on host).

   El almacén de datos seleccionado debe estar disponible en todos los hosts del clúster elegido.

   Si seleccionó **Especificado en el host** (Specified on host), el almacén de datos del host ESX debe especificarse en la opción **Configuración de máquinas virtuales de agente** (AgentVM Settings) del host antes de agregarse al clúster. Consulte la *documentación de vSphere API/SDK*.

8 Seleccione el grupo de puertos virtuales distribuidos donde se alojará la interfaz de administración. Este grupo de puertos debe poder comunicarse con el grupo de puertos de NSX Manager.

   Si el almacén de datos se configura como **Especificado en el host** (Specified on host), la red que se utilizará debe especificarse en la propiedad **agentVmNetwork** de cada host en el clúster. Consulte la *documentación de vSphere API/SDK*.

   Cuando agrega hosts al clúster, la propiedad **agentVmNetwork** del host debe configurarse antes de agregarse al clúster.

   El grupo de puertos seleccionado debe estar disponible en todos los hosts del clúster seleccionado.

9 En la asignación de direcciones IP, seleccione una de las siguientes opciones:

Seleccionar	Para
DHCP	Asigne una dirección IP a las máquinas virtuales del servicio Data Security a través del protocolo de configuración dinámica de host (DHCP).
Grupo de direcciones IP	Asigne una dirección IP a las máquinas virtuales del servicio Data Security desde el grupo de direcciones IP seleccionado.

   Tenga en cuenta que no se admiten direcciones IP estáticas.

10 Haga clic en **Siguiente** (Next) y, a continuación, en **Finalizar** (Finish) en la página Listo para finalizar (Ready to complete).

11 Supervise la implementación hasta que la columna **Estado de instalación** (Installation Status) muestre **Correcto** (Succeeded).

12 Si la columna **Estado de instalación** (Installation Status) muestra **Con errores** (Failed), haga clic en el icono junto a Con errores. Se muestran todos los errores de implementación. Haga clic en **Resolver** (Resolve) para solucionar los errores. En algunos casos, al resolver los errores aparecen otros nuevos. Realice la acción necesaria y vuelva a hacer clic en **Resolver** (Resolve).

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

1 Elimine la snapshot de NSX Manager tomada durante la instalación.

2 Realice una copia de seguridad actualizada tras la actualización.

3 Asegúrese de que los VIB estén instalados en los hosts.

NSX Instala los siguientes VIB:

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Si se ha instalado Guest Introspection, compruebe también que este VIB se encuentra en los hosts:

```
esxcli software vib get --vibname epsec-mux
```

4 Vuelva a sincronizar el bus de mensajería del host. VMware aconseja a todos sus clientes que vuelvan a realizar una sincronización tras la actualización.

Puede usar la siguiente llamada API para volver a realizar la sincronización en cada host.

```
URL : 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
```

Actualizar de vCloud Networking and Security 5.5.x a NSX en un entorno de vCloud Director

La versión de vCloud Director determinará a qué versión de NSX puede actualizar. VMware le recomienda que actualice a la última versión de NSX que sea compatible con las otras soluciones y herramientas de su entorno.

Consulte la matriz de interoperabilidad de productos de VMware en https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Para actualizar a NSX, debe actualizar los componentes de vCloud Networking and Security en el orden documentado en esta guía.

Los componentes de vCloud Networking and Security deben actualizarse en el siguiente orden:

1 vShield Manager a NSX Manager

2 Implementar el clúster de NSX Controller - opcional, necesario para los enrutadores lógicos (distribuidos) y para cambiar el modo del plano de control a híbrido o unidifusión

3 Actualizar clústeres y hosts

4 Actualizar la zona de transporte - opcional, si se implementa el clúster de NSX Controller, puede cambiar el modo del plano de control a híbrido o unidifusión

5 NSX Edge - actualice a NSX Edge solo si utiliza la versión 8.10 o superior de vCloud Director.

Componentes opcionales de vCloud Networking and Security no integrados con vCloud Director:

1 vShield App - consulte "Actualizar vShield App a Distributed Firewall," página 31.

2 vShield Endpoint - consulte "Actualizar vShield Endpoint a NSX Guest Instrospection," página 35.

3 vShield Data Security - no es compatible con la actualización. Consulte las instrucciones para desinstalar el producto: "Servicios NSX Services que no admiten actualización directa," página 36 y las instrucciones de instalación: "Instalar NSX Data Security," página 37.

Actualizar vShield Manager a NSX Manager en un entorno de vCloud Director

El primer paso en el proceso de actualización de la infraestructura NSX es actualizar el dispositivo NSX Manager.

ADVERTENCIA: No desinstale ninguna instancia implementada de un dispositivo de vShield Manager.

Prerequisitos

- Compruebe que completó todas las tareas de preparación de la actualización descritas en "Prepararse para actualizar vCloud Networking and Security a NSX," página 11, incluida la comprobación de los requisitos del sistema y la realización de copias de seguridad.
- Compruebe que vShield Manager disponga de suficiente espacio en disco para realizar la actualización a NSX Manager. Consulte "Requisitos del sistema para NSX," página 6.
- Aumente la memoria reservada del dispositivo virtual de vShield Manager como mínimo a 16 GB y asigne 4 vCPU antes de realizar la actualización a NSX 6.2.x.

  Consulte "Requisitos del sistema para NSX," página 6.
- Asegúrese de que las instancias de vShield Edge anteriores a la versión 5.5 (si las hay) se actualizaron a la versión 5.5 de vShield.

  Las instancias anteriores a la versión 5.5 de vShield Edge no pueden administrarse ni eliminarse una vez que vShield Manager se actualice a NSX Manager.

Procedimiento

1 Descargue el paquete de actualización de NSX en una ubicación a la que vShield Manager pueda acceder. El nombre del paquete de actualización es similar a `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`release-buildNumber`*`.tar.gz`.

2 Haga clic en **Configuración e informes** (Setting & Reports) en el panel de inventario de vShield Manager 5.5.

3 Haga clic en la pestaña **Actualizaciones** (Updates) y, a continuación, en **Subir paquete de actualizaciones** (Upload Upgrade Bundle).

4 Haga clic en **Seleccionar archivo** (Choose File), seleccione el archivo `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`releasebuildNumber`*`.tar.gz` y haga clic en **Abrir** (Open).

5 Haga clic en **Subir archivo** (Upload File).

  La subida puede tardar unos minutos.

6 Haga clic en **Instalar** (Install) para comenzar la actualización.

7 Haga clic en **Confirmar instalación** (Confirm Install). El proceso de actualización reinicia vShield Manager, por lo que puede perder conexión a la interfaz de usuario de vShield Manager. No se reinician ninguno de los demás componentes de vShield.

8 Tras el reinicio, abra una ventana del navegador para iniciar sesión en el dispositivo virtual de NSX Manager e introduzca la dirección IP, por ejemplo, https://10.10.10.10. NSX Manager actualizado tiene la misma dirección IP que vShield Manager.

   La pestaña Resumen (Summary) muestra la versión de NSX Manager que tiene instalada.

9 Acceda a **Inicio (Home) > Administrar registro de Manage vCenter (Manage vCenter Registration)** y compruebe que el estado de vCenter Server sea `Conectado` (Connected).

10 Cierre el resto de navegadores que accedan a vSphere Web Client. Espere unos minutos y limpie la caché del navegador antes de volver a iniciar sesión en vSphere Web Client.

11 Si SSH estaba habilitado en vShield Manager, debe habilitarlo en NSX Manager tras la actualización. Inicie sesión en la aplicación virtual de NSX Manager y haga clic en **Ver resumen** (View Summary). En los componentes a nivel de sistema, haga clic en **Iniciar** (Start) para comenzar el servicio SSH.

IMPORTANTE: Tras actualizar desde vCloud Networking and Security 5 a NSX 6.x, deberá usar sus credenciales administrativas de inicio de sesión de CLI para iniciar sesión en NSX Manager. Previamente, en vCloud Networking and Security eran necesarias dos contraseñas: una para la CLI y otra para la interfaz de usuario. Para iniciar NSX 6.x, solo es necesaria una contraseña. Por ejemplo:

Contraseñas de vCloud Networking and Security

- micontraseña#123 para la CLI
- micontraseña#456 para la interfaz de usuario

Contraseñas tas la actualización de NSX

- micontraseña#123 para la CLI
- micontraseña#123 para la interfaz de usuario

Después de actualizar NSX Manager y de conectarlo a una instancia de vCenter Server existente, restablezca el servidor Web Client para permitir que también se actualicen los complementos de NSX.

- También puede hacer esto en vCenter 5.5. Para ello, abra https://<vcenter-ip>:5480 y reinicie el servidor Web Client.
- Para hacerlo en vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como raíz y ejecute los comandos siguientes.

  ```
  Command> shell.set --enabled True
  Command> shell
  localhost:~ # cd /bin
  localhost:~ # service-control --stop vsphere-client
  localhost:~ # service-control --start vsphere-client
  ```

- En vCenter Server 6.0, puede ejecutar los siguientes comandos en Windows.

  ```
  cd C:\Program Files\VMware\vCenter Server\bin
  service-control --stop vspherewebclientsvc
  service-control --start vspherewebclientsvc
  ```

Se requiere reiniciar para evitar errores inesperados, como grupos de seguridad configurados que no aparecen en la pestaña **Grupos de seguridad** (Security Groups) de Service Composer.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su navegador.

Se recomienda utilizar diferentes servidores Web Client para administrar los servidores vCenter Server que ejecutan distintas versiones de NSX Manager a fin de evitar errores inesperados cuando diferentes versiones de complementos de NSX están en ejecución.

Una vez actualizado NSX Manager, cree un nuevo archivo de copia de seguridad de NSX Manager. Consulte "Copia de seguridad y restauración de NSX," página 62. La copia de seguridad anterior de NSX Manager solo es válida para la versión anterior.

Qué hacer a continuación

"Instalar y asignar una licencia NSX en un entorno vCloud Director," página 42

Instalar y asignar una licencia NSX en un entorno vCloud Director

Una vez finalizada la actualización de NSX Manager se puede instalar y asignar una licencia NSX for vSphere mediante vSphere Web Client.

Al iniciar NSX 6.2.3, la licencia predeterminada al completar la instalación será NSX para vShield Endpoint. Esta licencia habilita el uso de NSX para implementar y administrar vShield Endpoint solo para descarga de antivirus y tiene un cumplimiento forzado para restringir el uso de VXLAN, firewall y servicios Edge, bloqueando la preparación del host y la creación de instancias de NSX Edge.

Para utilizar NSX con vCloud Director, debe adquirir una licencia NSX que cubra las funciones adicionales de NSX necesarias, incluido NSX Edge.

Consulte las preguntas más recientes sobre la licencia de NSX en https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Para obtener más información sobre las licencias de NSX, consulte http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

Procedimiento

- En vSphere 5.5, complete los siguientes pasos para agregar una licencia para NSX.
  a. Inicie sesión en vSphere Web Client.
  b. Haga clic en **Administración** (Administration) y, a continuación, en **Licencias** (Licenses).
  c. Haga clic en la pestaña **Soluciones** (Solutions).
  d. Seleccione NSX for vSphere en la lista Soluciones (Solutions). Haga clic en **Asignar una clave de licencia** (Assign a license key).
  e. Seleccione **Asignar una nueva clave de licencia** (Assign a new license key) en el menú desplegable.
  f. Escriba la clave de licencia y una etiqueta opcional para la nueva clave.
  g. Haga clic en **Descodificar** (Decode).

     Descodifique la clave de licencia para comprobar que tenga el formato correcto y suficiente capacidad para conceder una licencia a los activos.
  h. Haga clic en **Aceptar** (OK).
- En vSphere 6.0, complete los siguientes pasos para agregar una licencia para NSX.
  a. Inicie sesión en vSphere Web Client.
  b. Haga clic en **Administración** (Administration) y, a continuación, en **Licencias** (Licenses).
  c. Haga clic en la pestaña **Activos** (Assets) y luego en la pestaña **Soluciones** (Solutions).
  d. Seleccione NSX for vSphere en la lista Soluciones (Solutions). En el menú desplegable **Todas las acciones** (All Actions), seleccione **Asignar licencia...** (Assign license...).

e Haga clic en el icono **Agregar (** **)** (Add). Introduzca la clave de licencia y haga clic en **Siguiente** (Next). Agregue un nombre para las licencias y haga clic en **Siguiente** (Next). Haga clic en **Finalizar** (Finish) para agregar la licencia.

f Seleccione la nueva licencia.

g (Opcional) Haga clic en el icono **Ver características** para ver qué características están habilitadas con esta licencia. Revise la columna de **Capacidad** para comprobar la capacidad de la licencia.

h Haga clic en **Aceptar** (OK) para asignar la nueva licencia a NSX.

Qué hacer a continuación

"Implementar el clúster de NSX Controller para NSX en un entorno de vCloud Director," página 43 (opcional, le permite elegir un modo de plano de control diferente a multidifusión).

En caso de no implementar controladoras, "Actualizar los clústeres del host de vCNS a NSX en un entorno de vCloud Director," página 47

Implementar el clúster de NSX Controller para NSX en un entorno de vCloud Director

NSX Controller es un sistema de administración de estado avanzado distribuido que proporciona funciones del plano de control para funciones de enrutamiento y conmutación lógicos de NSX. Sirve como punto de control central para todos los conmutadores lógicos de una red y mantiene información sobre todos los hosts, conmutadores lógicos (VXLAN) y enrutadores lógicos distribuidos. Las controladoras se requieren cuando se planean implementar 1) enrutadores lógicos distribuidos o 2) VXLAN en modo híbrido o de unidifusión.

Más allá del tamaño de la implementación de NSX, VMware requiere que cada clúster de NSX Controller tenga tres nodos de controladora. No se admite otra cantidad de nodos de controladora.

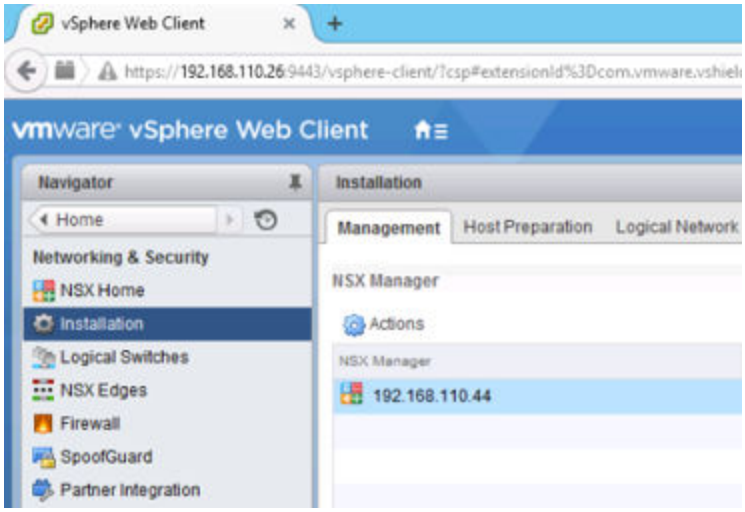
Prerequisitos

- Antes de implementar las instancias de NSX Controller, debe implementar un dispositivo NSX Manager y registrar vCenter con NSX Manager.
- Determine la configuración del grupo de direcciones IP del clúster de controladoras, incluidos la puerta de enlace y el rango de direcciones IP. La configuración de DNS es opcional. La red IP de NSX Controller debe tener conexión a NSX Manager y a las interfaces de administración de los hosts ESXi.

Procedimiento

1 En vCenter, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation) y seleccione la pestaña **Administración** (Management).

Por ejemplo:

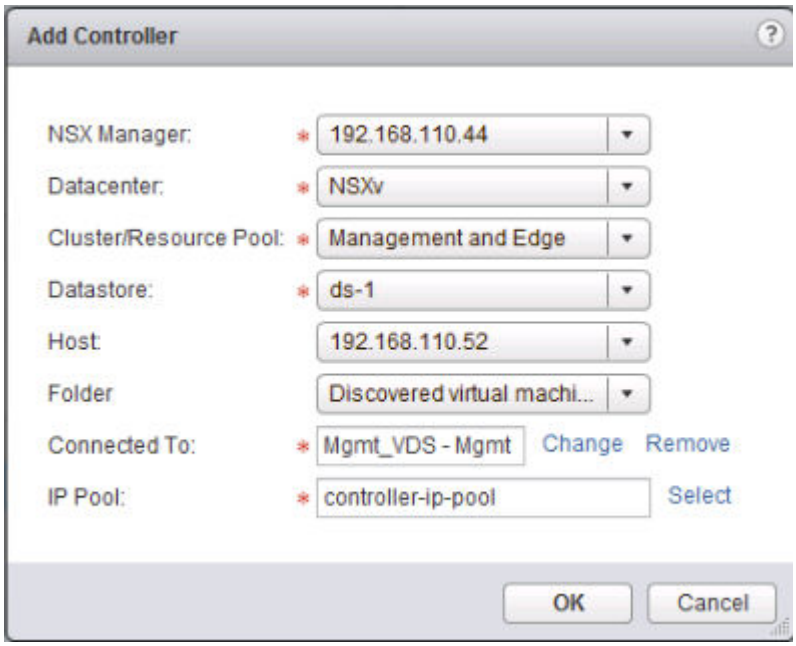


2 En la sección de nodos de NSX Controller, haga clic en el icono **Agregar nodo** (Add Node) ( ).

3 Introduzca la configuración de NSX Controller adecuada para el entorno.

Las instancias de NSX Controller deben implementarse en un grupo del puerto de vSphere Distributed Switch o de vSphere Standard Switch que no esté basado en VXLAN y que tenga conexión a NSX Manager, a otros controladores y a hosts a través de IPv4.

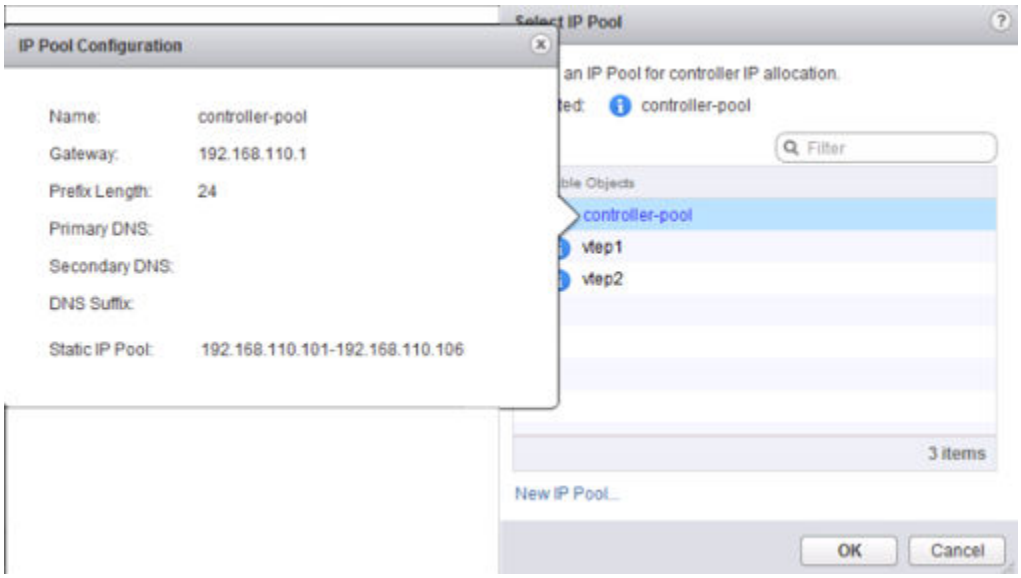
Por ejemplo:



4 Si todavía no configuró un grupo de direcciones IP para el clúster de controladoras, haga clic en **Nuevo grupo de direcciones IP** (New IP Pool) para hacerlo.

De ser necesario, las controladoras individuales pueden estar en subredes de IP distintas.

Por ejemplo:



5 Introduzca y vuelva a introducir una contraseña para la controladora.

NOTA: La contraseña no debe contener el nombre de usuario como subcadena. Los caracteres no deben repetirse 3 o más veces consecutivas.

La contraseña debe tener al menos 12 caracteres y cumplir con al menos 3 de las siguientes 4 reglas:

- Al menos una letra en mayúscula
- Al menos una letra en minúscula
- Al menos un número
- Al menos un carácter especial

6 Una vez implementada la primera controladora, implemente otras dos más.

Es obligatorio tener tres controladoras. Le recomendamos que configure una regla antiafinidad DRS para evitar que las controladoras residan en el mismo host.

Una vez implementadas todas correctamente, el estado de las controladoras es **Normal** y aparece una marca de verificación de color verde.

Acceda a cada controladora mediante SSH y compruebe que se pueda hacer ping en las direcciones IP de la interfaz de administración del host. Si no se puede hacer ping, compruebe que todas las controladoras tengan la puerta de enlace predeterminada que corresponde. Para ver la tabla de enrutamiento de una controladora, ejecute el comando **show network routes**. Para cambiar la puerta de enlace predeterminada de una controladora, ejecute el comando **clear network routes** y, a continuación, el comando **add network default-route <dirección IP>**.

Ejecute los siguientes comandos para comprobar que el comportamiento del clúster de control sea el esperado.

