Guía de actualización de NSX

Actualización 8
Modificado el 12 de octubre de 2017
VMware NSX for vSphere 6.3

vmware®

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

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

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 la *Guía de actualización de NSX* se describe cómo actualizar el sistema VMware NSX® for vSphere® mediante la interfaz de usuario de NSX Manager y vSphere Web Client. La información incluye instrucciones de actualización paso a paso y prácticas recomendadas.

Público objetivo

Este manual está destinado a quienes deseen actualizar 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 las operaciones de centros de datos. En este manual se da por sentado que está familiarizado con VMware vSphere, incluidos VMware ESXi, vCenter Server y vSphere Web Client.

Glosario de publicaciones técnicas de VMware

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

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, compruebe 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.

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 por cada host ESXi™ y varias instancias de NSX Edge por cada centro de datos.

Hardware

Tabla 1. Requisitos de hardware para dispositivos

Dispositivo	Memoria	vCPU	Espacio de 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	28 GB
NSX Edge	■ Compacto: 512 MB ■ Grande: 1 GB ■ Cuádruple: 2 GB ■ Extra grande: 8 GB	■ Compacto: 1 ■ Grande: 2 ■ Tamaño cuádruple: 4 ■ Extra grande: 6	■ Compacto, grande, cuádruple: 1 disco de 584 MB + 1 disco de 512 MB ■ Extra grande: 1 disco de 584 MB + 1 disco de 2 GB + 1 disco de 256 MB
Guest Introspection	1 GB	2	4 GB

*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 aumentar la asignación de memoria y vCPU para sus dispositivos virtuales, consulte Asignar recursos de memoria y Cambiar el número de CPU virtuales en *Administración de máquinas virtuales de vSphere*.

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.

Para conocer las versiones recomendadas de NSX, vCenter Server y ESXi, consulte las notas de la versión en https://www.vmware.com/support/pubs/nsx_pubs.html y https://kb.vmware.com/kb/2144295.

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 Usar Modo vinculado mejorado (Enhanced Linked Mode) en *Administración de vCenter Server y hosts* .

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. Consulte Usar vSphere Web Client en la documentación de *Administración de vCenter Server y hosts* para obtener información detallada.

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 (Protocol)	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	443	TCP	Preparación del host ESXi	No	No	
vCenter Server	Host ESXi	443	TCP	Preparación del host ESXi	No	No	
Host ESXi	NSX Manager	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ
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 controladores, sincronización de estado	No	Sí	IPsec
NSX Controller	NSX Controller	7777	TCP	Puerto RPC entre controladores	No	Sí	IPsec
NSX Controller	NSX Controller	30865	TCP	Clúster de controladores, sincronización de estado	No	Sí	IPsec
NSX Manager	NSX Controller	443	TCP	Comunicación de controlador a Manager	No	Sí	Usuario/contraseña
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	No	Sí	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	No	Sí	
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 DNS	53	UDP	Conexión de cliente DNS	No	No	

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

Origen	Destino	Puerto	Protocolo (Protocol)	Propósito	Sensible	TLS	Autenticación
NSX Manager	Servidor syslog	514	TCP	Conexión de Syslog	No	Sí	
NSX Manager	Servidor syslog	514	UDP	Conexión de Syslog	No	Sí	
NSX Manager	Servidor horario NTP	123	TCP	Conexión de cliente NTP	No	Sí	
NSX Manager	Servidor horario NTP	123	UDP	Conexión de cliente NTP	No	Sí	
vCenter Server	NSX Manager	80	TCP	Preparación del host	No	Sí	
Cliente REST	NSX Manager	443	TCP	API de REST de NSX Manager	No	Sí	Usuario/contraseña
Terminal de túnel de VXLAN (VTEP)	Terminal de túnel de VXLAN (VTEP)	8472 (valor predeterminado antes de NSX 6.2.3) o 4789 (valor predeterminado en las instalaciones nuevas de NSX 6.2.3 y versiones posteriores)	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	
Máquina virtual de Guest Introspection	NSX Manager	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ

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

Origen	Destino	Puerto	Protocolo (Protocol)	Propósito	Sensible	TLS	Autenticación
NSX Manager principal	NSX Manager secundario	443	TCP	Servicio de sincronización Universal de Cross-vCenter NSX	No	Sí	
NSX Manager principal	vCenter Server	443	TCP	vSphere API	No	Sí	
NSX Manager secundario	vCenter Server	443	TCP	vSphere API	No	Sí	
NSX Manager principal	Clúster de controladores universal de NSX	443	TCP	API de REST de NSX Controller	No	Sí	Usuario/contraseña
NSX Manager secundario	Clúster de controladores universal de NSX	443	TCP	API de REST de NSX Controller	No	Sí	Usuario/contraseña
Host ESXi	Clúster de controladores universal de NSX	1234	TCP	Protocolo del plano de control de NSX	No	Sí	
Host ESXi	NSX Manager principal	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ
Host ESXi	NSX Manager secundario	5671	TCP	RabbitMQ	No	Sí	Usuario y contraseña de RabbitMQ

Puertos para Cross-vCenter NSX y Enhanced Linked Mode

Si tiene un entorno de Cross-vCenter NSX y los sistemas de vCenter Server están en modo Enhanced Linked Mode, cada dispositivo de NSX Manager debe tener la conectividad requerida por cada sistema de vCenter Server del entorno con el fin de administrar cualquier NSX Manager desde cualquier sistema de vCenter Server.

Actualizar NSX

1

Este capítulo cubre los siguientes temas:

- Prepararse para la actualización de NSX
- Actualizar a NSX 6.3.x
- Actualizar a NSX 6.3.x con Cross-vCenter NSX

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 cumpla los requisitos del sistema de NSX. Consulte el documento Requisitos del sistema para NSX.
2. Si se implementan los servicios de partners Extensibilidad de NSX y Guest Introspection, compruebe la compatibilidad antes de realizar la actualización:
   - En la mayoría de los casos, se puede actualizar NSX sin que esto afecte a las soluciones de los partners. Sin embargo, si su solución de partner no es compatible con la versión de NSX a la que está realizando la actualización, deberá actualizar la solución de partner a una versión compatible antes de actualizar NSX.
   - Consulte la Guía de compatibilidad de VMware para Redes y seguridad. 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 a NSX. Data Security no es compatible con NSX 6.3.x. Consulte el documento Desinstalar NSX Data Security.

4 Si tiene una puerta de enlace de hardware (hardware VTEP) instalada en su entorno, la actualización a NSX 6.3.0 y 6.3.1 estará bloqueada. Debe ponerse en contacto con el soporte técnico de VMware para continuar con la actualización. Consulte https://kb.vmware.com/kb/2148511 para obtener más información. Se permite la actualización a NSX 6.3.2.

5 Si tiene dispositivosNSX 5.5 o versiones anteriores de NSX Edge, debe actualizarlos a NSX 6.x antes de realizar la actualización a NSX 6.3.x.

6 Si va a actualizar a la versión 6.3.3 de NSX, el clúster de NSX Controller debe tener tres nodos de controlador. Si tiene menos de tres, debe agregar nodos adicionales antes de iniciar la actualización. Consulte "Implementar clúster de NSX Controller" en la *Guía de instalación de NSX* si desea saber los pasos necesarios para agregar nodos de controlador.

7 Planifique la actualización de todas las instancias de NSX Manager que estén conectadas a los sistemas de vCenter Server que utilicen el mismo servidor SSO (incluidos los sistemas de vCenter Server en Enhanced Linked Mode). Si no puede hacerlo, consulte https://kb.vmware.com/kb/2127061 para encontrar una solución alternativa.

8 Verifique 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.

9 Cree un paquete de servicio técnico.

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

11 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.

12 Descargue y organice el paquete de actualización, y valídelo con md5sum. Consulte Descargar el paquete de actualización de NSX y comprobar MD5.

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

14 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 de NSX 6.2.2 o una versión anterior a NSX 6.2.3 o una versión posterior, su licencia actual se convertirá en una licencia NSX Enterprise y tendrá derecho a las mismas funciones que se ofrece en Enterprise.