- `show control-cluster status`

```
Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   05/04 02:36:03
Majority status:    Connected to cluster majority                   05/19 23:57:23
Restart status:     This controller can be safely restarted         05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  En el estado Unirse (Join), compruebe que el nodo de controladora informe sobre el estado Unión completa (Join Complete).

  En el estado Mayoría (Majority), compruebe que la controladora esté conectada a la mayoría del clúster.

  En el identificador del clúster, todos los nodos de controladora de un clúster deben tener el mismo identificador de clúster.

  En los estados Configurado (Configured) y Activo (Active), compruebe que todas las funciones de la controladora están habilitadas y activadas.

- `show control-cluster roles`

```
                        Listen-IP  Master?    Last-Changed  Count
api_provider         Not configured      Yes  06/02 08:49:31      4
persistence_server              N/A      Yes  06/02 08:49:31      4
switch_manager            127.0.0.1      Yes  06/02 08:49:31      4
logical_manager                 N/A      Yes  06/02 08:49:31      4
directory_server                N/A      Yes  06/02 08:49:31      4
```

  Cada rol tendrá un nodo de controladora maestro. En este ejemplo, un único nodo es el nodo maestro de todos los roles.

  Si se produce un error en una instancia principal de NSX Controller de una función, el clúster elegirá una nueva instancia principal para esa función entre las instancias de NSX Controller disponibles.

  Las instancias de NSX Controller están en el plano de control, por lo que un error en NSX Controller no afectará al tráfico del plano de datos.

- `show control-cluster connections`

```
role                port            listening open conns
------------------------------------------------------------
api_provider        api/443         Y         2
------------------------------------------------------------
persistence_server  server/2878     Y         2
                    client/2888     Y         1
                    election/3888   Y         0
------------------------------------------------------------
switch_manager      ovsmgmt/6632    Y         0
```

```
                    openflow/6633   Y         0
------------------------------------------------------------
system              cluster/7777    Y         0
```

Este comando muestra el estado de comunicación en dentro del clúster.

El líder por mayoría de clúster de controladoras escucha en el puerto 2878 (como muestra la "Y" en la columna "escuchando" [listening]). En los otros nodos de controladoras aparece un guión (-) en la columna "escuchando" (listening) para el puerto 2878.

Todos los otros puertos deben escuchar en los tres nodos de controladora.

La columna "conex. abiertas" (open conns.) muestra la cantidad de conexiones abiertas que tiene el nodo de controladora con los otros nodos de controladora. En un clúster de controladoras de tres nodos, el nodo de controladora no debe tener más de dos conexiones abiertas.

Qué hacer a continuación

ADVERTENCIA: Mientras una controladora está en estado **Implementando** (Deploying), no agregue ni modifique conmutadores lógicos o enrutamiento distribuido en el entorno. Tampoco continúe con el procedimiento de preparación del host. Después de agregar una nueva controladora al clúster de controladoras, todas las controladoras quedan inactivas durante un breve período (5 minutos como máximo). Durante este tiempo de inactividad, cualquier operación relacionada con las controladoras, por ejemplo, la preparación del host, puede tener resultados inesperados. Aunque parezca que la preparación del host se completó satisfactoriamente, es posible que la certificación SSL no se establezca correctamente, lo que provoca problemas en la red VXLAN.

Si necesita eliminar una controladora implementada, consulte la sección sobre cómo solucionar un error de NSX Controller en *Guía de administración de NSX*.

NSX habilita el apagado o el inicio automáticos de la máquina virtual en los hosts en los que los nodos de NSX Controller se implementan primero. Si las máquinas virtuales del nodo de controladoras se migran a otros hosts posteriormente, es posible que los nuevos hosts no tengan habilitado el inicio/apagado automático de máquinas virtuales. Por este motivo, VMware recomienda que compruebe todos los hosts del clúster para asegurarse de que la opción de encendido/apagado automático esté habilitada. Consulte http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html.

Actualizar los clústeres del host de vCNS a NSX en un entorno de vCloud Director

Debe preparar su entorno para la virtualización de la red mediante la instalación de los componentes de la infraestructura de red a nivel de clúster para cada servidor vCenter. De esta forma se implementa el software necesario en todos los hosts del clúster y se vuelve a nombrar a los cables virtuales como conmutadores lógicos de NSX. Durante este proceso, se actualiza el software de cada host del clúster y, a continuación, el host se reinicia.

Debe preparar su entorno para la virtualización de la red mediante la instalación de los componentes de la infraestructura de red a nivel de clúster para cada servidor vCenter. De esta forma se implementa el software necesario en todos los hosts del clúster y se vuelve a nombrar a los cables virtuales como conmutadores lógicos de NSX. Durante este proceso, se actualiza el software de cada host del clúster y, a continuación, el host se reinicia.

Se recomienda actualizar a conmutadores lógicos en una ventana de mantenimiento del centro de datos.

Mientras se esté realizando la actualización, no implemente, actualice ni desinstale ningún servicio ni componente.

Tras instalarlo o actualizarlo, NSX intentará poner automáticamente cada host en modo mantenimiento y reiniciarlo. Esto no está recomendado para entornos de vCloud Director.

En su lugar, debe actualizar los VIB en cada clúster, pero no haga clic en **Resolver** (Resolve). Debe deshabilitar el host en vCloud Director antes de entrar en el modo mantenimiento y reiniciar.

NOTA: Los VTEP que se crearon en vCloud Networking and Security no utilizan grupos de IP, sino un DHCP o direcciones IP asignadas de forma manual.

Procedimiento

1 Actualizar los VIB en los hosts en un entorno de vCloud Director página 48

En un ambiente de vCloud Director, debe establecer DRS en manual antes de actualizar los VIB en los clústeres. De lo contrario, NSX intentará establecer el modo mantenimiento en los hosts.

2 Reiniciar los hosts de forma manual después de instalar VIB en un entorno de vCloud Director página 50

Se deben reiniciar los host para que los VIB de NSX instalados surtan efecto. Debe deshabilitar los hosts de vCloud Director antes de reiniciarlos. Esto evita que vCloud Director intente utilizar los hosts durante el reinicio.

Actualizar los VIB en los hosts en un entorno de vCloud Director

En un ambiente de vCloud Director, debe establecer DRS en manual antes de actualizar los VIB en los clústeres. De lo contrario, NSX intentará establecer el modo mantenimiento en los hosts.

Prerequisitos

- Compruebe que vShield Manager está actualizado a NSX Manager.
- Compruebe que la columna VXLAN de la pestaña Preparación del host (Host Preparation) aparece **Habilitada** (Enabled).
- Compruebe que puedan resolverse los nombres de dominio completos (FQDN) de todos los hosts.
- Antes de iniciar la actualización, asegúrese de que DRS funcione en el entorno.
  - Compruebe que DRS esté habilitado en los clústeres del host.
  - Compruebe que vMotion funcione correctamente.
  - Compruebe el estado de la conexión del host con vCenter.
  - Compruebe si cuenta con tres hosts ESXi como mínimo en cada clúster de host. Durante una actualización de NSX, hay más probabilidades de que un clúster de hosts con solo uno o dos hosts presente problemas con el control de admisión de DRS. Para que la actualización de NSX funcione, VMware recomienda que cada clúster de hosts tenga al menos tres hosts. Si un clúster contiene menos de tres hosts, se recomienda evacuarlos manualmente.
- Si DRS está habilitado, las máquinas virtuales en ejecución se moverán automáticamente durante la actualización del clúster de hosts. Antes de iniciar la actualización, asegúrese de que DRS funcione en el entorno.
  - Compruebe que DRS esté habilitado en los clústeres del host.
  - Compruebe que vMotion funcione correctamente.
  - Compruebe el estado de la conexión del host con vCenter.
  - Compruebe si cuenta con tres hosts ESXi como mínimo en cada clúster de host. Durante una actualización de NSX, hay más probabilidades de que un clúster de hosts con solo uno o dos hosts presente problemas con el control de admisión de DRS. Para que la actualización de NSX funcione, VMware recomienda que cada clúster de hosts tenga al menos tres hosts. Si un clúster contiene menos de tres hosts, se recomienda evacuarlos manualmente.

Procedimiento

1 En vSphere Web Client, acceda a **Inicio (Home) > Hosts y clústeres (Hosts and Clusters)**.

2 Establezca DRS en el modo manual en los clústeres de hosts. Repita estos pasos para todos los clústeres que tengan vCloud Networking and Security instalado.

ADVERTENCIA: No deshabilite DRS. Si deshabilita DRS, los grupos de recursos se eliminarán y la instalación de vCloud Director se dañará.

a Seleccione un clúster y acceda a **Administrar (Manage) > Configuración (Settings) > vSphere DRS**.

b Tenga en cuenta la configuración actual de **Automatización de DRS** (DRS Automation), ya que deshará este cambio más adelante.

c Haga clic en **Editar** (Edit). En la sección **Automatización de DRS** (DRS Automation), seleccione **Manual** y haga clic en **Aceptar** (OK).

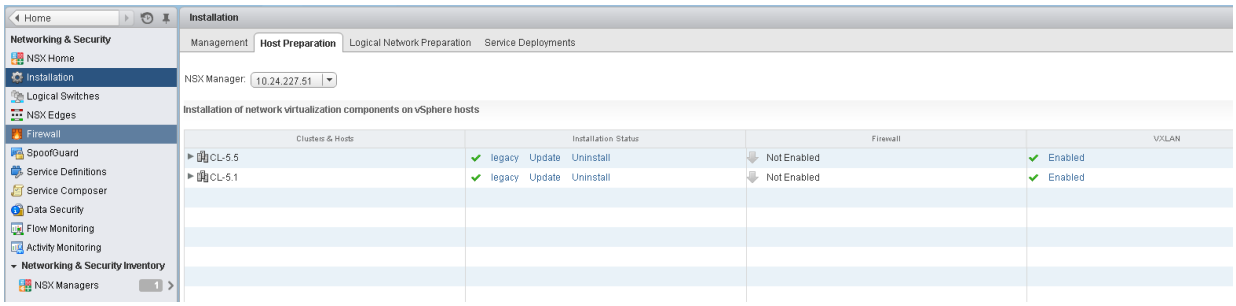
3 Acceda a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation)**.

4 Haga clic en la pestaña **Preparación de host** (Host Preparation).

Se muestran todos los clústeres que se encuentren en su infraestructura.

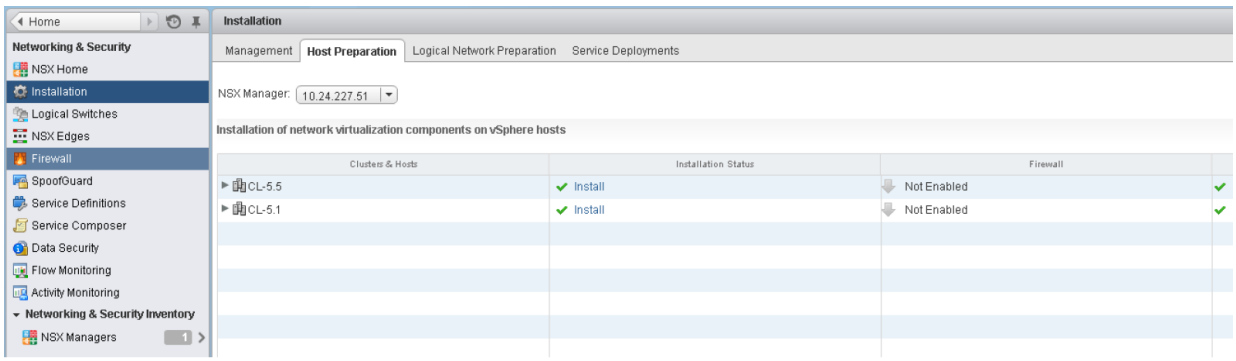
Si cuenta con Virtual Wires en su entorno 5.5, la columna **Estado de instalación** (Installation Status) muestra **heredado** (legacy), **Actualizar** (Update) y **Desinstalar** (Uninstall).

Figura 1-3. La columna Estado de instalación (Installation Status) muestra Actualizar (Update) si cuenta con Virtual Wires en su entorno 5.5



Si no cuenta con Virtual Wires en su entorno 5.5, en la columna **Estado de instalación** (Installation Status) aparece **Instalar** (Install).

Figura 1-4. En Estado de instalación (Installation Status) aparece Instalar (Install) si no tiene Virtual Wires en su entorno 5.5.



5 En cada clúster, haga clic en **Actualizar** (Update) o **Instalar** (Install) en la columna Estado de Instalación (Installation Status).

Cada host del clúster recibe el nuevo software de conmutador lógico.

La actualización del host inicia un análisis del host. Los VIB anteriores se eliminan (aunque no desaparecen por completo hasta después del reinicio). Los nuevos VIB se instalan en la partición altboot. Para ver los nuevos VIB en un host que aún no se reinició, se puede ejecutar el comando `esxcli software vib list --rebooting-image | grep esx`.

6 Supervise la instalación hasta que la columna **Estado de instalación** (Installation Status) muestre la opción **No está listo** (Not Ready).

No haga clic en **Resolver** (Resolve).

7 Acceda a **Inicio (Home) > Hosts and Clusters (Hosts y clústeres)**.

8 Deshaga los cambios de DRS en los clústeres de host. Repita estos pasos para todos los clústeres que tengan NSX instalado.

a Seleccione un clúster y acceda a **Administrar (Manage) > Configuración (Settings)**.

b Seleccione **vSphere DRS** y haga clic en **Editar** (Edit). En la sección **Automatización de DRS** (DRS Automation), seleccione la configuración de DRS original y haga clic en **Aceptar** (OK).

Qué hacer a continuación

"Reiniciar los hosts de forma manual después de instalar VIB en un entorno de vCloud Director," página 50.

Reiniciar los hosts de forma manual después de instalar VIB en un entorno de vCloud Director

Se deben reiniciar los host para que los VIB de NSX instalados surtan efecto. Debe deshabilitar los hosts de vCloud Director antes de reiniciarlos. Esto evita que vCloud Director intente utilizar los hosts durante el reinicio.

Prerequisitos

- Compruebe que todos los hosts muestran el estado **No preparado** (Not Ready).
- Compruebe que cada clúster de vSphere tiene capacidad suficiente para funcionar temporalmente sin ningún host.
- Compruebe que DRS está habilitado y no está configurado como Manual.

Procedimiento

1 En vCloud Director, deshabilite el host.

a Diríjase a **Administrar y supervisar > Hosts** (Manage & Monitor > Hosts).

b Haga clic con el botón secundario en un host y seleccione **Deshabilitar Host** (Disable Host).

2 En vSphere Web Client, acceda a **Inicio (Home) > Hosts y clústeres (Hosts and Clusters)**.

3 Haga clic con el botón secundario en el host que ha deshabilitado en vCloud Director y seleccione **Comenzar el modo mantenimiento** (Enter Maintenance Mode). En el cuadro de diálogo Confirmar modo de mantenimiento (Confirm Maintenance Mode), seleccione **Enviar máquinas virtuales apagadas y suspendidas a otros hosts en el clúster** (Move powered-off and suspended virtual machines to other hosts in the cluster) y haga clic en **Sí** (OK).

4 Si no se envían todas las máquinas virtuales a otros hosts, hágalo manualmente.

5 Una vez que los hosts están en modo mantenimiento, haga clic con el botón secundario en el host y seleccione **Reiniciar** (Reboot). Introduzca una razón para reiniciar y haga clic en **Sí** (OK).

6 Una vez realizada la copia de seguridad del host, haga clic con el botón secundario y seleccione **Salir del modo mantenimiento** (Exit Maintenance Mode).

7 En vCloud Director, habilite el host.

   a Diríjase a **Administrar y supervisar > Hosts** (Manage & Monitor > Hosts).

   b Haga clic con el botón secundario en el host y seleccione **Habilitar Host** (Enable Host).

8 Una vez que el host está habilitado en vCloud Director, repita estos pasos para el host siguiente.

Los nombres de todas las conexiones virtuales de la infraestructura de la versión 5.5 se cambian a los conmutadores lógicos de NSX y la columna VXLAN del clúster aparece **Habilitada** (Enabled).

Habilitada

Cuando el clúster está actualizado, la columna **Estado de instalación** (Installation Status) muestra la versión de software a la que se actualizó.

Para confirmar la actualización del host, inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list | grep esx`. Asegúrese de que los siguientes VIB estén actualizados a la versión prevista.

- esx-vsip
- esx-vxlan

NOTA: En NSX 6.2, el VIB esx-dvfilter-switch-security se incluye dentro del VIB esx-vxlan.

Si la actualización de un host tiene errores, soluciónelos con los siguientes pasos:

- Revise ESX Agent Manager en vCenter y busque alertas y errores.
- Inicie sesión en el host, compruebe el archivo de registro `/var/log/esxupdate.log` y, a continuación, busque alertas y errores.
- Asegúrese de que DNS y NTP estén configurados en el host.

Qué hacer a continuación

Si implementó un clúster de NSX Controller, puede cambiar el modo del plano de control si lo desea: "Actualizar las zonas de transporte y los conmutadores lógicos en un entorno de vCloud Director.," página 51.

De lo contrario, consulte "Determinar si actualizar Upgrade vShield Edge en un entorno de vCloud Director," página 52.

Actualizar las zonas de transporte y los conmutadores lógicos en un entorno de vCloud Director.

Si se implementa un clúster de NSX Controller, no se debe confiar en la multidifusión para redes lógicas. Puede actualizar a unidifusión o a híbrido el modo del plano de control de sus zonas de transporte y conmutadores lógicos.

El cambio del modo del plano de control y la migración de los conmutadores lógicos existentes no afecta al tráfico del plano de datos de la red.

Procedimiento

1 En el vSphere Web Client, diríjase a **Inicio (Home) > Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación de la red lógica (Logical Network Preparation) > Zona de Transporte (Transport Zones)**.

2 Seleccione su zona de transporte y haga clic en **Acciones (Actions) > Editar configuración (Edit Settings)**. Seleccione el modo de replicación que desee:

- **Multidifusión** (Multicast): para el plano de control se utilizan las direcciones IP de multidifusión de la red física. Este modo se recomienda únicamente para actualizar a partir de implementaciones de VXLAN anteriores. Se requiere PIM/IGMP en la red física.
- **Unidifusión** (Unicast): el plano de control es operado por NSX Controller. El tráfico de unidifusión aprovecha la replicación de cabecera optimizada. No se requieren direcciones IP de multidifusión ni ninguna configuración de red especial.
- **Híbrido** (Hybrid): descarga la replicación de tráfico local en la red física (multidifusión de Capa 2). Para esto se requiere la intromisión de IGMP en el conmutador del primer salto y el acceso a un solicitante de IGMP en cada subred de VTEP, pero no se requiere tecnología PIM. El conmutador del primer salto administra la replicación de tráfico de la subred.

3 Seleccione la casilla **Migrar conmutadores lógicos existentes al nuevo modo de plano de control** (Migrate existing Logical Switches to the new control plane method) y haga clic en **Aceptar** (OK).

Qué hacer a continuación

"Determinar si actualizar Upgrade vShield Edge en un entorno de vCloud Director," página 52

Determinar si actualizar Upgrade vShield Edge en un entorno de vCloud Director

La versión de vCloud Director determina si debe o no actualizar vShield Edge.

Si utiliza una versión anterior a vCloud Director 8.10, no debe actualizar vShield Edge.

Además, si utiliza la versión 5.x de vCloud Director, debe realizar un cambio en la configuración de la base de datos de vCloud Director para evitar que vCloud Director actualice las instancias de Edge en una reimplementación. Consulte "Evitar la reimplementación del vShield Edge heredado en un entorno de vCloud Director," página 52.

A partir de la versión 8.10 de vCloud Director, se admite NSX Edge 6.x y puede actualizar vShield Edge a NSX Edge 6.x. Consulte "Actualizar vShield Edge a NSX Edge en un entorno de vCloud Director," página 53.

Evitar la reimplementación del vShield Edge heredado en un entorno de vCloud Director

Si está utilizando vCloud Director 5.x, después de realizar la actualización a NSX debe hacer un cambio en la base de datos para evitar que los dispositivos heredados de vShield Edge se implementen como dispositivos de NSX Edge.

Es importante que no actualice las puertas de enlace de los servicios Edge heredados a la versión 6.x de VMware NSX ya que se anulará la compatibilidad de vCloud Director. vCloud Director 5.x actualizará una instancia de Edge en vCloud Director cuando dicha instancia se vuelva a implementar. Para evitar que esto ocurra, es necesario que realice el siguiente cambio en la base de datos de vCloud Director antes de migrar vCloud Network and Security.

Para obtener más información, consulte los siguientes artículos en la base de conocimientos de VMware: http://kb.vmware.com/kb/2096351 y http://kb.vmware.com/kb/2108913.

Procedimiento

1 Inicie sesión en la base de datos del servidor SWL de vCloud Director.

2 Agregue esta línea a la tabla de configuración.

```
INSERT INTO config (cat, name, value, sortorder) VALUES
('vcloud','networking.edge_version_for_vsm6.2', '5.5', 0);
```

NOTA: Utilice `networking.edge_version_for_vsm6.1` con NSX 6.1 o `networking.edge_version_for_vsm6.0` con NSX 6.0.

Actualizar vShield Edge a NSX Edge en un entorno de vCloud Director

vCloud Director 8.10 es compatible con NSX Edge 6.x y le permite actualizar vShield Edge a NSX Edge. Si utiliza una versión anterior de vCloud Director, no será compatible con NSX Edge 6.x y no podrá actualizar NSX Edge.

Es posible actualizar vShield Edge a NSX Edge de dos maneras, mediante NSX o a través de vCloud Director.

Para actualizar Edge con vCloud Director, consulte cómo actualizar los sistemas de vCenter Server, los hosts y las instancias de NSX Edge en la *Guía de instalación y actualizaciones de vCloud Director* (Installation and Upgrade Guide).

Attention Si utiliza una versión anterior a vCloud Director 8.10, no actualice NSX Edge.

Prerequisitos

- Compruebe que vShield Manager está actualizado a NSX Manager.
- Tenga en cuenta el impacto operativo que produce la actualización de NSX Edge cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de vCloud Networking and Security," página 13.
- Compruebe que cuenta con un grupo de identificadores de segmento local aunque no tenga previsto crear conmutadores lógicos de NSX.
- Compruebe que los hosts tienen recursos suficientes para implementar dispositivos de puerta de enlace de servicios NSX Edge durante la actualización, sobre todo si está actualizando varios dispositivos NSX Edge en paralelo. Consulte "Requisitos del sistema para NSX," página 6 para los recursos que sean necesarios según el tamaño de NSX Edge.
  - Para una instancia sencilla de NSX Edge son necesarios dos dispositivos NSX Edge del tamaño adecuado que se mantengan encendidos durante la actualización.
  - A partir de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, se implementarán los dos dispositivos de sustitución antes de reemplazar los dispositivos anteriores. Esto significa que habrá cuatro dispositivos NSX Edge de tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualice de nuevo, cualquiera de los dispositivos con HA podrá activarse.
  - Antes de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, solo se implementaba un dispositivo de sustitución a la vez cuando se sustituían los dispositivos antiguos. Esto significa que habrá tres dispositivos NSX Edge del tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualiza, el dispositivo NSX Edge con HA con índice 0 se suele activar.
- Si tiene habilitada la VPN de Capa 2 en NSX Edge, debe eliminar su configuración antes de iniciar la actualización. Después de la actualización, puede volver a configurar la VPN de Capa 2.

Procedimiento

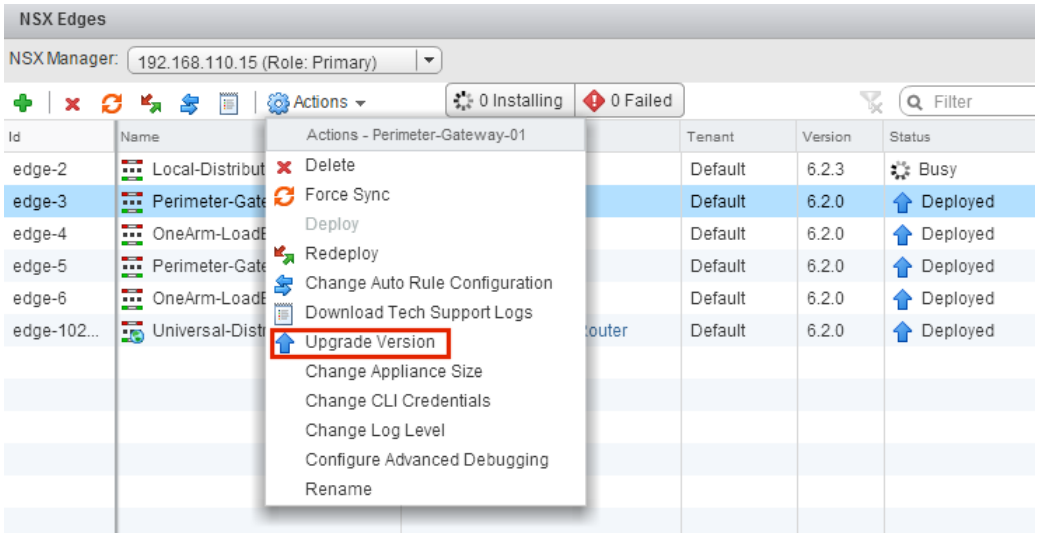
1 En vSphere Web Client, seleccione **Redes y seguridad (Networking & Security) > NSX Edge**.

2 Haga doble clic en cada instancia de NSX Edge y, antes de actualizar, compruebe que tiene establecida la siguiente configuración.

   a Haga clic en **Administrar > VPN > VPN de Capa 2** (Manage > VPN > L2 VPN) y compruebe si la VPN de Capa 2 está habilitada. Si es así, elimine la configuración de la VPN de Capa 2 después de apuntar los detalles de dicha configuración.

   b Haga clic en **Administrar > Enrutamiento > Rutas estáticas** y compruebe si alguna de las rutas estáticas no tiene la configuración del siguiente salto. Si alguna no la tiene, agregue el siguiente salto antes de actualizar NSX Edge.

3 Para cada instancia de NSX Edge, seleccione la opción **Versión de actualización** (Upgrade Version) en el menú **Acciones** (Actions).



   Si en la actualización aparece el mensaje de error "No se pudo implementar el dispositivo Edge" (Failed to deploy edge appliance), asegúrese de que el host donde se implementa el dispositivo NSX Edge esté conectado y no esté en modo de mantenimiento.

Una vez que NSX Edge se actualiza correctamente, el **Estado** (Status) se implementa (Deployed) y la columna **Versión** (Version) muestra la nueva versión de NSX.

Si un dispositivo Edge no se puede actualizar y tampoco hay una reversión a la versión anterior, haga clic en el icono **Volver a implementar NSX Edge** (Redeploy NSX Edge) e intente actualizar nuevamente.

Las reglas del firewall de NSX Edge no admiten sourcePort, por eso las reglas de la versión 5.5 de vShield Edge que contienen sourcePort se modifican durante la actualización tal y como se especifica a continuación:

- Si no existen aplicaciones que se usen en la regla, se crea un servicio con protocol=any, port=any y sourcePort=asDefinedInTheRule.
- Si en la regla se usan aplicaciones o grupos de aplicaciones, estos objetos agrupados se duplican al agregarles el sourcePort. Debido a esto, el identificador groupingObjectIds utilizado en la regla del firewall cambia tras la actualización.

Las reglas de firewall de usuario en NSX Edge 6.x no generan IPSets ni applicationSets internos basados en entradas procedentes de API de REST. En su lugar, se mantendrán en el formato sin procesar. Durante la actualización, el IPSet y los applicationSets generados internamente se utilizan para crear reglas con datos sin procesar. El identificador interno groupingObjects ya no aparecerá en las reglas de firewall (firewallRules) del usuario.

Qué hacer a continuación

Vuelva a configurar la VPN de Capa 2. Consulte la Descripción general de la VPN de Capa 2 en la *Guía de instalación de NSX*.

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

1 Elimine la snapshot de NSX Manager tomada durante la instalación.

2 Realice una copia de seguridad actualizada tras la actualización.

3 Asegúrese de que los VIB estén instalados en los hosts.

NSX Instala los siguientes VIB:

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Si se ha instalado Guest Introspection, compruebe también que este VIB se encuentra en los hosts:

```
esxcli software vib get --vibname epsec-mux
```

4 Vuelva a sincronizar el bus de mensajería del host. VMware aconseja a todos sus clientes que vuelvan a realizar una sincronización tras la actualización.

Puede usar la siguiente llamada API para volver a realizar la sincronización en cada host.