Para obtener información sobre las ediciones de licencias de NSX y sus características asociadas, consulte https://kb.vmware.com/kb/2145269.

Impactos operativos de las actualizaciones de NSX

El proceso de actualización de NSX puede tardar algún tiempo. 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 la actualización de todos los componentes de NSX en una sola ventana de interrupción para minimizar el tiempo de inactividad y reducir la confusión entre los usuarios de NSX que no puedan 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 información siguiente puede ayudar a los usuarios de NSX a entender cuáles son las funciones 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 hosts de NSX —> Enrutadores (lógicos) distribuidos —> Guest Introspection

Las puertas de enlace de servicios de Edge (ESG) se pueden actualizar en cualquier momento después de actualizar NSX Manager.

IMPORTANTE: Antes de iniciar la actualización, lea Prepararse para la actualización de NSX y las *Notas de la versión de NSX for vSphere* para obtener información detallada sobre los requisitos previos de actualización y los problemas conocidos de actualización.

Actualización de NSX Manager

Planificación de la actualización de NSX Manager:

- En un entorno cross-vCenter NSX, debe actualizar primero la instancia principal de NSX Manager y, a continuación, las instancias secundarias de NSX Manager.
- En un entorno cross-vCenter NSX, debe actualizar todas las instancias de NSX Manager en la misma ventana de mantenimiento.
- Si está actualizando de NSX 6.1.x a NSX 6.2.x o una versión posterior, debe actualizar NSX Manager y el clúster NSX Controller en la misma ventana de mantenimiento.

Impacto durante la actualización de NSX Manager:

- La configuración de NSX Manager mediante vSphere Web Client y la API está bloqueada.
- 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 a NSX ni desconectarse de los conmutadores lógicos durante la actualización de NSX Manager.

- Durante la actualización de NSX Manager en un entorno de Cross-vCenter NSX, no realice ningún cambio en los objetos universales hasta que el NSX Manager principal y todos los secundarios se actualicen. Esto incluye crear, actualizar o eliminar objetos universales y realizar operaciones relativas a objetos universales (por ejemplo, aplicar una etiqueta de seguridad universal a una máquina virtual).

Tras la actualización de NSX Manager:

- Se permiten todos los cambios de configuración de NSX.
- En esta etapa, si se implementa cualquier dispositivo NSX Controller, se implementará con la versión que coincida con el clúster de NSX Controller existente hasta que el clúster de NSX Controller esté actualizado.
- 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.
- Según la versión de NSX, una vez que NSX Manager se ha actualizado, el estado del canal de comunicación aparecerá como Desconocido (Unknown) para el plano de control. Debe completar las actualizaciones de hosts y controladores para ver el estado Activo (Up).

Actualización de clústeres de NSX Controller

Planificación de la actualización de NSX Controller:

- Puede actualizar el clúster de NSX Controller después de que se haya actualizado NSX Manager.
- En un entorno cross-vCenter NSX, debe actualizar todas las instancias de NSX Manager antes de actualizar el clúster de NSX Controller.
- VMware recomienda la actualización del clúster de NSX Controller en la misma ventana de mantenimiento que la actualización de NSX Manager.
- Si está actualizando de NSX 6.1.x a NSX 6.2.x o una versión posterior, debe actualizar NSX Manager y el clúster NSX Controller en la misma ventana de mantenimiento.

Impacto durante la actualización de NSX Controller:

- 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 clústeres de NSX Controller esté 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.
- No permita cambios en las rutas dinámicas durante la actualización.

Tras la actualización de NSX Controller:

- Se permiten cambios en la configuración.

Actualización de hosts NSX

Planificación de la actualización de clústeres de hosts de NSX:

- Puede actualizar los clústeres de hosts después de actualizar las instancias de NSX Manager y el clúster de NSX Controller.
- Puede actualizar sus clústeres de hosts en una ventana de mantenimiento independiente desde las actualizaciones del clúster de NSX Controllery de NSX Manager.
- No necesita actualizar todos los clústeres de hosts en la misma ventana de mantenimiento.
- Las nuevas características de la versión de NSX instalada en NSX Manager aparecen en vSphere Web Client y la API, pero puede que no funcionen hasta que se actualicen los VIB.
- Para aprovechar todas las nuevas características de una versión de NSX, actualice los clústeres de host para que los VIB de host coincidan con la versión de NSX Manager.