```
URL : 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
```

Actualización de NSX 2

Este capítulo cubre los siguientes temas:

Prepararse para la actualización de NSX

Para garantizar que la actualización de NSX se realice correctamente, asegúrese de revisar las notas de la versión para comprobar si existen problemas de actualización, de usar la secuencia de actualización correcta y de que la infraestructura esté preparada para la actualización.

ADVERTENCIA: Las versiones anteriores no son compatibles:

- Realice siempre una copia de seguridad de NSX Manager antes de realizar una actualización.
- Una vez que NSX Manager se actualiza correctamente, NSX no puede volver a una versión anterior.

VMware recomienda realizar actualizaciones en una ventana de mantenimiento tal y como indica su empresa.

Pueden usarse las siguientes instrucciones como lista de comprobación previa a la actualización.

1. Compruebe que vCenter cumple los requisitos del sistema de NSX. Consulte "Requisitos del sistema para NSX," página 6.
2. Si se implementa un servicio de partners de Guest Introspection, compruebe la compatibilidad antes de la actualización:
   - Consulte la Guía de compatibilidad de VMware para Networking and Security. Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.
   - Consulte la documentación del partner para obtener más detalles sobre compatibilidad y actualización.
3. Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte "Desinstalar NSX Data Security," página 62.
4. Compruebe que cuenta con una copia de seguridad actualizada de NSX Manager, vCenter y otros componentes de NSX. Consulte "Copia de seguridad y restauración de NSX," página 62.
5. Realice un snapshot de NSX Manager, incluida su memoria virtual. Consulte el artículo 2129224.
6. Cree un paquete de servicio técnico.

7 Asegúrese de que la resolución de nombres directa o inversa funcione utilizando el comando nslookup.

8 Si se utiliza VUM en el entorno, compruebe que a la marca bypassVumEnabled se le asigne el valor true en vCenter. Esta opción configura EAM para que instale los VIB directamente en los hosts ESXi aunque VUM esté instalado o no esté disponible. Acceda a la página http://kb.vmware.com/kb/2053782.

9 Descargue y organice el paquete de actualización, y valídelo con md5sum. Consulte "Descargar el paquete de actualización de NSX y comprobar MD5," página 66.

10 Le recomendamos que desactive todas las operaciones del entorno hasta que todas las secciones de la actualización se completen.

11 No apague ni elimine ningún componente ni dispositivo de NSX si no se le indica.

Necesidades de la licencia de evaluación al actualizar NSX

NSX introdujo un nuevo modelo de licencia en mayo de 2016.

Si cuenta con un contrato de soporte activo, cuando actualice una versión anterior de NSX a NSX 6.2.3, su licencia actual se convertirá en una licencia NSX Enterprise y tendrá derecho a las mismas funciones que se ofrece en Enterprise.

Consulte las preguntas más recientes sobre la licencia de NSX en https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Impactos operativos de las actualizaciones de NSX

El proceso de actualización de NSX puede llevar algo de tiempo, especialmente al actualizar hosts ESXi, ya que deben reiniciarse los hosts. Es importante comprender el estado operativo de los componentes de NSX durante una actualización, por ejemplo, cuando se han actualizado algunos hosts pero no todos, o cuando no se han actualizado los dispositivos NSX Edge.

VMware recomienda ejecutar la actualización en una sola ventana de interrupción para minimizar el tiempo de inactividad y reducir la confusión entre los usuarios de NSX que no pueden acceder a ciertas funciones de administración de NSX durante la actualización. Sin embargo, si los requisitos del sitio no permiten completar la actualización en una sola ventana de interrupción, la siguiente información puede ayudar a que los usuarios de NSX comprendan cuáles son las características disponibles durante la actualización.

La actualización de una implementación de NSX se desarrolla de la siguiente manera:

NSX Manager —> Clúster de NSX Controller —> Clústeres de host de NSX—> NSX Edge

Actualización de vCenter

Si utiliza el SSO integrado de vCenter y está actualizando vCenter 5.5 a vCenter 6.0, es posible que vCenter pierda conectividad con NSX. Esto sucede si vCenter 5.5 se registró en NSX con el nombre de usuario raíz A partir de la versión NSX 6.2, ya no se utiliza el registro de vCenter con el nombre de usuario raíz. Como solución alternativa, vuelva a registrar vCenter en NSX con el nombre de usuario administrator@vsphere.local en lugar de utilizar el nombre de usuario raíz.

Si utiliza un SSO externo, no es necesario realizar cambios. Puede mantener el mismo nombre de usuario, por ejemplo, admin@miempresa.midominio, y la conectividad de vCenter no se perderá.

Actualización de NSX Manager

Durante:

- Se bloquea la configuración de NSX Manager. El servicio NSX API no está disponible. No pueden realizarse cambios en la configuración de NSX. La comunicación con las máquinas virtuales existentes sigue funcionando. El nuevo aprovisionamiento de máquinas virtuales continúa funcionando en vSphere, pero las nuevas máquinas virtuales no pueden conectarse con los conmutadores lógicos de NSX durante la actualización de NSX Manager.

Después:

- Se permiten todos los cambios de configuración de NSX. En esta etapa, si se implementa cualquier controladora NSX Controller nueva, esta se inicia con la versión anterior hasta que se actualiza el clúster de NSX Controller existente. Se permiten cambios en la configuración de NSX existente. Pueden implementarse nuevos conmutadores lógicos, enrutadores lógicos y puertas de enlace de servicios Edge. En el caso de firewall distribuido, las nuevas características introducidas después de la actualización, si las hubiera, no estarán disponibles para la configuración (atenuadas) en la interfaz de usuario hasta que se actualicen todos los hosts.

Actualización de clústeres de NSX Controller

Durante:

- La creación de redes lógicas y las modificaciones en ellas están bloqueadas durante el proceso de actualización. No realice cambios en la configuración de redes lógicas mientras la actualización de un clúster de NSX Controller está en curso. No aprovisione máquinas virtuales nuevas durante este proceso. Además, no mueva máquinas virtuales ni permita que DRS mueva máquinas virtuales durante la actualización.

  Durante la actualización, cuando existe un estado temporal no mayoritario, las máquinas virtuales existentes no pierden conectividad de red.

  La creación de redes lógicas nuevas se bloquea automáticamente durante la actualización.

  No permita cambios en las rutas dinámicas durante la actualización.

Después:

- Se permiten cambios en la configuración. Pueden crearse redes lógicas nuevas. Las redes lógicas existentes siguen funcionando.

Actualización de hosts NSX

Durante:

- Los cambios de configuración no están bloqueados en NSX Manager. La actualización se realiza por clúster. Si DRS está habilitado en el clúster, se encarga de administrar el orden de actualización de los hosts. Se permiten cambios y modificaciones en la red lógica. El host que se está sometiendo a una actualización está en modo de mantenimiento. El aprovisionamiento de máquinas virtuales nuevas sigue funcionando en los hosts que no están actualmente en modo de mantenimiento.

Cuando se actualizan algunos hosts NSX en un clúster y otros no:

- No se bloquean los cambios en la configuración de NSX Manager. La comunicación de la controladora al host posee compatibilidad con versiones anteriores, es decir que las controladoras actualizadas pueden comunicarse con los hosts no actualizados. Se permiten cambios y modificaciones en las redes lógicas. El aprovisionamiento de máquinas virtuales sigue funcionando en los hosts que no están sometiéndose a una actualización. Los hosts que se están sometiendo a una actualización se colocan en modo de mantenimiento, por los que las máquinas virtuales deben apagarse o evacuarse a otros hosts. Esto puede realizarse con DRS o manualmente.

Actualización de NSX Edge

Pueden actualizarse dispositivos NSX Edge sin ningún tipo de dependencia de las actualizaciones de NSX Controller o de hosts. Puede actualizar un dispositivo NSX Edge incluso si todavía no ha actualizado NSX Controller o los hosts.

Durante:

- En el dispositivo NSX Edge que se está actualizando, se bloquean los cambios de configuración. Se permiten cambios y modificaciones en los conmutadores lógicos. El aprovisionamiento de máquinas virtuales nuevas sigue funcionando.
- El envío de paquetes se interrumpió temporalmente.
- En NSX Edge 6.0 y en versiones posteriores, las adyacencias OSPF se retiran durante la actualización si no se habilita el reinicio estable.

Después:

- No se bloquean los cambios de configuración. Todas las características nuevas introducidas en la actualización de NSX no serán configurables hasta que todas las controladoras NSX Controller y todos los clústeres de hosts se actualicen a la versión 6.2.x de NSX.
- La VPN de Capa 2 se debe volver a configurar después de la actualización.
- Los clientes de VPN SSL se deben volver a instalar después de la actualización.

Actualización de Guest Introspection

Durante una actualización de NSX, la interfaz de usuario de NSX le solicita que actualice el servicio Guest Instrospection.

Durante:

- Cuando se realiza un cambio en las máquinas virtuales, estas tienen menos protección en el clúster de NSX, por ejemplo, eliminaciones, vMotions o adiciones en la máquina virtual.

Después:

- Las máquinas virtuales están protegidas cuando se realiza en ellas adiciones, vMotions y eliminaciones.

Comprobar el estado de funcionamiento de NSX

Antes de empezar la actualización, es importante probar el estado de funcionamiento de NSX. De lo contrario, no podrá determinar si los problemas posteriores a la actualización ocurrieron debido al proceso de actualización o si ya existían.

No dé por sentado que todo funciona correctamente antes de empezar a actualizar la infraestructura de NSX. Asegúrese de revisarla primero.

Procedimiento

1 Observe las versiones actuales de NSX Manager, vCenter Server, ESXi y NSX Edge.

2 Identifique las contraseñas y los identificadores de usuario administrador.

3 Compruebe que puede iniciar sesión en los siguientes componentes:

   - vCenter Server
   - Interfaz de usuario de NSX Manager Web
   - Dispositivos de puerta de enlace de los servicios Edge
   - Dispositivos del enrutador lógico distribuido

- Dispositivos NSX Controller

4 Compruebe que los segmentos de la VXLAN funcionen.

Asegúrese de establecer el tamaño del paquete correctamente y de incluir el bit "don't fragment" (no fragmentar).

- Puede hacer ping entre dos máquinas virtuales que corresponden al mismo conmutador lógico pero están en dos hosts diferentes.
  - Desde una máquina virtual Windows: haga ping en -l 1472 –f <dest VM>
  - Desde una máquina virtual Linux: haga ping en -s 1472 –M do <dest VM>
- Puede hacer ping entre las interfaces VTEP de dos hosts.
  - hacer ping en ++netstack=vxlan -d -s 1572 <dest VTEP IP>

  NOTA: Para obtener la dirección IP VTEP de un host, busque la dirección IP vmknicPG en la página **Administrar > Redes > Conmutadores virtuales** (Manage > Networking > Virtual Switches) del host.

5 Valide la conectividad Norte-Sur. Para ello, haga ping hacia afuera desde una máquina virtual.

6 Inspeccione visualmente el entorno de NSX para asegurarse de que todos los indicadores de estado estén en color verde, muestren una condición normal y estén implementados.

- Revise **Instalación > Administración** (Installation > Management).
- Revise **Instalación > Preparación del host** (Installation > Host Preparation).
- Revise **Instalación > Preparación de red lógica > Transporte de VXLAN** (Installation > Logical Network Preparation > VXLAN Transport).
- Revise **Conmutadores lógicos** (Logical Switches).
- Revise **NSX Edge**.

7 Registre los estados de BGP y OSPF en los dispositivos NSX Edge.

- `show ip ospf neighbor`
- `show ip bgp neighbor`
- `show ip route`

8 Compruebe que Syslog esté configurado.

Consulte Especificar un servidor de Syslog (Specify a Syslog Server).

9 Si es posible, en el entorno previo a la actualización, cree algunos componentes nuevos y pruebe que funcionen.

- Cree un nuevo conmutador lógico.
- Cree una nueva puerta de enlace de servicios Edge y un nuevo enrutador lógico distribuido.
- Conecte una máquina virtual al nuevo conmutador lógico y pruebe que funcione.

10 Valide las conexiones de agente del ámbito del usuario (UWA) netcpad y vsfwd.

- En un host ESXi, ejecute `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` y revise el estado de conexión de la controladora.
- En NSX Manager, ejecute el comando `show tech-support save session` y busque el valor "5671" para garantizar que todos los hosts estén conectados a NSX Manager.

11 (Opcional) Si cuenta con un entorno de prueba, pruebe que funcionen las opciones de actualización y posteriores a la actualización antes de actualizar el entorno de un producto.

Desinstalar NSX Data Security

Desinstale NSX Data Security si ya no lo usa o si está actualizando NSX Manager. NSX Data Security no es compatible con una actualización directa. Antes de actualizar NSX Manager, es importante desinstalar NSX Data Security y volver a instalarlo después de la actualización.

Desde la versión 6.2.3 de NSX, la función de seguridad de datos de NSX pasó a estar obsoleta. En la versión 6.2.3 de NSX puede seguir utilizando esta función como desee, pero tenga en cuenta que se eliminará de NSX en versiones futuras.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

2 Seleccione el servicio NSX Data Security y haga clic en el icono **Eliminar implementación de servicios** () (Delete Service Deployment).

3 En el cuadro de diálogo Confirmar eliminación (Confirm Delete), haga clic en **Eliminar ahora** (Delete now) o seleccione la fecha y hora en que tendrá lugar la eliminación.

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

Copia de seguridad y restauración de NSX

Realizar copias de seguridad apropiadas de todos los componentes de NSX es crucial para restaurar el sistema a su estado funcional en caso de errores.

La copia de seguridad de NSX Manager contiene toda la configuración de vShield, incluidas las controladoras, la conmutación lógica, las entidades en red, la seguridad, las reglas de firewall y todo lo que configure dentro de la UPI o la API de NSX Manager. Se debe realizar una copia de seguridad por separado de la base de datos de vCenter y los elementos relacionados como por ejemplo, los conmutadores virtuales.

Como mínimo, recomendamos realizar copias de seguridad regulares de NSX Manager y vCenter. La frecuencia y la programación de las copias de seguridad pueden variar según las necesidades comerciales y los procedimientos operativos. Recomendamos realizar copias de seguridad de NSX con frecuencia en momentos de cambios de configuración continuos.

Las copias de seguridad de NSX Manager pueden realizarse a petición o por hora, por día o por semana.

Recomendamos realizar copias de seguridad en las siguientes situaciones:

- Antes de una actualización de NSX o vCenter.
- Después de una actualización de NSX o vCenter.
- Después de una implementación desde cero y de la configuración inicial de componentes de NSX. Por ejemplo, después de crear controladoras NSX Controller, conmutadores lógicos, enrutadores lógicos, puertas de enlace de servicios Edge y directivas de seguridad y firewall.
- Después de cambios de infraestructura o topología.
- Después de cualquier cambio importante de día 2.

Para proporcionar el estado de todo un sistema al que se pueda revertir en un momento determinado, se recomiendan sincronizar las copias de seguridad de los componentes de NSX (por ejemplo, NSX Manager) con la programación de copias de seguridad de otros componentes con los que exista interacción, como vCenter, sistemas de administración en la nube, herramientas operativas, etc.

Hacer copias de seguridad de los datos de NSX Manager

Para hacer copias de seguridad de los datos de NSX Manager, puede hacer una copia de seguridad a petición o una copia de seguridad programada.

La copia de seguridad y la restauración de NSX Manager pueden configurarse desde la interfaz web del dispositivo virtual de NSX Manager o a través de la API de NSX Manager Las copias de seguridad pueden programarse por hora, por día o por semana.

El archivo de copia de seguridad se guarda en una ubicación de FTP o SFTP remota a la que NSX Manager tenga acceso. Los datos de NSX Manager incluyen tablas de configuración, de eventos y de registros de auditoría. Las tablas de configuración se incluyen en todas las copias de seguridad.

La restauración solo se permite en la misma versión de NSX Manager que la versión de la copia de seguridad. Por este motivo, es importante crear un nuevo archivo de copia de seguridad antes y después de realizar una actualización de NSX, una para la versión anterior y otra para la nueva.

Procedimiento

1 Inicie sesión en el dispositivo virtual de NSX Manager.

2 En Administración de dispositivos (Appliance Management), haga clic en **Copias de seguridad y restauración** (Backups & Restore).

3 Para especificar la ubicación de la copia de seguridad, haga clic en **Cambiar** (Change), junto a Configuración de servidor FTP (FTP Server Settings).

   a Escriba la dirección IP o el nombre del host del sistema de copia de seguridad.

   b En el menú desplegable **Protocolo de transferencia** (Transfer Protocol), seleccione **SFTP** o **FTP**, según lo que admita el destino.

   c Si es necesario, edite el puerto predeterminado.

   d Escriba el nombre de usuario y la contraseña requeridos para iniciar sesión en el sistema de copia de seguridad.

   e En el campo **Directorio de copia de seguridad** (Backup Directory), escriba la ruta de acceso absoluta donde se almacenarán las copias de seguridad.

   Para determinar la ruta de acceso absoluta, puede iniciar sesión en el servidor FTP, desplazarse hasta el directorio que desea utilizar y ejecutar el comando de directorio de trabajo presente (`pwd`). Por ejemplo:

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

f Escriba una cadena de texto en **Prefijo de nombre de archivo** (Filename Prefix).

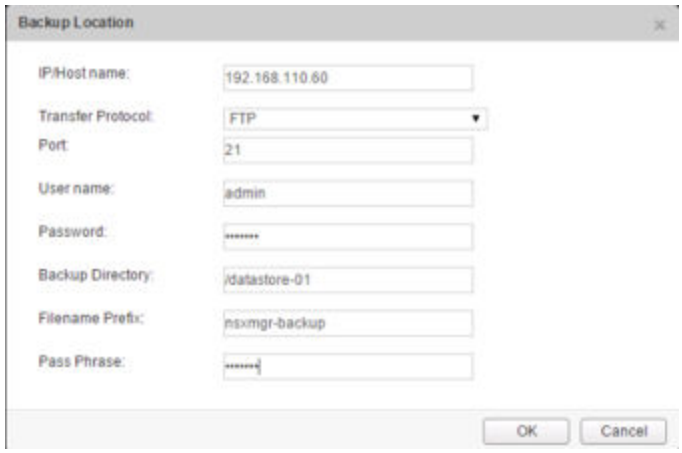
Este texto se agrega antes del nombre de archivo de cada copia de seguridad para que el sistema de copia de seguridad lo reconozca fácilmente. Por ejemplo, si escribe **ppdb**, la copia de seguridad resultante se denominará `ppdbHH_MM_SS_DayDDMonYYYY`.

g Escriba la frase de contraseña para proteger la copia de seguridad.

Necesitará esta frase de contraseña para restaurar la copia de seguridad.

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

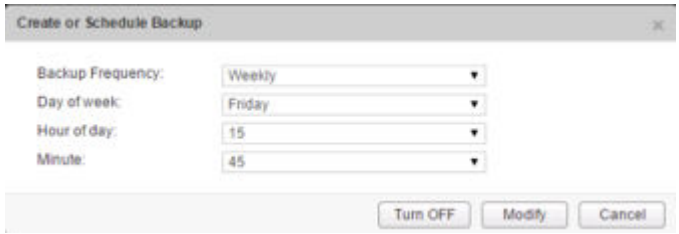
Por ejemplo:



4 En el caso de una copia de seguridad a petición, haga clic en **Copia de seguridad** (Backup).

Se agrega un archivo nuevo en **Historial de copias de seguridad** (Backup History).

5 En el caso de una copia de seguridad programada, haga clic en **Cambiar** (Change), junto a Programación (Scheduling).



a En el menú desplegable **Frecuencia de copia de seguridad** (Backup Frequency), seleccione **Por hora** (Hourly), **Por día** (Daily) o **Por semana** (Weekly). Los menús desplegables Día de la semana (Day of Week), Hora del día (Hour of Day) y Minuto (Minute) se deshabilitan según la frecuencia seleccionada. Por ejemplo, si selecciona Por día (Daily), el menú desplegable Día de la semana (Day of Week) se deshabilita, ya que este campo no se aplica a una frecuencia diaria.

b Para las copias de seguridad por semana, seleccione el día de la semana en que debe realizarse una copia de seguridad de los datos.

c Para las copias de seguridad por semana o por día, seleccione la hora en que debe iniciarse la copia de seguridad.

d Seleccione el minuto en que desea comenzar y haga clic en **Programar** (Schedule).

6 Para excluir datos de registros y flujos de la copia de seguridad, haga clic en **Cambiar** (Change), junto a Excluir (Exclude).

   a Seleccione los elementos que desea excluir de la copia de seguridad.

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

7 Guarde la dirección IP o el nombre del host, las credenciales, los detalles de directorio y la frase de contraseña del servidor FTP. Esta información es necesaria para restaurar la copia de seguridad.

Restaurar una copia de seguridad de NSX Manager

La restauración de NSX Manager provoca que se cargue un archivo de copia de seguridad en un dispositivo NSX Manager. El archivo de copia de seguridad debe guardarse en una ubicación de FTP o SFTP remota a la que tenga acceso NSX Manager. Los datos de NSX Manager incluyen tablas de configuración, de eventos y de registros de auditoría.

IMPORTANTE: Haga una copia de seguridad de los datos actuales antes de restaurar un archivo de copia de seguridad.

Prerequisitos

Antes de restaurar los datos de NSX Manager, se recomienda volver a instalar el dispositivo NSX Manager. Ejecutar la operación de restauración en un dispositivo NSX Manager existente también podría ser efectivo, pero no posee soporte oficial. Se da por sentado que el dispositivo NSX Manager existente posee errores y, en consecuencia, se implementa un nuevo dispositivo NSX Manager.

La práctica recomendada es realizar capturas de pantalla o tomar notas de la configuración actual del dispositivo NSX Manager antiguo para utilizarlas en el momento de especificar la información de dirección IP y ubicación de copias de seguridad del dispositivo NSX Manager recientemente implementado.

Procedimiento

1 Realice capturas de pantalla o anote todas las opciones de configuración del dispositivo NSX Manager existente.

2 Implemente un nuevo dispositivo NSX Manager.

   La versión debe ser igual a la del dispositivo NSX Manager de la copia de seguridad.

3 Inicie sesión en el dispositivo NSX Manager nuevo.

4 En Administración de dispositivos (Appliance Management), haga clic en **Copias de seguridad y restauración** (Backups & Restore).

5 En Configuración del servidor FTP (FTP Server Settings), haga clic en **Cambiar** (Change) y agregue las opciones de configuración.

   En los campos **Dirección IP de host** (Host IP Address), **Nombre de usuario** (User Name), **Contraseña** (Password), **Directorio de copia de seguridad** (Backup Directory), **Prefijo de nombre de archivo** (Filename Prefix) y **Frase de contraseña** (Pass Phrase) en la pantalla Ubicación de copia de seguridad (Backup Location) se debe poder identificar la ubicación de la copia de seguridad que se desea restaurar.

6 En la sección Historial de copias de seguridad (Backups History), active la casilla de la copia de seguridad que desea restaurar y haga clic en **Restaurar** (Restore).

Hacer copias de seguridad de NSX Edge

Se hacen copias de seguridad de todas las configuraciones de NSX Edge (enrutadores lógicos y puertas de enlace de servicios Edge) como parte de las copias de seguridad de datos de NSX Manager.

Si tiene una configuración de NSX Manager intacta, puede recrear una máquina virtual de dispositivo Edge inaccesible o con errores volviendo a implementar NSX Edge (haga clic en el icono **Volver a implementar NSX Edge** [Redeploy NSX Edge] en vSphere Web Client).

No se admite la realización de copias de seguridad individuales de NSX Edge.

Hacer copias de seguridad de conmutadores distribuidos de vSphere

Puede exportar la configuración de un conmutador distribuido de vSphere y de un grupo de puertos distribuidos a un archivo.

El archivo conserva los valores de red válidos, lo que permite la distribución de estos valores a otras implementaciones.

Esta funcionalidad solo está disponible con vSphere Web Client 5.1 o posterior. La configuración de VDS y la configuración del grupo de puertos se incluyen en la importación.

La práctica recomendada consiste en importar la configuración de VDS antes de preparar el clúster para VXLAN. Para obtener instrucciones detalladas, consulte http://kb.vmware.com/kb/2034602.

Hacer una copia de seguridad de vCenter

Para proteger la implementación de NSX, es importante hacer una copia de seguridad de la base de datos de vCenter y crear instantáneas de las máquinas virtuales.

Consulte la documentación de su versión de vCenter para conocer los procedimientos y las prácticas recomendadas de copias de seguridad y restauraciones de vCenter.

Para las instantáneas de máquinas virtuales, consulte http://kb.vmware.com/kb/1015180.

Vínculos útiles para vCenter 5.5:

- http://kb.vmware.com/kb/2057353
- http://kb.vmware.com/kb/2034505
- http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf

Vínculos útiles para vCenter 6.0:

- https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
- http://kb.vmware.com/kb/2110294

Descargar el paquete de actualización de NSX y comprobar MD5

El paquete de actualización de NSX contiene todos los archivos necesarios para actualizar la infraestructura de NSX. Antes de actualizar NSX Manager, en primer lugar debe descargar el paquete de actualización de la versión a la que desea actualizar.

Prerequisitos

Una herramienta de suma de comprobación de MD5.

Procedimiento

1 Descargue el paquete de actualización de NSX en una ubicación a la que NSX Manager pueda acceder. El nombre del archivo del paquete de actualización tiene un formato similar a `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz`.

2 Compruebe que el nombre del archivo de la actualización de NSX Manager acabe en tar.gz.

Es posible que algunos exploradores alteren la extensión del archivo. Por ejemplo, si el nombre del archivo descargado es:

VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz

Cámbielo a:

VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.tar.gz

En caso contrario, después de cargar el paquete de actualización, aparecerá el siguiente mensaje de error : "Archivo no válido de paquete de actualización VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx,gz, el nombre del archivo de actualización tiene la extensión tar.gz" (Invalid upgrade bundle file VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx,gz, el nombre de archivo de actualización tiene la extensión tar.gz).

3 Utilice una herramienta de suma de comprobación MD5 para comparar la suma MD5 oficial del paquete de actualización mostrada en el sitio web de VMware con la suma MD5 calculada por la herramienta de suma de comprobación.

a En la herramienta de suma de comprobación MD5, desplácese hasta el paquete de actualización.

b Utilice la herramienta para calcular la suma de comprobación del paquete.

c Pegue la suma de comprobación indicada en el sitio web de VMware.

d Utilice la herramienta para comparar las dos sumas de comprobación.

Si las dos sumas de comprobación no coinciden, repita la descarga del paquete de actualización.

Actualizar de NSX 6.1.x o 6.2.x a NSX 6.2.x

Para actualizar a NSX 6.2.x, debe actualizar los componentes de NSX en el orden documentado en esta guía.

Los componentes de NSX deben actualizarse en el siguiente orden:

1 Dispositivo NSX Manager

2 NSX Controller clúster

3 Clústeres de hosts

4 NSX Edge

5 Guest Introspection

La administración del proceso de actualización está a cargo de NSX Manager. Si ocurre un error en la actualización de un componente o si se interrumpe y es necesario repetirla o reiniciarla, el proceso empieza por el punto donde se detuvo y no desde el principio.

El estado de la actualización se actualiza en cada nodo y en el nivel del clúster.

Actualizar NSX Manager

El primer paso en el proceso de actualización de la infraestructura NSX es actualizar el dispositivo NSX Manager.

Durante la actualización, es posible unirse al Programa de mejora de la experiencia de cliente (CEIP) de NSX. Consulte el Programa de mejora de la experiencia de cliente en *Guía de administración de NSX* para obtener más información acerca del programa, incluyendo cómo unirse o salir de él.

Prerequisitos

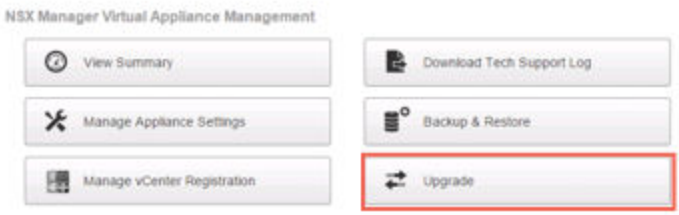
- Compruebe el uso del sistema de archivos de NSX Manager y realice una limpieza si el uso de dicho sistema está al 100 por cien.
  a Inicie sesión en NSX Manager y habilite `show filesystems` para mostrar el uso del sistema de archivos /dev/sda2.
  b Si el uso está al 100 por cien, ejecute los comandos `purge log manager` y `purge log system`.
  c Reinicia el dispositivo NSX Manager para poder realizar la limpieza del registro.
- Antes de actualizar a NSX 6.2.x, aumente la memoria reservada del dispositivo virtual NSX Manager como mínimo, a 16 GB.

  Consulte "Requisitos del sistema para NSX," página 6.
- Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte "Desinstalar NSX Data Security," página 62.
- Haga una copia de seguridad de la configuración actual y descargue los registros de soporte técnico antes de actualizar. Consulte "Copia de seguridad y restauración de NSX," página 62.
- Descargue el paquete de actualización y compruebe MD5. Consulte "Descargar el paquete de actualización de NSX y comprobar MD5," página 66.
- Asegúrese de entender el impacto operativo que produce la actualización de NSX Manager cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.

Procedimiento

1 Inicie sesión en el dispositivo virtual NSX Manager.

2 En la página de inicio de NSX Manager, haga clic en **Actualizar** (Upgrade).



3 Haga clic en **Actualizar** (Upgrade) y, a continuación, en Seleccionar archivo`VMware-NSX-Manager-upgrade-bundle-` (Choose File) y desplácese hasta el archivo *releaseNumber-NSXbuildNumber*`.tar.gz`. Haga clic en **Continuar** (Continuar) para iniciar la migración.

El estado de la carga se muestra en la ventana del explorador.

4 En el cuadro de diálogo, especifique si desea habilitar SSH y si desea participar en el Programa de mejora de la experiencia de cliente (CEIP) de VMware. Haga clic en **Actualizar** (Upgrade) para iniciar la actualización.

El estado de la actualización se muestra en la ventana del explorador.

Espere a que el procedimiento de actualización se complete y aparezca la página de inicio de sesión en NSX Manager.

5 Inicie sesión nuevamente en el dispositivo virtual NSX Manager y confirme que el estado de actualización sea **Finalizado** (Complete) y que los números de versión y compilación en la parte superior derecha coincidan con el paquete de actualización recientemente instalado.

Después de actualizar NSX Manager y de conectarlo a una instancia de vCenter Server existente, restablezca el servidor Web Client para permitir que también se actualicen los complementos de NSX.

- También puede hacer esto en vCenter 5.5. Para ello, abra https://<vcenter-ip>:5480 y reinicie el servidor Web Client.
- Para hacerlo en vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como raíz y ejecute los comandos siguientes.

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- En vCenter Server 6.0, puede ejecutar los siguientes comandos en Windows.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Se requiere reiniciar para evitar errores inesperados, como grupos de seguridad configurados que no aparecen en la pestaña **Grupos de seguridad** (Security Groups) de Service Composer.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su navegador.

Se recomienda utilizar diferentes servidores Web Client para administrar los servidores vCenter Server que ejecutan distintas versiones de NSX Manager a fin de evitar errores inesperados cuando diferentes versiones de complementos de NSX están en ejecución.

Una vez actualizado NSX Manager, cree un nuevo archivo de copia de seguridad de NSX Manager. Consulte "Copia de seguridad y restauración de NSX," página 62. La copia de seguridad anterior de NSX Manager solo es válida para la versión anterior.

Qué hacer a continuación

Actualice el clúster de NSX Controller.

Actualizar el clúster de NSX Controller

Las controladoras del entorno se actualizan en el nivel del clúster. Si hay una actualización disponible para un nodo de controladora, aparece un vínculo de actualización en NSX Manager.

Se recomienda actualizar las controladoras durante un período de mantenimiento.

La actualización de NSX Controller produce la descarga de un archivo de actualización en cada nodo de controladora. Las controladoras se actualizan de a una por vez. Mientras una actualización está en curso, no es posible seleccionar el vínculo **Actualización disponible** (Upgrade Available), y las llamadas API para actualizar el clúster de la controladora se bloquean hasta que finaliza la actualización.

Si se implementan controladoras nuevas antes de que se actualicen las existentes, se implementan en la versión anterior. Los nodos de controladora deben ser de la misma versión para poder unirse a un clúster.

Prerequisitos

- Asegúrese de que todas las controladoras estén en estado normal. La actualización no es posible si una o varias controladoras están en estado desconectado. Para reconectar una controladora desconectada, intente restablecer el dispositivo virtual de la controladora. En la vista **Hosts y clústeres** (Hosts and Clusters), haga clic con el botón derecho en la controladora y seleccione **Alimentación > Restablecer** (Power > Reset).

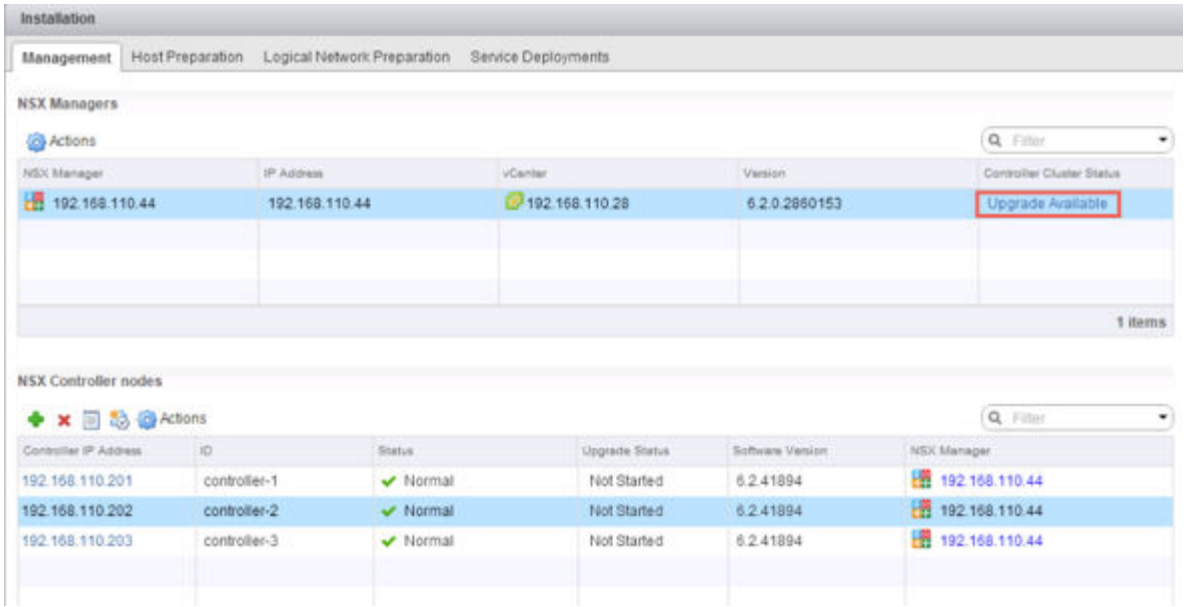
- Un clúster de NSX Controller válido contiene tres nodos de controladora. Inicie sesión en los tres nodos de controladora y ejecute el comando **show controller-cluster status**.

```
controller-node# show control-cluster status

Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   05/04 02:36:03
Majority status:    Connected to cluster majority                   05/19 23:57:23
Restart status:     This controller can be safely restarted         05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  - En el estado Unirse (Join), compruebe que el nodo de controladora informe sobre el estado Unión completa (Join Complete).
  - En el estado Mayoría (Majority), compruebe que la controladora esté conectada a la mayoría del clúster.
  - En el identificador del clúster, todos los nodos de controladora de un clúster deben tener el mismo identificador de clúster.
  - En los estados Configurado (Configured) y Activo (Active), compruebe que todas las funciones de la controladora están habilitadas y activadas.
- Asegúrese de entender el impacto operativo que produce la actualización de NSX Controller cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.

Procedimiento

- En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation), seleccione la pestaña **Administración** (Management) y haga clic en **Actualización disponible** (Upgrade Available) en la columna **Estado de clúster de controladora** (Controller Cluster Status).



  Las controladoras del entorno se actualizan y se reinician de a una por vez. Después de iniciar la actualización, el sistema descarga el archivo de actualización, actualiza y reinicia cada controladora, y actualiza el estado de actualización de cada controladora. Los siguientes campos muestran el estado de la controladora:

  - La columna **Estado de clúster de controladora** (Controller Cluster Status) de la sección NSX Manager muestra el estado de actualización del clúster. Cuando la actualización se inicia, el estado muestra el mensaje **Descargando archivo de actualización** (Downloading upgrade file). Una vez que se descargó el archivo de actualización en todas las controladoras del clúster, el estado cambia a **En curso** (In progress). Una vez actualizadas todas las controladoras del clúster, el estado que aparece es **Finalizado** (Complete) y la columna ya no se muestra.
  - La columna **Estado** (Status) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de cada controladora, que empieza siendo **Normal**. Cuando los servicios de la controladora se apagan y se reinicia la controladora, el estado cambia a **Desconectada** (Disconnected). Una vez completada la actualización de la controladora, el estado vuelve a ser **Normal**.
  - La columna **Estado de actualización** (Upgrade Status) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de actualización de cada controladora. El primer estado que se muestra es **Descargando archivo de actualización** (Downloading upgrade file), después aparece **Actualización en curso** (Upgrade in progress) y, por último, **Reiniciando** (Rebooting). Cuando la controladora está actualizada, el estado indica **Actualizada** (Upgraded).

Una vez completada la actualización, la columna **Versión de software** (Software Version) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el número **6.2.***buildNumber* para cada controladora. Vuelva a ejecutar el comando **show controller-cluster status** para garantizar que las controladoras puedan crear una mayoría. Si no se vuelve a formar la mayoría del clúster de NSX Controller, revise los registros de la controladora y de NSX Manager.

El tiempo promedio para cada actualización es de 6 a 8 minutos. Si la actualización no se completa dentro del período de espera (30 minutos), la columna **Estado de actualización** (Upgrade Status) muestra **Con errores** (Failed). Haga clic nuevamente en **Actualización disponible** (Upgrade Available) en la sección NSX Manager para reanudar el proceso desde el punto donde se detuvo.

Si los problemas de red impiden que la actualización se realice correctamente dentro del período de espera de 30 minutos, debe configurar un tiempo de espera más largo. Para diagnosticar y solucionar cualquier problema subyacente, puede trabajar con el equipo de soporte técnico de VMware y, si fuera necesario, configurar un período de espera más largo.

Si la actualización de la controladora tiene errores, revise la conectividad entre las controladoras y NSX Manager.

Hay casos en los que la primera controladora se actualiza correctamente y la segunda no lo hace. Supongamos que el clúster tiene tres controladoras: la primera se actualizó correctamente a la nueva versión y la segunda se está actualizando. Si la actualización de la segunda controladora tiene errores, esta controladora podría quedar en estado desconectado. Al mismo tiempo, la primera controladora y la tercera ahora tienen dos versiones diferentes (una actualizada y la otra, no), por lo cual no pueden formar una mayoría. En este punto, la actualización no puede reiniciarse. Para solucionar este problema, cree otra controladora. La nueva controladora tendrá la versión anterior (coincidente con la tercera controladora) y, por lo tanto, formará una mayoría con la tercera controladora. En este punto, se puede reiniciar el procedimiento de actualización.

Póngase en contacto con el equipo de soporte técnico de VMware para poder restaurar la instantánea de la controladora. La instantánea corresponde únicamente a los datos de la controladora de la misma versión. Las instantáneas no pueden restaurarse a una versión más reciente. En otras palabras: no intente aplicar una instantánea a una controladora correctamente actualizada.

Qué hacer a continuación

Actualice los clústeres de hosts.

Actualizar los clústeres de host

Después de actualizar NSX Manager y las instancias de NSX Controller a la versión 6.2.x, se pueden actualizar los clústeres correspondientes del entorno. Durante este proceso, se actualiza el software de cada host del clúster y, a continuación, el host se reinicia.

IMPORTANTE: Cuando se actualizan hosts ESXi con estado junto con NSX, hay un orden de actualización que debe respetarse:

1 Actualice NSX Manager.

2 Actualice el clúster de NSX Controller.

3 Coloque manualmente los hosts ESXi en modo de mantenimiento.

4 Actualice los VIB de NSX (este procedimiento).

5 Reinicie los hosts (para obtener los VIB 5.5).

6 Actualice los hosts ESXi a la versión 6.0.

7 Vuelva a iniciar los hosts ESXi (para obtener los VIB 6.0).

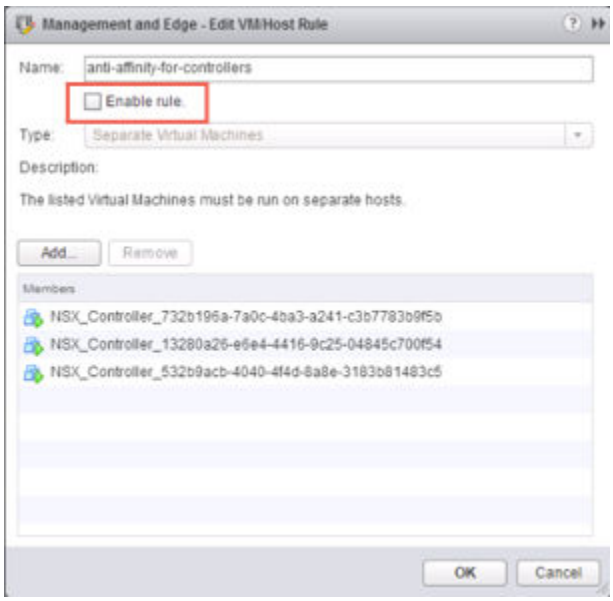
8 Extraiga manualmente los hosts ESXi del modo de mantenimiento.

Conserve los hosts en el modo de mantenimiento durante este proceso. No permita que salgan del modo de mantenimiento antes de tiempo.

Prerequisitos

- Asegúrese de que puedan resolverse los nombres de dominio completos (FQDN) de todos los hosts.

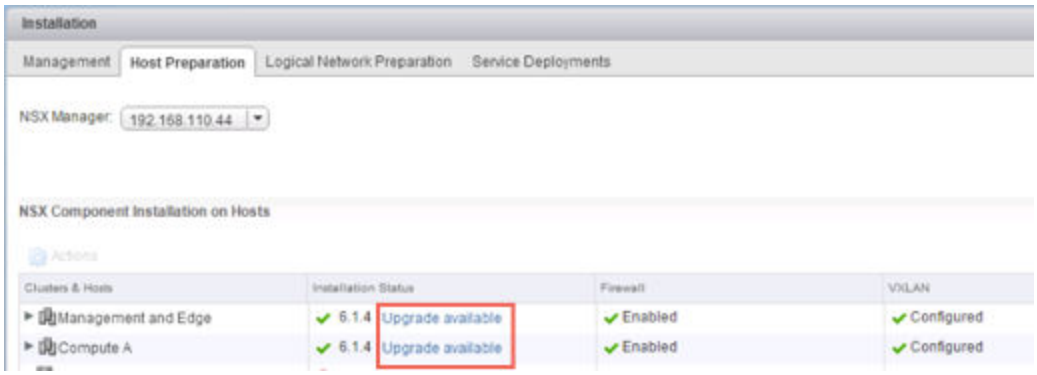
- Inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list`. Observe la versión actual de los siguientes VIB:
  - esx-vsip
  - esx-vxlan
  - esx-dvfilter-switch-security: si actualiza a una versión de NSX posterior a la versión 6.2.
- Actualice NSX Manager y el clúster de NSX Controller.
- Asegúrese de entender el impacto operativo que produce la actualización de un clúster de hosts cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.
- Si DRS está deshabilitado, apague o transfiera por vMotion las máquinas virtuales manualmente antes de empezar la actualización.
- Si DRS está habilitado, las máquinas virtuales en ejecución se moverán automáticamente durante la actualización del clúster de hosts. Antes de iniciar la actualización, asegúrese de que DRS funcione en el entorno.
  - Asegúrese de que DRS esté habilitado en los clústeres del host.
  - Asegúrese de que vMotion funcione correctamente.
  - Compruebe el estado de la conexión del host con vCenter.
  - Compruebe si cuenta con tres hosts ESXi como mínimo en cada clúster de hosts. Durante una actualización de NSX, hay más probabilidades de que un clúster de hosts con solo uno o dos hosts presente problemas con el control de admisión de DRS. Para que la actualización de NSX funcione, VMware recomienda que cada clúster de hosts tenga al menos tres hosts. Si un clúster contiene menos de tres hosts, se recomienda evacuarlos manualmente.
  - En un clúster pequeño con solo dos o tres hosts, si se crearon reglas de antiafinidad por las cuales ciertas máquinas virtuales deben residir en hosts distintos, estas reglas pueden impedir que DRS mueva las máquinas virtuales durante la actualización. Agregue más hosts al clúster o deshabilite las reglas de antiafinidad durante la actualización y vuelva a habilitarlas una vez completada la actualización. Para deshabilitar una regla de antiafinidad, desactive **Habilitar regla** (Enable rule).



Procedimiento

1 En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation), y seleccione la pestaña **Preparación del host** (Host Preparation).

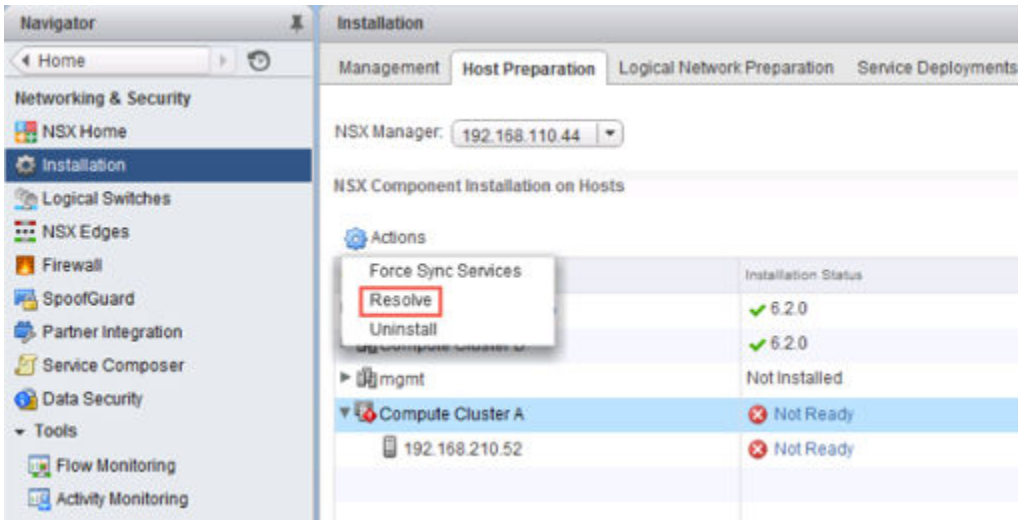
2 Para cada clúster que desea actualizar, haga clic en **Actualización disponible** (Upgrade available).



La actualización del host inicia un análisis del host. Los VIB anteriores se eliminan (aunque no desaparecen por completo hasta después del reinicio). Los nuevos VIB se instalan en la partición altboot. Para ver los nuevos VIB en un host que aún no se reinició, se puede ejecutar el comando `esxcli software vib list --rebooting-image | grep esx`.

Si el clúster tiene DRS habilitado, DRS intenta reiniciar los hosts de una forma controlada que permite que las máquinas virtuales continúen en ejecución. vMotion mueve las máquinas virtuales en ejecución a otros hosts del clúster y coloca al host en el modo de mantenimiento. Si se requiere colocar los hosts manualmente en el modo de mantenimiento (por ejemplo, debido a requisitos de HA o a reglas de DRS), el proceso de actualización se detiene y el clúster **Estado de instalación** (Installation Status) muestra la opción **No está listo** (Not Ready). Haga clic en para mostrar los errores.

Después de evacuar manualmente los hosts, seleccione el clúster y haga clic en la acción **Resolver** (Resolve). La acción **Resolver** (Resolve) intenta completar la actualización y reinicia todos los hosts del clúster. Si se produce un error en el reinicio del host por alguna razón, la acción **Resolver** (Resolve) se detiene. Compruebe el estado de los hosts en la vista **Hosts y clústeres** (Hosts and Clusters) y asegúrese de que estén encendidos, conectados y que no contengan máquinas virtuales en ejecución. A continuación, vuelva a intentar ejecutar la acción **Resolver** (Resolve).



Cuando el clúster está actualizado, la columna **Estado de instalación** (Installation Status) muestra la versión de software a la que se actualizó.

Para confirmar la actualización del host, inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list | grep esx`. Asegúrese de que los siguientes VIB estén actualizados a la versión prevista.

- esx-vsip

- esx-vxlan

NOTA: En NSX 6.2 y versiones posteriores, el VIB esx-dvfilter-switch-security se incluye dentro del VIB esx-vxlan.

Si la actualización de un host tiene errores, soluciónelos con los siguientes pasos:

- Revise ESX Agent Manager en vCenter y busque alertas y errores.
- Inicie sesión en el host, compruebe el archivo de registro `/var/log/esxupdate.log` y, a continuación, busque errores y alertas recientes.
- Asegúrese de que DNS y NTP estén configurados en el host.

Qué hacer a continuación

"Cambiar el puerto de VXLAN," página 75

Cambiar el puerto de VXLAN

Es posible cambiar el puerto utilizado para el tráfico de VXLAN.

En NSX 6.2.3., el puerto VXLAN predeterminado es el 4789, el puerto estándar que asigna la IANA. Antes de NSX 6.2.3, el número de puerto UDP de VXLAN predeterminado era el 8472.

Las instalaciones nuevas de NSX utilizarán el puerto UDP 4789 para VXLAN.

Si en la actualización a NSX 6.2.3 y en la instalación se utilizó el puerto antiguo predeterminado (8472) o un número de puerto personalizado predeterminado (por ejemplo, el 8888) antes de la actualización, dicho puerto seguirá utilizándose tras la actualización a menos que realice los pasos necesarios para cambiarlo.

Si la instalación que actualizó utiliza o utilizará puertas de enlace de VTEP de hardware (puertas de enlace ToR), debe cambiar al puerto 4789 de VXLAN.

No es necesario que utilice el puerto 4789 para el puerto VXLAN en Cross-vCenter NSX; sin embargo, todos los hosts de un entorno de Cross-vCenter NSX deben estar configurados para usar el mismo puerto VXLAN. Si cambia al puerto 4789, garantiza que las nuevas instalaciones de NSX agregadas al entorno de Cross-vCenter NSX utilizan el mismo puerto que las implementaciones de NSX.

El cambio del puerto de VXLAN se realiza en un proceso de tres fases y no interrumpirá el tráfico de VXLAN. En un entorno de Cross-vCenter NSX, el cambio se propagará a todos los dispositivos de NSX Manager y a todos los hosts del entorno de Cross-vCenter NSX.

Prerequisitos

- Compruebe que un firewall no bloquee el puerto que desea utilizar para VXLAN.
- Compruebe que la preparación del host no se esté ejecutando a la vez que cambia el puerto de VXLAN.

Procedimiento

1 Inicie sesión en vSphere Web Client.

2 Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).

3 Haga clic en la pestaña **Preparación de red lógica** (Logical Network Preparation) y, a continuación, haga clic en **Transporte de VXLAN** (VXLAN Transport).

4 Haga clic en el botón **Cambiar** (Change) en el panel del puerto de VXLAN. Introduzca el puerto al que desee cambiar. El puerto 4789 es el que asigna la IANA para VXLAN.

El cambio de puerto tardará un breve periodo de tiempo en propagarse a todos los hosts.

5 (Opcional) Compruebe el progreso del cambio de puerto con la solicitud API de `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus`.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>PHASE_TWO</taskPhase>
    <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>FINISHED</taskPhase>
    <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

Qué hacer a continuación

"Actualizar NSX Edge," página 76

Actualizar NSX Edge

NSX Edge puede actualizarse independientemente de las actualizaciones del clúster de NSX Controller o del clúster del host. Puede actualizar NSX Edge aunque aún no haya actualizado el clúster de NSX Controller ni los clústeres del host.

Durante el proceso de actualización, se implementa un nuevo dispositivo virtual Edge junto con el existente. Cuando el nuevo dispositivo Edge está listo, las vNIC del dispositivo Edge anterior se desconectan y se conectan las del nuevo Edge. A continuación, el nuevo Edge envía paquetes gratuitos de ARP (GARP) para actualizar la caché de ARP de los conmutadores conectados. Cuando se implementa HA, el proceso de actualización se realiza dos veces.

Este proceso puede afectar de forma temporal el reenvío de paquetes. Para minimizar el impacto, configure el dispositivo Edge para que funcione en modo ECMP.

Las adyacencias de OSPF se retiran durante la actualización si el reinicio estable no está habilitado.

Prerequisitos

- Compruebe que NSX Manager está actualizado a la versión 6.2.x.
- Compruebe que cuenta con un grupo de identificadores de segmento local aunque no tenga previsto crear conmutadores lógicos de NSX.
- Compruebe que los hosts tienen recursos suficientes para implementar dispositivos de puerta de enlace de servicios NSX Edge durante la actualización, sobre todo si está actualizando varios dispositivos NSX Edge en paralelo. Consulte "Requisitos del sistema para NSX," página 6 para los recursos que sean necesarios según el tamaño de NSX Edge.
  - Para una instancia sencilla de NSX Edge son necesarios dos dispositivos NSX Edge del tamaño adecuado que se mantengan encendidos durante la actualización.

- A partir de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, se implementarán los dos dispositivos de sustitución antes de reemplazar los dispositivos anteriores. Esto significa que habrá cuatro dispositivos NSX Edge de tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualice de nuevo, cualquiera de los dispositivos con HA podrá activarse.
- Antes de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, solo se implementaba un dispositivo de sustitución a la vez cuando se sustituían los dispositivos antiguos. Esto significa que habrá tres dispositivos NSX Edge del tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualiza, el dispositivo NSX Edge con HA con índice 0 se suele activar.

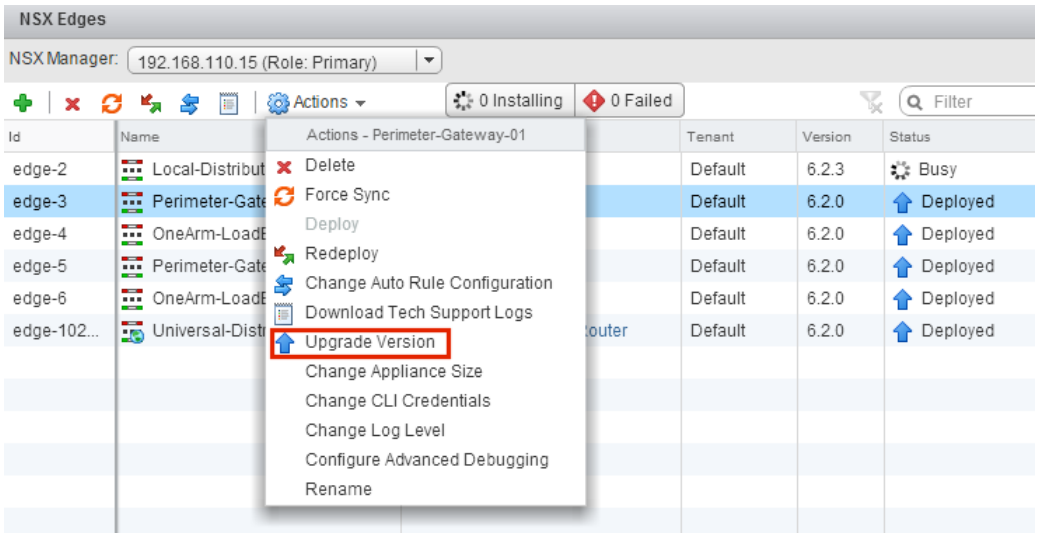
- Tenga en cuenta el impacto operativo que produce la actualización de NSX Edge cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.
- Si tiene habilitada la VPN de Capa 2 en NSX Edge, debe eliminar su configuración antes de iniciar la actualización. Después de la actualización, puede volver a configurar la VPN de Capa 2.
- Si está actualizando de NSX 6.2.x a NSX 6.2.3 y tiene el equilibrador de carga configurado, revise el siguiente artículo de la base de conocimientos para evitar problemas con la actualización: https://kb.vmware.com/kb/2145887.

Procedimiento

1 En vSphere Web Client, seleccione **Redes y seguridad (Networking & Security) > NSX Edge**.

2 Haga doble clic en cada instancia de NSX Edge y, a continuación, haga clic en **Administrar > VPN > VPN de Capa 2** (Manage > VPN > L2 VPN) y compruebe si la VPN de Capa 2 está habilitada. Si es así, elimine la configuración de la VPN de Capa 2 después de apuntar los detalles de dicha configuración.

3 Para cada instancia de NSX Edge, seleccione la opción **Versión de actualización** (Upgrade Version) en el menú **Acciones** (Actions).



Si en la actualización aparece el mensaje de error "No se pudo implementar el dispositivo Edge" (Failed to deploy edge appliance), asegúrese de que el host donde se implementa el dispositivo NSX Edge esté conectado y no esté en modo de mantenimiento.

Una vez que NSX Edge se actualiza correctamente, el **Estado** (Status) se implementa (Deployed) y la columna **Versión** (Version) muestra la nueva versión de NSX.

Si un dispositivo Edge no se puede actualizar y tampoco hay una reversión a la versión anterior, haga clic en el icono **Volver a implementar NSX Edge** (Redeploy NSX Edge) e intente actualizar nuevamente.

Qué hacer a continuación

Vuelva a configurar la VPN de Capa 2. Consulte la Descripción general de la VPN de Capa 2 en la *Guía de instalación de NSX*.

Actualizar Guest Introspection

Es importante que actualice Guest Introspection para que coincida con la versión de NSX Manager.

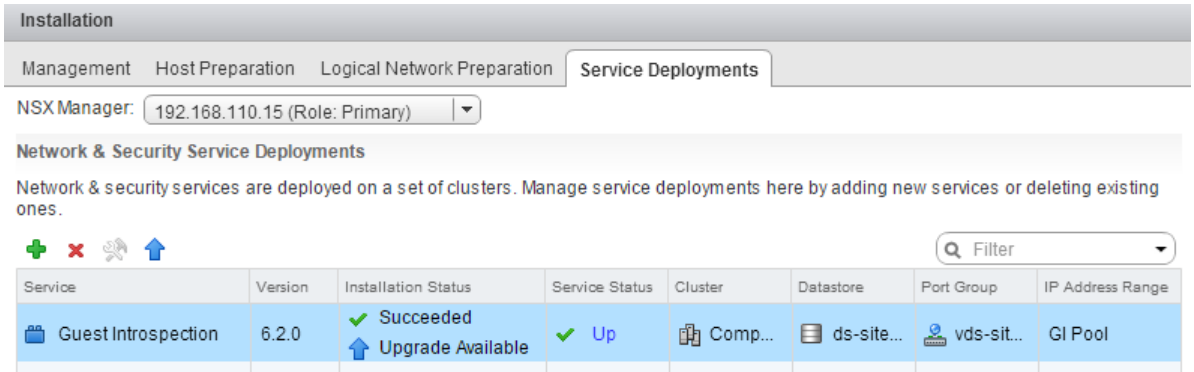
NOTA: Las máquinas virtuales de servicio de Guest Introspection se pueden actualizar desde vSphere Web Client. No es necesario eliminar la máquina virtual de servicio después de la actualización de NSX Manager para que se actualice. Si elimina la máquina virtual de servicio, el estado del servicio (Service Status) aparecerá como `Error` (Failed) ya que falta la máquina virtual agente. Haga clic en **Resolver** (Resolve) para implementar una nueva máquina virtual de servicio y, a continuación, haga clic en **Actualización disponible** (Upgrade Available) para implementar la máquina virtual de servicio de Guest Introspection más reciente.

Prerequisitos

NSX Manager, las controladoras, los clústeres del host preparados y NSX Edge deben estar actualizados a la versión 6.2.x.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

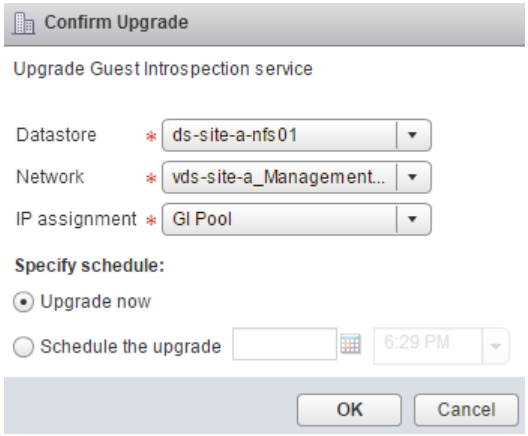


La columna **Estado de instalación** (Installation Status) indica **Actualización disponible** (Upgrade Available).

2 Seleccione la implementación de Guest Introspection que desea actualizar.

Se habilita el icono **Actualizar** (↑) (Upgrade) en la barra de herramientas ubicada encima de la tabla de servicios.

3 Haga clic en el icono **Actualizar** (⬆) (Upgrade) y siga las indicaciones de la interfaz de usuario.



Tras la actualización de Guest Introspection, el estado de la instalación es `Correcto` (Succeeded) y el estado del servicio aparece como `Listo` (Up). Las máquinas de servicio virtual de Guest Introspection están visibles en el inventario de vCenter Server.

Después de actualizar Guest Introspection en un clúster concreto, puede actualizar las soluciones de los partners. Si las soluciones de los partners están habilitadas, consulte la documentación sobre la actualización que ellos mismos proporcionan. Aunque no se actualice la solución del partner, se mantiene la protección.

Servicios NSX Services que no admiten actualización directa

Algunas instancias de NSX Services como por ejemplo, los dispositivos virtuales de seguridad de VMware Partner, no admiten actualizaciones directas. En estos casos, debe desinstalar los servicios y volver a instalarlos.

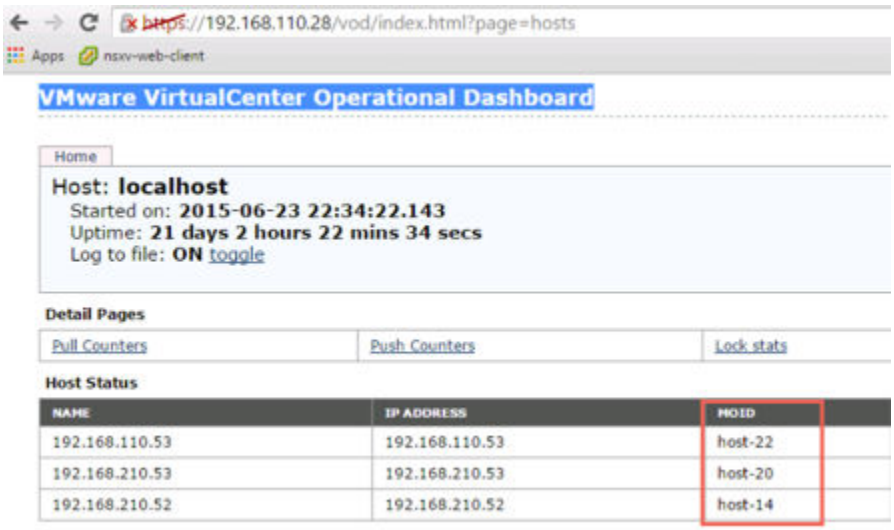
NSX Data Security

Lo ideal es desinstalar NSX Data Security antes de actualizar NSX, para volver a instalarlo después de completar la actualización de NSX. Si actualizó NSX sin desinstalar primero NSX Data Security, debe desinstalarlo con una llamada API de REST.

Emita la siguiente llamada API:

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

El identificador del host es el MOID del host ESXi. Para recuperar el MOID, abra el panel operativo de VMware VirtualCenter: https://<vcenter-ip>/vod/index.html?page=hosts.



Para el host ESXi con el MOID "host-22" en vCenter Server 192.168.110.28, la llamada API debería tener el siguiente formato:

```
DELETE https://192.168.110.28/api/1.0/vshield/host-22/vsds
```

Asegúrese de emitir la llamada API en todos los hosts ESXi.

Después de desinstalar Data Security, puede instalar la versión nueva. Consulte "Instalar NSX Data Security," página 37.

VPN SSL de NSX

A partir de NSX 6.2, la puerta de enlace de la VPN SSL solo acepta el protocolo TLS. A partir de NSX 6.2.3, el protocolo TLS 1.0 está obsoleto. Los dispositivos virtuales de seguridad de VMware Partner no admiten actualizaciones directas. Sin embargo, después de actualizar a NSX 6.2.x, todos los clientes nuevos de NSX 6.2.x creados utilizan automáticamente el protocolo TLS al establecer la conexión.

Cuando un cliente de NSX 6.0.x intenta conectarse con una puerta de enlace de NSX 6.2.x, se produce un error en el paso del enlace SSL al establecer la conexión. Este error se debe al cambio de protocolo.

Después de la actualización a NSX 6.2.x, desinstale los clientes de VPN SSL anteriores e instale la versión 6.2.x de NSX de los clientes de VPN SSL. Consulte "Instalar cliente SSL en un sitio remoto" en la *Guía de administración de NSX*.

VPN de Capa 2 de NSX

La configuración de una VPN de Capa 2 en una instancia de NSX Edge se debe eliminar para poder actualizar NSX Edge a NSX 6.2.x.

Instalar NSX Data Security

NOTA: Desde la versión 6.2.3 de NSX, la función de seguridad de datos de NSX pasó a estar obsoleta. En la versión 6.2.3 de NSX puede seguir utilizando esta función como desee, pero tenga en cuenta que se eliminará de NSX en versiones futuras.

Prerequisitos

NSX Guest Introspection debe instalarse en el clúster donde se va a instalar Data Security.

Si desea asignar una dirección IP a la máquina virtual del servicio Data Security desde un grupo de direcciones IP, cree el grupo de direcciones IP antes de instalar Data Security. Consulte Agrupar objetos en la *Guía de administración de NSX*.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

2 Haga clic en el icono **Nueva implementación de servicios** (New Service Deployment) ( ).

3 En el cuadro de diálogo Implementar servicios de red y seguridad (Deploy Network and Security Services), seleccione **Data Security** y haga clic en **Siguiente** (Next).

4 En **Especificar programación** (Specify schedule), en la parte inferior del cuadro de diálogo, seleccione **Implementar ahora** (Deploy now) para implementar Data Security apenas se instale, o bien seleccione una fecha y una hora de implementación.

5 Haga clic en **Siguiente** (Next).

6 Seleccione el centro de datos y los clústeres donde desea instalar Data Security y, a continuación, haga clic en **Siguiente** (Next).

7 En la página Seleccionar red de almacenamiento y administración (Select storage and Management Network), seleccione el almacén de datos en el que desea agregar las máquinas virtuales de servicio, o bien seleccione **Especificado en el host** (Specified on host).

   El almacén de datos seleccionado debe estar disponible en todos los hosts del clúster elegido.

   Si seleccionó **Especificado en el host** (Specified on host), el almacén de datos del host ESX debe especificarse en la opción **Configuración de máquinas virtuales de agente** (AgentVM Settings) del host antes de agregarse al clúster. Consulte la *documentación de vSphere API/SDK*.

8 Seleccione el grupo de puertos virtuales distribuidos donde se alojará la interfaz de administración. Este grupo de puertos debe poder comunicarse con el grupo de puertos de NSX Manager.

   Si el almacén de datos se configura como **Especificado en el host** (Specified on host), la red que se utilizará debe especificarse en la propiedad **agentVmNetwork** de cada host en el clúster. Consulte la *documentación de vSphere API/SDK*.

   Cuando agrega hosts al clúster, la propiedad **agentVmNetwork** del host debe configurarse antes de agregarse al clúster.

   El grupo de puertos seleccionado debe estar disponible en todos los hosts del clúster seleccionado.

9 En la asignación de direcciones IP, seleccione una de las siguientes opciones:

Seleccionar	Para
DHCP	Asigne una dirección IP a las máquinas virtuales del servicio Data Security a través del protocolo de configuración dinámica de host (DHCP).
Grupo de direcciones IP	Asigne una dirección IP a las máquinas virtuales del servicio Data Security desde el grupo de direcciones IP seleccionado.

   Tenga en cuenta que no se admiten direcciones IP estáticas.

10 Haga clic en **Siguiente** (Next) y, a continuación, en **Finalizar** (Finish) en la página Listo para finalizar (Ready to complete).

11 Supervise la implementación hasta que la columna **Estado de instalación** (Installation Status) muestre **Correcto** (Succeeded).

12 Si la columna **Estado de instalación** (Installation Status) muestra **Con errores** (Failed), haga clic en el icono junto a Con errores. Se muestran todos los errores de implementación. Haga clic en **Resolver** (Resolve) para solucionar los errores. En algunos casos, al resolver los errores aparecen otros nuevos. Realice la acción necesaria y vuelva a hacer clic en **Resolver** (Resolve).

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

1 Elimine la snapshot de NSX Manager tomada durante la instalación.

2 Realice una copia de seguridad actualizada tras la actualización.

3 Asegúrese de que los VIB estén instalados en los hosts.

NSX Instala los siguientes VIB:

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Si se ha instalado Guest Introspection, compruebe también que este VIB se encuentra en los hosts:

```
esxcli software vib get --vibname epsec-mux
```

4 Vuelva a sincronizar el bus de mensajería del host. VMware aconseja a todos sus clientes que vuelvan a realizar una sincronización tras la actualización.

Puede usar la siguiente llamada API para volver a realizar la sincronización en cada host.

```
URL : 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
```

Actualizar a NSX 6.2.x con Cross-vCenter NSX

Para actualizar a NSX 6.2.x en un entorno de Cross-vCenter NSX, debe actualizar los componentes de NSX en el orden documentado en esta guía.

Los componentes de NSX deben actualizarse en el siguiente orden:

1 Dispositivo NSX Manager principal

2 Todos los dispositivos NSX Manager secundarios

3 Clúster de NSX Controller

4 Clústeres de hosts

5 NSX Edge

6 Guest Introspection

La administración del proceso de actualización está a cargo de NSX Manager. Si ocurre un error en la actualización de un componente o si se interrumpe y es necesario repetirla o reiniciarla, el proceso empieza por el punto donde se detuvo y no desde el principio.

El estado de la actualización se actualiza en cada nodo y en el nivel del clúster.

Actualizar NSX Manager principal en Cross-vCenter NSX

El primer paso en el proceso de actualización de la infraestructura NSX es actualizar el dispositivo NSX Manager principal.

Durante la actualización, es posible unirse al Programa de mejora de la experiencia de cliente (CEIP) de NSX. Consulte el Programa de mejora de la experiencia de cliente en *Guía de administración de NSX* para obtener más información acerca del programa, incluyendo cómo unirse o salir de él.

ADVERTENCIA: No se puede ejecutar dispositivos NSX Manager de diferentes versiones en un entorno de Cross-vCenter NSX. Una vez que haya actualizado el dispositivo NSX Manager principal, debe actualizar los dispositivos NSX Manager secundarios.

Prerequisitos

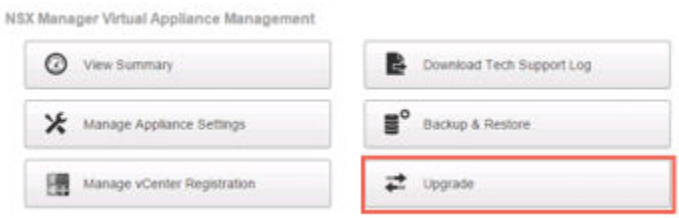
- Compruebe el uso del sistema de archivos de NSX Manager y realice una limpieza si el uso de dicho sistema está al 100 por cien.
  a Inicie sesión en NSX Manager y habilite `show filesystems` para mostrar el uso del sistema de archivos /dev/sda2.
  b Si el uso está al 100 por cien, ejecute los comandos `purge log manager` y `purge log system`.
  c Reinicia el dispositivo NSX Manager para poder realizar la limpieza del registro.
- Antes de actualizar a NSX 6.2.x, aumente la memoria reservada del dispositivo virtual NSX Manager como mínimo, a 16 GB.

  Consulte "Requisitos del sistema para NSX," página 6.
- Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte "Desinstalar NSX Data Security," página 62.
- Haga una copia de seguridad de la configuración actual y descargue los registros de soporte técnico antes de actualizar. Consulte "Copia de seguridad y restauración de NSX," página 62.
- Descargue el paquete de actualización y compruebe MD5. Consulte "Descargar el paquete de actualización de NSX y comprobar MD5," página 66.
- Asegúrese de entender el impacto operativo que produce la actualización de NSX Manager cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.

Procedimiento

1 Inicie sesión en el dispositivo virtual NSX Manager.

2 En la página de inicio de NSX Manager, haga clic en **Actualizar** (Upgrade).



3 Haga clic en **Actualizar** (Upgrade) y, a continuación, en Seleccionar archivo`VMware-NSX-Manager-upgrade-bundle-` (Choose File) y desplácese hasta el archivo *releaseNumber-NSXbuildNumber*`.tar.gz`. Haga clic en **Continuar** (Continuar) para iniciar la migración.

   El estado de la carga se muestra en la ventana del explorador.

4 En el cuadro de diálogo, especifique si desea habilitar SSH y si desea participar en el Programa de mejora de la experiencia de cliente (CEIP) de VMware. Haga clic en **Actualizar** (Upgrade) para iniciar la actualización.

   El estado de la actualización se muestra en la ventana del explorador.

   Espere a que el procedimiento de actualización se complete y aparezca la página de inicio de sesión en NSX Manager.

5 Inicie sesión nuevamente en el dispositivo virtual NSX Manager y confirme que el estado de actualización sea **Finalizado** (Complete) y que los números de versión y compilación en la parte superior derecha coincidan con el paquete de actualización recientemente instalado.

Si inició sesión en vSphere Web Client durante la actualización, verá las advertencias de problemas con la sincronización en la página **Networking and Security > Instalación > Administración** (Networking and Security > Installation > Management). Esto ocurre porque tiene dispositivos NSX Manager con distintas versiones de NSX. Debe actualizar los dispositivos NSX Manager secundarios antes de seguir con otra parte de la actualización.

Después de actualizar NSX Manager y de conectarlo a una instancia de vCenter Server existente, restablezca el servidor Web Client para permitir que también se actualicen los complementos de NSX.

- También puede hacer esto en vCenter 5.5. Para ello, abra https://<vcenter-ip>:5480 y reinicie el servidor Web Client.
- Para hacerlo en vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como raíz y ejecute los comandos siguientes.

  ```
  Command> shell.set --enabled True
  Command> shell
  localhost:~ # cd /bin
  localhost:~ # service-control --stop vsphere-client
  localhost:~ # service-control --start vsphere-client
  ```

- En vCenter Server 6.0, puede ejecutar los siguientes comandos en Windows.

  ```
  cd C:\Program Files\VMware\vCenter Server\bin
  service-control --stop vspherewebclientsvc
  service-control --start vspherewebclientsvc
  ```

Se requiere reiniciar para evitar errores inesperados, como grupos de seguridad configurados que no aparecen en la pestaña **Grupos de seguridad** (Security Groups) de Service Composer.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su navegador.

Se recomienda utilizar diferentes servidores Web Client para administrar los servidores vCenter Server que ejecutan distintas versiones de NSX Manager a fin de evitar errores inesperados cuando diferentes versiones de complementos de NSX están en ejecución.

Una vez actualizado NSX Manager, cree un nuevo archivo de copia de seguridad de NSX Manager. Consulte "Copia de seguridad y restauración de NSX," página 62. La copia de seguridad anterior de NSX Manager solo es válida para la versión anterior.

Qué hacer a continuación

Actualice todos los dispositivos NSX Manager secundarios.

Actualizar todos los dispositivos NSX Manager secundarios en Cross-vCenter NSX

Debe actualizar todos los dispositivos NSX Manager secundarios antes de actualizar cualquier componente de NSX.

Complete los siguientes pasos para actualizar un dispositivo NSX Manager secundario. Repita estos pasos con todos los dispositivos NSX Manager secundarios en el entorno de Cross-vCenter NSX.

Durante la actualización, es posible unirse al Programa de mejora de la experiencia de cliente (CEIP) de NSX. Consulte el Programa de mejora de la experiencia de cliente en *Guía de administración de NSX* para obtener más información acerca del programa, incluyendo cómo unirse o salir de él.

Prerequisitos

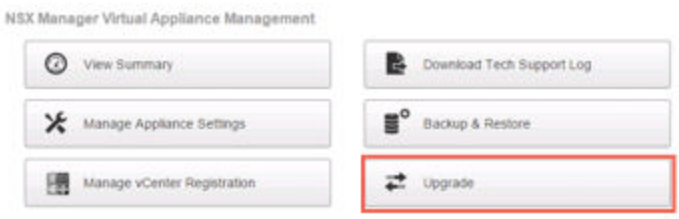
- Compruebe que la instancia de NSX Manager principal está actualizada.
- Compruebe el uso del sistema de archivos de NSX Manager y realice una limpieza si el uso de dicho sistema está al 100 por cien.
  a Inicie sesión en NSX Manager y habilite `show filesystems` para mostrar el uso del sistema de archivos /dev/sda2.
  b Si el uso está al 100 por cien, ejecute los comandos `purge log manager` y `purge log system`.
  c Reinicia el dispositivo NSX Manager para poder realizar la limpieza del registro.
- Antes de actualizar a NSX 6.2.x, aumente la memoria reservada del dispositivo virtual NSX Manager como mínimo, a 16 GB.

  Consulte "Requisitos del sistema para NSX," página 6.
- Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte "Desinstalar NSX Data Security," página 62.
- Haga una copia de seguridad de la configuración actual y descargue los registros de soporte técnico antes de actualizar. Consulte "Copia de seguridad y restauración de NSX," página 62.
- Descargue el paquete de actualización y compruebe MD5. Consulte "Descargar el paquete de actualización de NSX y comprobar MD5," página 66.
- Asegúrese de entender el impacto operativo que produce la actualización de NSX Manager cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.

Procedimiento

1 Inicie sesión en el dispositivo virtual NSX Manager.

2 En la página de inicio de NSX Manager, haga clic en **Actualizar** (Upgrade).



3 Haga clic en **Actualizar** (Upgrade) y, a continuación, en Seleccionar archivo`VMware-NSX-Manager-upgrade-bundle-` (Choose File) y desplácese hasta el archivo *releaseNumber-NSXbuildNumber*`.tar.gz`. Haga clic en **Continuar** (Continuar) para iniciar la migración.

El estado de la carga se muestra en la ventana del explorador.

4 En el cuadro de diálogo, especifique si desea habilitar SSH y si desea participar en el Programa de mejora de la experiencia de cliente (CEIP) de VMware. Haga clic en **Actualizar** (Upgrade) para iniciar la actualización.

   El estado de la actualización se muestra en la ventana del explorador.

   Espere a que el procedimiento de actualización se complete y aparezca la página de inicio de sesión en NSX Manager.

5 Inicie sesión nuevamente en el dispositivo virtual NSX Manager y confirme que el estado de actualización sea **Finalizado** (Complete) y que los números de versión y compilación en la parte superior derecha coincidan con el paquete de actualización recientemente instalado.

Después de actualizar NSX Manager y de conectarlo a una instancia de vCenter Server existente, restablezca el servidor Web Client para permitir que también se actualicen los complementos de NSX.

- También puede hacer esto en vCenter 5.5. Para ello, abra https://<vcenter-ip>:5480 y reinicie el servidor Web Client.
- Para hacerlo en vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como raíz y ejecute los comandos siguientes.

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- En vCenter Server 6.0, puede ejecutar los siguientes comandos en Windows.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Se requiere reiniciar para evitar errores inesperados, como grupos de seguridad configurados que no aparecen en la pestaña **Grupos de seguridad** (Security Groups) de Service Composer.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su navegador.

Se recomienda utilizar diferentes servidores Web Client para administrar los servidores vCenter Server que ejecutan distintas versiones de NSX Manager a fin de evitar errores inesperados cuando diferentes versiones de complementos de NSX están en ejecución.

Una vez actualizado NSX Manager, cree un nuevo archivo de copia de seguridad de NSX Manager. Consulte "Copia de seguridad y restauración de NSX," página 62. La copia de seguridad anterior de NSX Manager solo es válida para la versión anterior.

Qué hacer a continuación

"Actualizar el clúster de NSX Controller en Cross-vCenter NSX," página 86

Actualizar el clúster de NSX Controller en Cross-vCenter NSX

Las controladoras del entorno se actualizan en el nivel del clúster. Si existe una actualización disponible para el clúster de NSX Controller, aparecerá un vínculo de actualización junto la instancia de NSX Manager principal en el panel **Redes y seguridad > Instalación > Administración** (Networking & Security > Installation > Management).

Se recomienda actualizar las controladoras durante un período de mantenimiento.

La actualización de NSX Controller produce la descarga de un archivo de actualización en cada nodo de controladora. Las controladoras se actualizan de a una por vez. Mientras una actualización está en curso, no es posible seleccionar el vínculo **Actualización disponible** (Upgrade Available), y las llamadas API para actualizar el clúster de la controladora se bloquean hasta que finaliza la actualización.

Si se implementan controladoras nuevas antes de que se actualicen las existentes, se implementan en la versión anterior. Los nodos de controladora deben ser de la misma versión para poder unirse a un clúster.

Prerequisitos

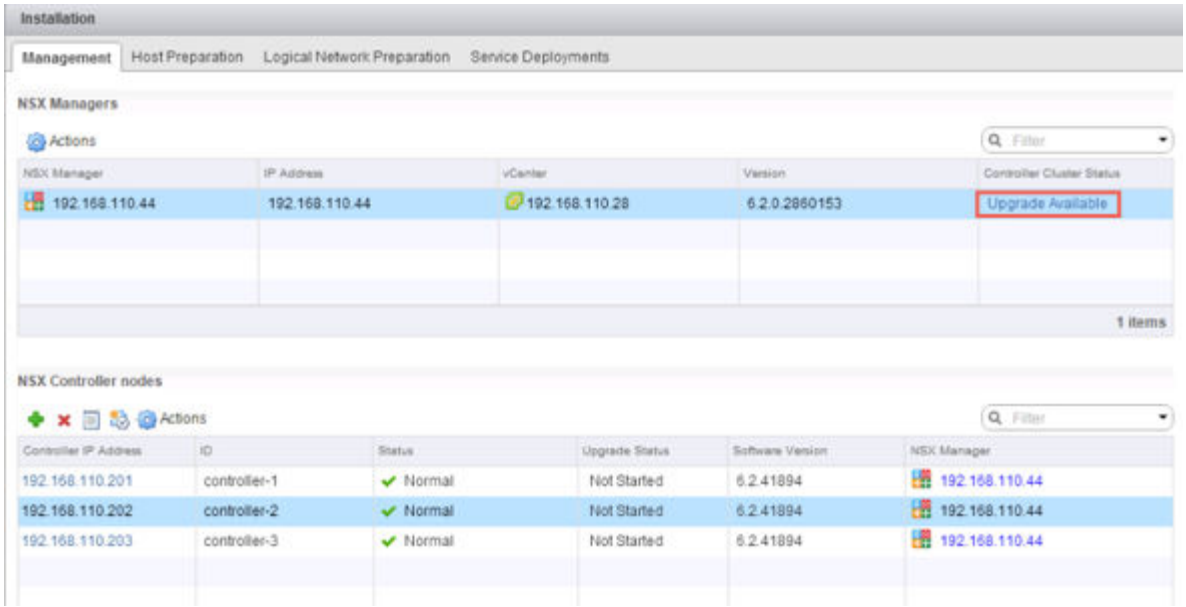
- Asegúrese de que todas las controladoras estén en estado normal. La actualización no es posible si una o varias controladoras están en estado desconectado. Para reconectar una controladora desconectada, intente restablecer el dispositivo virtual de la controladora. En la vista **Hosts y clústeres** (Hosts and Clusters), haga clic con el botón derecho en la controladora y seleccione **Alimentación > Restablecer** (Power > Reset).
- Un clúster de NSX Controller válido contiene tres nodos de controladora. Inicie sesión en los tres nodos de controladora y ejecute el comando **show controller-cluster status**.

```
controller-node# show control-cluster status

Type                Status                                           Since
--------------------------------------------------------------------------------
Join status:        Join complete                                    05/04 02:36:03
Majority status:    Connected to cluster majority                    05/19 23:57:23
Restart status:     This controller can be safely restarted          05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  - En el estado Unirse (Join), compruebe que el nodo de controladora informe sobre el estado Unión completa (Join Complete).
  - En el estado Mayoría (Majority), compruebe que la controladora esté conectada a la mayoría del clúster.
  - En el identificador del clúster, todos los nodos de controladora de un clúster deben tener el mismo identificador de clúster.
  - En los estados Configurado (Configured) y Activo (Active), compruebe que todas las funciones de la controladora están habilitadas y activadas.
- Asegúrese de entender el impacto operativo que produce la actualización de NSX Controller cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.

Procedimiento

- En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation), seleccione la pestaña **Administración** (Management) y haga clic en **Actualización disponible** (Upgrade Available) en la columna **Estado de clúster de controladora** (Controller Cluster Status).



  Las controladoras del entorno se actualizan y se reinician de a una por vez. Después de iniciar la actualización, el sistema descarga el archivo de actualización, actualiza y reinicia cada controladora, y actualiza el estado de actualización de cada controladora. Los siguientes campos muestran el estado de la controladora:

  - La columna **Estado de clúster de controladora** (Controller Cluster Status) de la sección NSX Manager muestra el estado de actualización del clúster. Cuando la actualización se inicia, el estado muestra el mensaje **Descargando archivo de actualización** (Downloading upgrade file). Una vez que se descargó el archivo de actualización en todas las controladoras del clúster, el estado cambia a **En curso** (In progress). Una vez actualizadas todas las controladoras del clúster, el estado que aparece es **Finalizado** (Complete) y la columna ya no se muestra.
  - La columna **Estado** (Status) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de cada controladora, que empieza siendo **Normal**. Cuando los servicios de la controladora se apagan y se reinicia la controladora, el estado cambia a **Desconectada** (Disconnected). Una vez completada la actualización de la controladora, el estado vuelve a ser **Normal**.
  - La columna **Estado de actualización** (Upgrade Status) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de actualización de cada controladora. El primer estado que se muestra es **Descargando archivo de actualización** (Downloading upgrade file), después aparece **Actualización en curso** (Upgrade in progress) y, por último, **Reiniciando** (Rebooting). Cuando la controladora está actualizada, el estado indica **Actualizada** (Upgraded).

Una vez completada la actualización, la columna **Versión de software** (Software Version) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el número **6.2.***buildNumber* para cada controladora. Vuelva a ejecutar el comando **show controller-cluster status** para garantizar que las controladoras puedan crear una mayoría. Si no se vuelve a formar la mayoría del clúster de NSX Controller, revise los registros de la controladora y de NSX Manager.

Después de actualizar las controladoras, es posible que se le asigne un nuevo ID de controladora a alguna de ellas. Este comportamiento es correcto y depende de si la instancia de NSX Manager secundario hace un sondeo en los nodos.

El tiempo promedio para cada actualización es de 6 a 8 minutos. Si la actualización no se completa dentro del período de espera (30 minutos), la columna **Estado de actualización** (Upgrade Status) muestra **Con errores** (Failed). Haga clic nuevamente en **Actualización disponible** (Upgrade Available) en la sección NSX Manager para reanudar el proceso desde el punto donde se detuvo.

Si los problemas de red impiden que la actualización se realice correctamente dentro del período de espera de 30 minutos, debe configurar un tiempo de espera más largo. Para diagnosticar y solucionar cualquier problema subyacente, puede trabajar con el equipo de soporte técnico de VMware y, si fuera necesario, configurar un período de espera más largo.

Si la actualización de la controladora tiene errores, revise la conectividad entre las controladoras y NSX Manager.

Hay casos en los que la primera controladora se actualiza correctamente y la segunda no lo hace. Supongamos que el clúster tiene tres controladoras: la primera se actualizó correctamente a la nueva versión y la segunda se está actualizando. Si la actualización de la segunda controladora tiene errores, esta controladora podría quedar en estado desconectado. Al mismo tiempo, la primera controladora y la tercera ahora tienen dos versiones diferentes (una actualizada y la otra, no), por lo cual no pueden formar una mayoría. En este punto, la actualización no puede reiniciarse. Para solucionar este problema, cree otra controladora. La nueva controladora tendrá la versión anterior (coincidente con la tercera controladora) y, por lo tanto, formará una mayoría con la tercera controladora. En este punto, se puede reiniciar el procedimiento de actualización.

Póngase en contacto con el equipo de soporte técnico de VMware para poder restaurar la instantánea de la controladora. La instantánea corresponde únicamente a los datos de la controladora de la misma versión. Las instantáneas no pueden restaurarse a una versión más reciente. En otras palabras: no intente aplicar una instantánea a una controladora correctamente actualizada.

Qué hacer a continuación

"Actualizar los clúster del host en Cross-vCenter NSX," página 89.

Actualizar los clúster del host en Cross-vCenter NSX

Una vez actualizados todos los dispositivos NSX Manager y el clúster de NSX Controller a NSX 6.2.x, debe actualizar todos los clústeres de los hosts en el entorno de Cross-vCenter NSX. Durante este proceso, se actualiza el software de cada host del clúster y, a continuación, el host se reinicia.

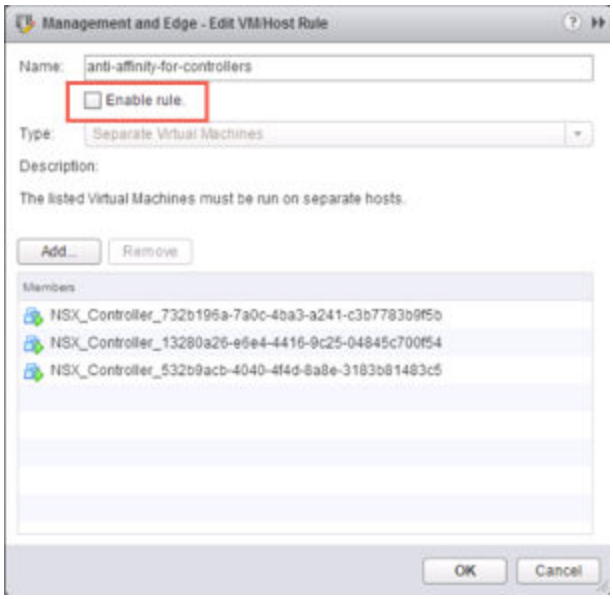
IMPORTANTE: Cuando se actualizan hosts ESXi con estado junto con NSX, hay un orden de actualización que debe respetarse:

1. Actualice NSX Manager.
2. Actualice el clúster de NSX Controller.
3. Coloque manualmente los hosts ESXi en modo de mantenimiento.
4. Actualice los VIB de NSX (este procedimiento).
5. Reinicie los hosts (para obtener los VIB 5.5).
6. Actualice los hosts ESXi a la versión 6.0.
7. Vuelva a iniciar los hosts ESXi (para obtener los VIB 6.0).
8. Extraiga manualmente los hosts ESXi del modo de mantenimiento.

Conserve los hosts en el modo de mantenimiento durante este proceso. No permita que salgan del modo de mantenimiento antes de tiempo.

Prerequisitos

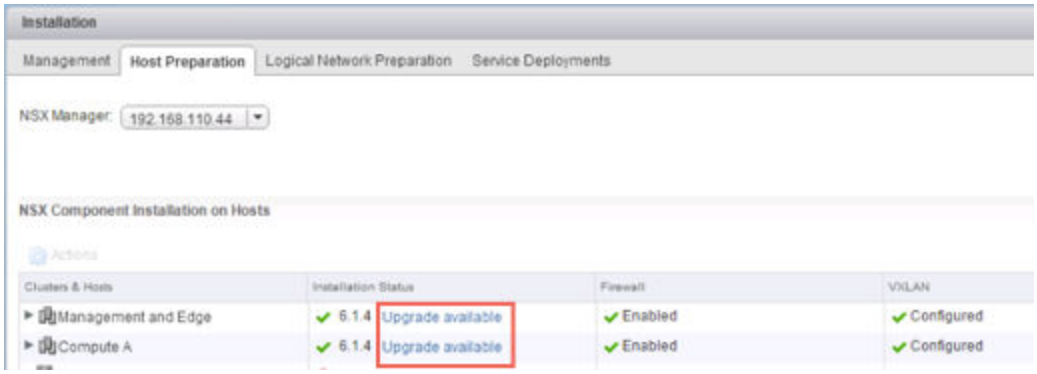
- Asegúrese de que puedan resolverse los nombres de dominio completos (FQDN) de todos los hosts.
- Inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list`. Observe la versión actual de los siguientes VIB:
  - esx-vsip
  - esx-vxlan
  - esx-dvfilter-switch-security: si actualiza a una versión de NSX posterior a la versión 6.2.
- Actualice NSX Manager y el clúster de NSX Controller.
- Asegúrese de entender el impacto operativo que produce la actualización de un clúster de hosts cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.
- Si DRS está deshabilitado, apague o transfiera por vMotion las máquinas virtuales manualmente antes de empezar la actualización.
- Si DRS está habilitado, las máquinas virtuales en ejecución se moverán automáticamente durante la actualización del clúster de hosts. Antes de iniciar la actualización, asegúrese de que DRS funcione en el entorno.
  - Asegúrese de que DRS esté habilitado en los clústeres del host.
  - Asegúrese de que vMotion funcione correctamente.
  - Compruebe el estado de la conexión del host con vCenter.
  - Compruebe si cuenta con tres hosts ESXi como mínimo en cada clúster de hosts. Durante una actualización de NSX, hay más probabilidades de que un clúster de hosts con solo uno o dos hosts presente problemas con el control de admisión de DRS. Para que la actualización de NSX funcione, VMware recomienda que cada clúster de hosts tenga al menos tres hosts. Si un clúster contiene menos de tres hosts, se recomienda evacuarlos manualmente.
  - En un clúster pequeño con solo dos o tres hosts, si se crearon reglas de antiafinidad por las cuales ciertas máquinas virtuales deben residir en hosts distintos, estas reglas pueden impedir que DRS mueva las máquinas virtuales durante la actualización. Agregue más hosts al clúster o deshabilite las reglas de antiafinidad durante la actualización y vuelva a habilitarlas una vez completada la actualización. Para deshabilitar una regla de antiafinidad, desactive **Habilitar regla** (Enable rule).



Procedimiento

1 En vSphere Web Client, desplácese hasta **Inicio > Redes y seguridad > Instalación** (Home > Networking & Security > Installation), y seleccione la pestaña **Preparación del host** (Host Preparation).

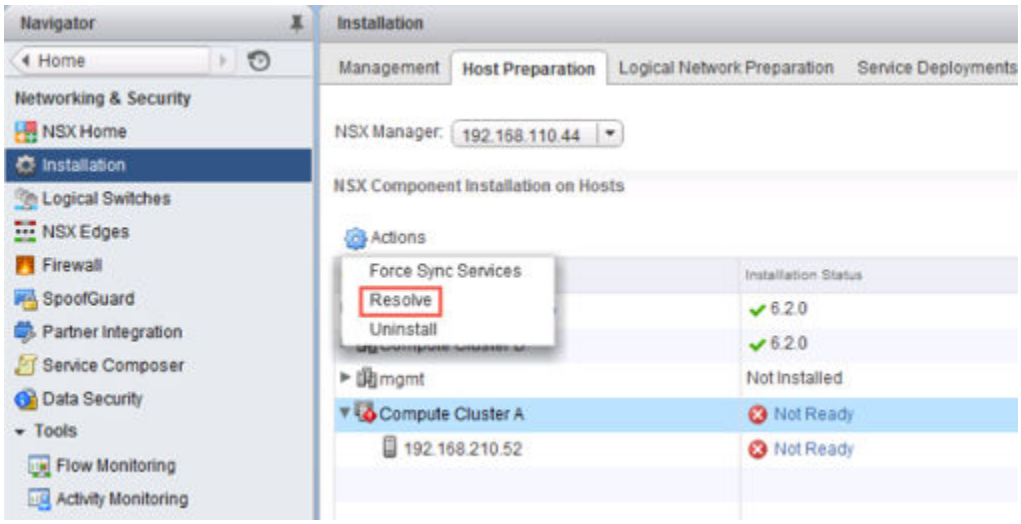
2 Para cada clúster que desea actualizar, haga clic en **Actualización disponible** (Upgrade available).



La actualización del host inicia un análisis del host. Los VIB anteriores se eliminan (aunque no desaparecen por completo hasta después del reinicio). Los nuevos VIB se instalan en la partición altboot. Para ver los nuevos VIB en un host que aún no se reinició, se puede ejecutar el comando `esxcli software vib list --rebooting-image | grep esx`.

Si el clúster tiene DRS habilitado, DRS intenta reiniciar los hosts de una forma controlada que permite que las máquinas virtuales continúen en ejecución. vMotion mueve las máquinas virtuales en ejecución a otros hosts del clúster y coloca al host en el modo de mantenimiento. Si se requiere colocar los hosts manualmente en el modo de mantenimiento (por ejemplo, debido a requisitos de HA o a reglas de DRS), el proceso de actualización se detiene y el clúster **Estado de instalación** (Installation Status) muestra la opción **No está listo** (Not Ready). Haga clic en ⚠ para mostrar los errores.

Después de evacuar manualmente los hosts, seleccione el clúster y haga clic en la acción **Resolver** (Resolve). La acción **Resolver** (Resolve) intenta completar la actualización y reinicia todos los hosts del clúster. Si se produce un error en el reinicio del host por alguna razón, la acción **Resolver** (Resolve) se detiene. Compruebe el estado de los hosts en la vista **Hosts y clústeres** (Hosts and Clusters) y asegúrese de que estén encendidos, conectados y que no contengan máquinas virtuales en ejecución. A continuación, vuelva a intentar ejecutar la acción **Resolver** (Resolve).



Cuando el clúster está actualizado, la columna **Estado de instalación** (Installation Status) muestra la versión de software a la que se actualizó.

Para confirmar la actualización del host, inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list | grep esx`. Asegúrese de que los siguientes VIB estén actualizados a la versión prevista.

- esx-vsip
- esx-vxlan

NOTA: En NSX 6.2 y versiones posteriores, el VIB esx-dvfilter-switch-security se incluye dentro del VIB esx-vxlan.

Si la actualización de un host tiene errores, soluciónelos con los siguientes pasos:

- Revise ESX Agent Manager en vCenter y busque alertas y errores.
- Inicie sesión en el host, compruebe el archivo de registro `/var/log/esxupdate.log` y, a continuación, busque errores y alertas recientes.
- Asegúrese de que DNS y NTP estén configurados en el host.

Cambiar el puerto de VXLAN en Cross-vCenter NSX

Es posible cambiar el puerto utilizado para el tráfico de VXLAN.

En NSX 6.2.3., el puerto VXLAN predeterminado es el 4789, el puerto estándar que asigna la IANA. Antes de NSX 6.2.3, el número de puerto UDP de VXLAN predeterminado era el 8472.

Las instalaciones nuevas de NSX utilizarán el puerto UDP 4789 para VXLAN.

Si en la actualización a NSX 6.2.3 y en la instalación se utilizó el puerto antiguo predeterminado (8472) o un número de puerto personalizado predeterminado (por ejemplo, el 8888) antes de la actualización, dicho puerto seguirá utilizándose tras la actualización a menos que realice los pasos necesarios para cambiarlo.

Si la instalación que actualizó utiliza o utilizará puertas de enlace de VTEP de hardware (puertas de enlace ToR), debe cambiar al puerto 4789 de VXLAN.

No es necesario que utilice el puerto 4789 para el puerto VXLAN en Cross-vCenter NSX; sin embargo, todos los hosts de un entorno de Cross-vCenter NSX deben estar configurados para usar el mismo puerto VXLAN. Si cambia al puerto 4789, garantiza que las nuevas instalaciones de NSX agregadas al entorno de Cross-vCenter NSX utilizan el mismo puerto que las implementaciones de NSX.

El cambio del puerto de VXLAN se realiza en un proceso de tres fases y no interrumpirá el tráfico de VXLAN. En un entorno de Cross-vCenter NSX, el cambio se propagará a todos los dispositivos de NSX Manager y a todos los hosts del entorno de Cross-vCenter NSX.

Prerequisitos

- Compruebe que un firewall no bloquee el puerto que desea utilizar para VXLAN.
- Compruebe que la preparación del host no se esté ejecutando a la vez que cambia el puerto de VXLAN.

Procedimiento

1. Inicie sesión en vSphere Web Client.
2. Haga clic en **Redes y seguridad** (Networking & Security) y seleccione **Instalación** (Installation).
3. Haga clic en la pestaña **Preparación de red lógica** (Logical Network Preparation) y, a continuación, haga clic en **Transporte de VXLAN** (VXLAN Transport).
4. Haga clic en el botón **Cambiar** (Change) en el panel del puerto de VXLAN. Introduzca el puerto al que desee cambiar. El puerto 4789 es el que asigna la IANA para VXLAN.

   El cambio de puerto tardará un breve periodo de tiempo en propagarse a todos los hosts.

5 (Opcional) Compruebe el progreso del cambio de puerto con la solicitud API de `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus`.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>PHASE_TWO</taskPhase>
    <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

```
...
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>FINISHED</taskPhase>
    <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

Qué hacer a continuación

"Actualizar NSX Edge en Cross-vCenter NSX," página 93

Actualizar NSX Edge en Cross-vCenter NSX

NSX Edge puede actualizarse independientemente de las actualizaciones del clúster de NSX Controller o del clúster del host. Puede actualizar NSX Edge aunque aún no haya actualizado el clúster de NSX Controller ni los clústeres del host. Actualizar todas las instancias de NSX Edge en todas las instalaciones de NSX en el entorno de cross-vCenter NSX.

Durante el proceso de actualización, se implementa un nuevo dispositivo virtual Edge junto con el existente. Cuando el nuevo dispositivo Edge está listo, las vNIC del dispositivo Edge anterior se desconectan y se conectan las del nuevo Edge. A continuación, el nuevo Edge envía paquetes gratuitos de ARP (GARP) para actualizar la caché de ARP de los conmutadores conectados. Cuando se implementa HA, el proceso de actualización se realiza dos veces.

Este proceso puede afectar de forma temporal el reenvío de paquetes. Para minimizar el impacto, configure el dispositivo Edge para que funcione en modo ECMP.

Las adyacencias de OSPF se retiran durante la actualización si el reinicio estable no está habilitado.

Prerequisitos

- Compruebe que NSX Manager está actualizado a la versión 6.2.x.
- Compruebe que cuenta con un grupo de identificadores de segmento local aunque no tenga previsto crear conmutadores lógicos de NSX.
- Compruebe que los hosts tienen recursos suficientes para implementar dispositivos de puerta de enlace de servicios NSX Edge durante la actualización, sobre todo si está actualizando varios dispositivos NSX Edge en paralelo. Consulte "Requisitos del sistema para NSX," página 6 para los recursos que sean necesarios según el tamaño de NSX Edge.
  - Para una instancia sencilla de NSX Edge son necesarios dos dispositivos NSX Edge del tamaño adecuado que se mantengan encendidos durante la actualización.

- A partir de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, se implementarán los dos dispositivos de sustitución antes de reemplazar los dispositivos anteriores. Esto significa que habrá cuatro dispositivos NSX Edge de tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualice de nuevo, cualquiera de los dispositivos con HA podrá activarse.
- Antes de la versión 6.2.3 de NSX, al actualizar una instancia de NSX Edge con High Availability, solo se implementaba un dispositivo de sustitución a la vez cuando se sustituían los dispositivos antiguos. Esto significa que habrá tres dispositivos NSX Edge del tamaño adecuado en el estado poweredOn durante la actualización de una instancia de NSX Edge determinada. Cuando la instancia de NSX Edge se actualiza, el dispositivo NSX Edge con HA con índice 0 se suele activar.

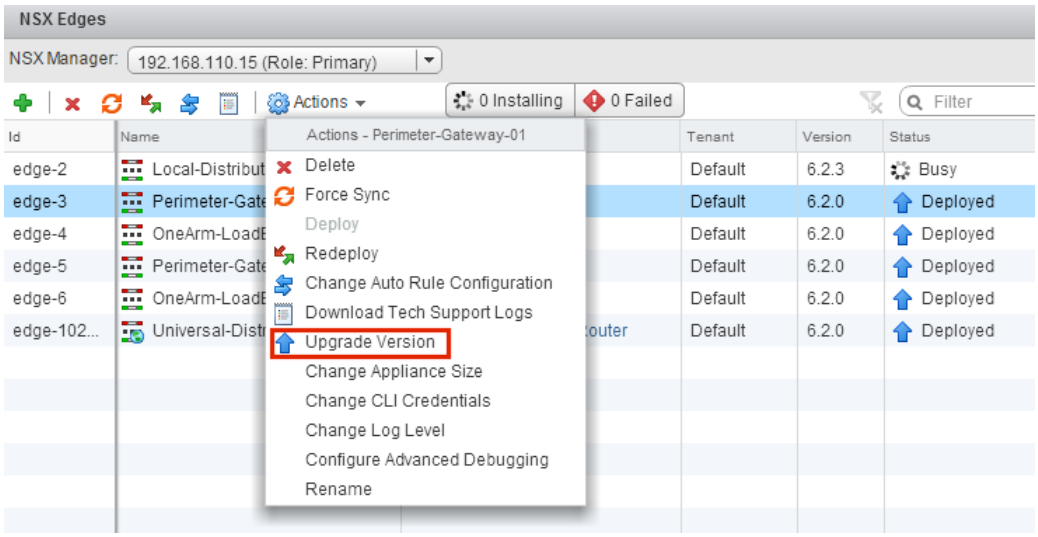
- Tenga en cuenta el impacto operativo que produce la actualización de NSX Edge cuando la actualización está en curso. Consulte "Impactos operativos de las actualizaciones de NSX," página 58.
- Si tiene habilitada la VPN de Capa 2 en NSX Edge, debe eliminar su configuración antes de iniciar la actualización. Después de la actualización, puede volver a configurar la VPN de Capa 2.
- Si está actualizando de NSX 6.2.x a NSX 6.2.3 y tiene el equilibrador de carga configurado, revise el siguiente artículo de la base de conocimientos para evitar problemas con la actualización: https://kb.vmware.com/kb/2145887.

Procedimiento

1 En vSphere Web Client, seleccione **Redes y seguridad (Networking & Security) > NSX Edge**.

2 Haga doble clic en cada instancia de NSX Edge y, a continuación, haga clic en **Administrar > VPN > VPN de Capa 2** (Manage > VPN > L2 VPN) y compruebe si la VPN de Capa 2 está habilitada. Si es así, elimine la configuración de la VPN de Capa 2 después de apuntar los detalles de dicha configuración.

3 Para cada instancia de NSX Edge, seleccione la opción **Versión de actualización** (Upgrade Version) en el menú **Acciones** (Actions).



Si en la actualización aparece el mensaje de error "No se pudo implementar el dispositivo Edge" (Failed to deploy edge appliance), asegúrese de que el host donde se implementa el dispositivo NSX Edge esté conectado y no esté en modo de mantenimiento.

Una vez que NSX Edge se actualiza correctamente, el **Estado** (Status) se implementa (Deployed) y la columna **Versión** (Version) muestra la nueva versión de NSX.

Si un dispositivo Edge no se puede actualizar y tampoco hay una reversión a la versión anterior, haga clic en el icono **Volver a implementar NSX Edge** (Redeploy NSX Edge) e intente actualizar nuevamente.

Qué hacer a continuación

Vuelva a configurar la VPN de Capa 2. Consulte la Descripción general de la VPN de Capa 2 en la *Guía de instalación de NSX*.

"Actualizar Guest Introspection en Cross-vCenter NSX," página 95

Actualizar Guest Introspection en Cross-vCenter NSX

Es importante que actualice Guest Introspection para que coincida con la versión de NSX Manager.

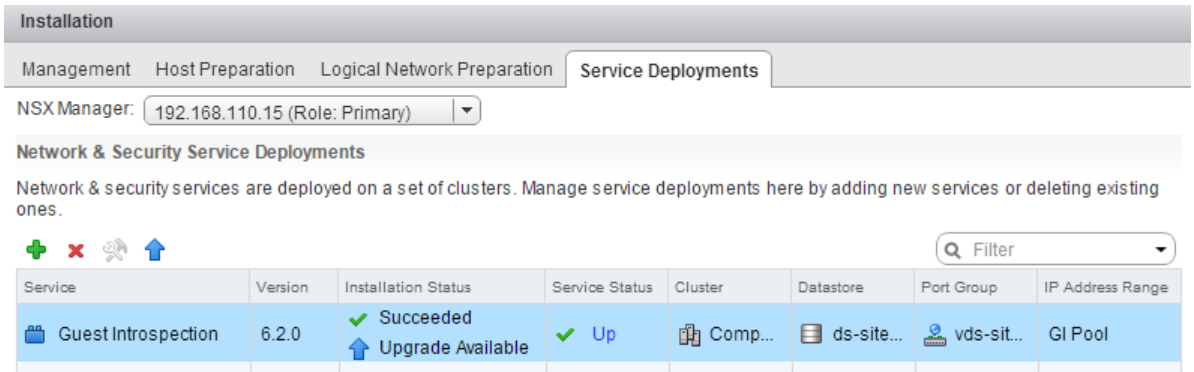
NOTA: Las máquinas virtuales de servicio de Guest Introspection se pueden actualizar desde vSphere Web Client. No es necesario eliminar la máquina virtual de servicio después de la actualización de NSX Manager para que se actualice. Si elimina la máquina virtual de servicio, el estado del servicio (Service Status) aparecerá como `Error` (Failed) ya que falta la máquina virtual agente. Haga clic en **Resolver** (Resolve) para implementar una nueva máquina virtual de servicio y, a continuación, haga clic en **Actualización disponible** (Upgrade Available) para implementar la máquina virtual de servicio de Guest Introspection más reciente.

Prerequisitos

NSX Manager, las controladoras, los clústeres del host preparados y NSX Edge deben estar actualizados a la versión 6.2.x.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

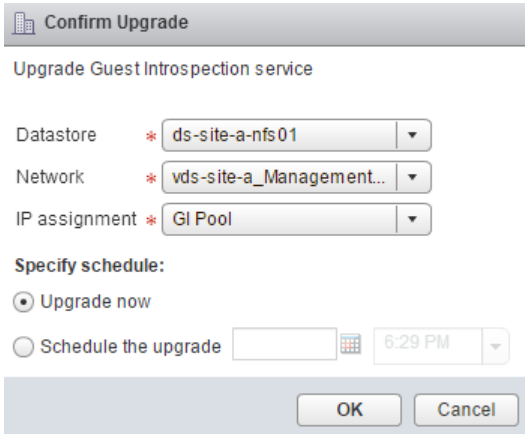


La columna **Estado de instalación** (Installation Status) indica **Actualización disponible** (Upgrade Available).

2 Seleccione la implementación de Guest Introspection que desea actualizar.

Se habilita el icono **Actualizar** (↑) (Upgrade) en la barra de herramientas ubicada encima de la tabla de servicios.

3 Haga clic en el icono **Actualizar** (⬆) (Upgrade) y siga las indicaciones de la interfaz de usuario.



Tras la actualización de Guest Introspection, el estado de la instalación es `Correcto` (Succeeded) y el estado del servicio aparece como `Listo` (Up). Las máquinas de servicio virtual de Guest Introspection están visibles en el inventario de vCenter Server.

Qué hacer a continuación

Después de actualizar Guest Introspection en un clúster concreto, puede actualizar las soluciones de los partners. Si las soluciones de los partners están habilitadas, consulte la documentación sobre la actualización que ellos mismos proporcionan. Aunque no se actualice la solución del partner, se mantiene la protección.

Servicios NSX Services que no admiten actualización directa

Algunas instancias de NSX Services como por ejemplo, los dispositivos virtuales de seguridad de VMware Partner, no admiten actualizaciones directas. En estos casos, debe desinstalar los servicios y volver a instalarlos.

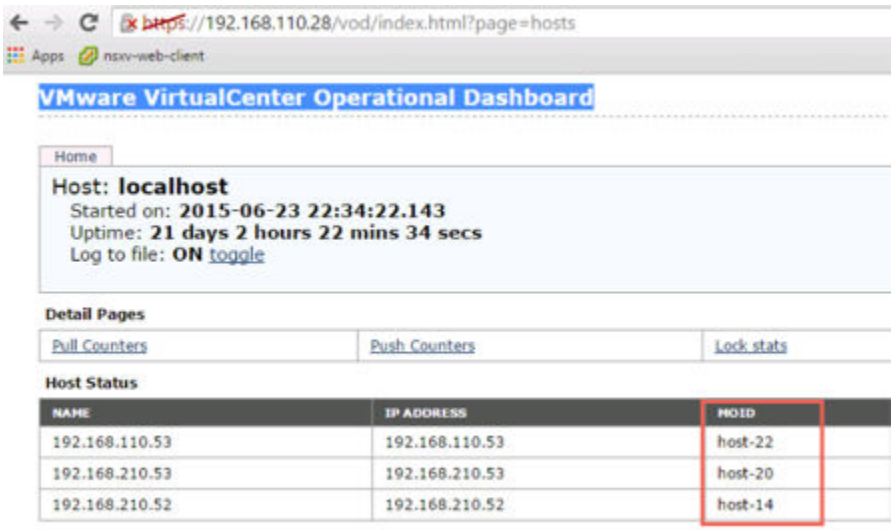
NSX Data Security

Lo ideal es desinstalar NSX Data Security antes de actualizar NSX, para volver a instalarlo después de completar la actualización de NSX. Si actualizó NSX sin desinstalar primero NSX Data Security, debe desinstalarlo con una llamada API de REST.

Emita la siguiente llamada API:

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

El identificador del host es el MOID del host ESXi. Para recuperar el MOID, abra el panel operativo de VMware VirtualCenter: https://<vcenter-ip>/vod/index.html?page=hosts.



Para el host ESXi con el MOID "host-22" en vCenter Server 192.168.110.28, la llamada API debería tener el siguiente formato:

```
DELETE https://192.168.110.28/api/1.0/vshield/host-22/vsds
```

Asegúrese de emitir la llamada API en todos los hosts ESXi.

Después de desinstalar Data Security, puede instalar la versión nueva. Consulte "Instalar NSX Data Security," página 37.

VPN SSL de NSX

A partir de NSX 6.2, la puerta de enlace de la VPN SSL solo acepta el protocolo TLS. A partir de NSX 6.2.3, el protocolo TLS 1.0 está obsoleto. Los dispositivos virtuales de seguridad de VMware Partner no admiten actualizaciones directas. Sin embargo, después de actualizar a NSX 6.2.x, todos los clientes nuevos de NSX 6.2.x creados utilizan automáticamente el protocolo TLS al establecer la conexión.

Cuando un cliente de NSX 6.0.x intenta conectarse con una puerta de enlace de NSX 6.2.x, se produce un error en el paso del enlace SSL al establecer la conexión. Este error se debe al cambio de protocolo.

Después de la actualización a NSX 6.2.x, desinstale los clientes de VPN SSL anteriores e instale la versión 6.2.x de NSX de los clientes de VPN SSL. Consulte "Instalar cliente SSL en un sitio remoto" en la *Guía de administración de NSX*.

VPN de Capa 2 de NSX

La configuración de una VPN de Capa 2 en una instancia de NSX Edge se debe eliminar para poder actualizar NSX Edge a NSX 6.2.x.

Instalar NSX Data Security

NOTA: Desde la versión 6.2.3 de NSX, la función de seguridad de datos de NSX pasó a estar obsoleta. En la versión 6.2.3 de NSX puede seguir utilizando esta función como desee, pero tenga en cuenta que se eliminará de NSX en versiones futuras.

Prerequisitos

NSX Guest Introspection debe instalarse en el clúster donde se va a instalar Data Security.

Si desea asignar una dirección IP a la máquina virtual del servicio Data Security desde un grupo de direcciones IP, cree el grupo de direcciones IP antes de instalar Data Security. Consulte Agrupar objetos en la *Guía de administración de NSX*.

Procedimiento

1 En la pestaña **Instalación** (Installation), haga clic en **Implementaciones de servicios** (Service Deployments).

2 Haga clic en el icono **Nueva implementación de servicios** (New Service Deployment) ( ).

3 En el cuadro de diálogo Implementar servicios de red y seguridad (Deploy Network and Security Services), seleccione **Data Security** y haga clic en **Siguiente** (Next).

4 En **Especificar programación** (Specify schedule), en la parte inferior del cuadro de diálogo, seleccione **Implementar ahora** (Deploy now) para implementar Data Security apenas se instale, o bien seleccione una fecha y una hora de implementación.

5 Haga clic en **Siguiente** (Next).

6 Seleccione el centro de datos y los clústeres donde desea instalar Data Security y, a continuación, haga clic en **Siguiente** (Next).

7 En la página Seleccionar red de almacenamiento y administración (Select storage and Management Network), seleccione el almacén de datos en el que desea agregar las máquinas virtuales de servicio, o bien seleccione **Especificado en el host** (Specified on host).

   El almacén de datos seleccionado debe estar disponible en todos los hosts del clúster elegido.

   Si seleccionó **Especificado en el host** (Specified on host), el almacén de datos del host ESX debe especificarse en la opción **Configuración de máquinas virtuales de agente** (AgentVM Settings) del host antes de agregarse al clúster. Consulte la *documentación de vSphere API/SDK*.

8 Seleccione el grupo de puertos virtuales distribuidos donde se alojará la interfaz de administración. Este grupo de puertos debe poder comunicarse con el grupo de puertos de NSX Manager.

   Si el almacén de datos se configura como **Especificado en el host** (Specified on host), la red que se utilizará debe especificarse en la propiedad **agentVmNetwork** de cada host en el clúster. Consulte la *documentación de vSphere API/SDK*.

   Cuando agrega hosts al clúster, la propiedad **agentVmNetwork** del host debe configurarse antes de agregarse al clúster.

   El grupo de puertos seleccionado debe estar disponible en todos los hosts del clúster seleccionado.

9 En la asignación de direcciones IP, seleccione una de las siguientes opciones:

Seleccionar	Para
DHCP	Asigne una dirección IP a las máquinas virtuales del servicio Data Security a través del protocolo de configuración dinámica de host (DHCP).
Grupo de direcciones IP	Asigne una dirección IP a las máquinas virtuales del servicio Data Security desde el grupo de direcciones IP seleccionado.

   Tenga en cuenta que no se admiten direcciones IP estáticas.

10 Haga clic en **Siguiente** (Next) y, a continuación, en **Finalizar** (Finish) en la página Listo para finalizar (Ready to complete).

11 Supervise la implementación hasta que la columna **Estado de instalación** (Installation Status) muestre **Correcto** (Succeeded).

12 Si la columna **Estado de instalación** (Installation Status) muestra **Con errores** (Failed), haga clic en el icono junto a Con errores. Se muestran todos los errores de implementación. Haga clic en **Resolver** (Resolve) para solucionar los errores. En algunos casos, al resolver los errores aparecen otros nuevos. Realice la acción necesaria y vuelva a hacer clic en **Resolver** (Resolve).

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

1 Elimine la snapshot de NSX Manager tomada durante la instalación.

2 Realice una copia de seguridad actualizada tras la actualización.

3 Asegúrese de que los VIB estén instalados en los hosts.

NSX Instala los siguientes VIB:

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Si se ha instalado Guest Introspection, compruebe también que este VIB se encuentra en los hosts:

```
esxcli software vib get --vibname epsec-mux
```

4 Vuelva a sincronizar el bus de mensajería del host. VMware aconseja a todos sus clientes que vuelvan a realizar una sincronización tras la actualización.

Puede usar la siguiente llamada API para volver a realizar la sincronización en cada host.

```
URL : 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
```

Índice

R

S

U

V