Impacto durante la actualización de clústeres de hosts de NSX:

- Los cambios en la configuración no se bloquean en NSX Manager.
- La comunicación del controlador al host posee compatibilidad con versiones anteriores, es decir que los controladores actualizados pueden comunicarse con los hosts no actualizados.
- La actualización se realiza por clúster. Si DRS está habilitado en el clúster, se encarga de administrar el orden de actualización de los hosts.
- Los hosts que se están sometiendo a una actualización se deben colocar en modo de mantenimiento, por lo que las máquinas virtuales deben apagarse o evacuarse a otros hosts. Esto puede realizarse con DRS o manualmente.
- Se permiten cambios y modificaciones en la red lógica.
- El aprovisionamiento de máquinas virtuales nuevas sigue funcionando en los hosts que no están actualmente en modo de mantenimiento.

Actualización de NSX Edge

Planificación de la actualización de NSX Edge:

- Puede actualizar NSX Edges en ventanas de mantenimiento independientes desde otros componentes de NSX.
- Puede actualizar los enrutadores lógicos después de que se hayan actualizado los clústeres de hosts, el cúster de NSX Controller y las instancias de NSX Manager.
- Puede actualizar una puerta de enlace de servicios Edge aunque aún no haya actualizado los clústeres de hosts ni el clúster de NSX Controller.
- No necesita actualizar todos los NSX Edges en la misma ventana de mantenimiento.

- Si hay una actualización disponible para NSX Edge pero aún no la ha implementado, se bloquearán las funciones de cambio de tamaño, recursos, almacén de datos, habilitar depuración avanzada y habilitar High Availability (HA) en el dispositivo hasta que esta actualización se lleve a cabo.

Impacto durante la actualización de NSX Edge:

- 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.

Tras la actualización de NSX Edge:

- No se bloquean los cambios de configuración. No es posible configurar todas las características nuevas introducidas para la puerta de enlace de servicios Edge (ESG) en la actualización de NSX no hasta que todas los controladores NSX Controller y todos los clústeres de hosts se hayan actualizado.

Actualización de Guest Introspection

Planificación de la actualización de Guest Introspection:

- Puede actualizar Guest Introspection después de que se hayan actualizado los clústeres de hosts, el clúster de NSX Controller y los NSX Manager.
- Consulte la documentación del partner para obtener información sobre la actualización de soluciones de partners.

Impacto durante la actualización de Guest Introspection:

- 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 de la actualización de Guest Introspection:

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

Información sobre el modo FIPS y la actualización de NSX

A partir de NSX 6.3.0, puede habilitar el modo FIPS, que activa los conjuntos de claves de cifrado que cumplen los requisitos de FIPS.

ADVERTENCIA: Cuando realice una actualización desde una versión de NSX anterior a NSX 6.3.0 a NSX 6.3.0 o versiones posteriores, no debe habilitar el modo FIPS antes de que se haya completado la actualización. Si habilita el modo FIPS antes de que se haya completado la actualización, la comunicación entre los componentes actualizados y no actualizados se interrumpirá.

Estado de FIPS y actualización de NSX

Tabla 1-1. Estado del modo FIPS en los componentes de NSX tras la actualización a NSX 3.3.x.pu

Componente de NSX	Estado del modo FIPS
NSX Manager	Después de actualizar a 6.3.x, el modo FIPS estará disponible y desactivado en los dispositivos NSX Manager. No habilite FIPS hasta que se haya completado la actualización de todos los componentes de NSX y FIPS haya sido habilitado en todos los dispositivos NSX Edge.
Clúster de NSX Controller	Después de actualizar a 6.3.x, el clúster de NSX Controller cumple los requisitos de FIPS. Esto no se puede configurar.
Clústeres de hosts de NSX	Después de actualizar a 6.3.x, los clústeres de hosts de NSX cumplen los requisitos de FIPS. Esto no se puede configurar.
NSX Edge	Después de actualizar a 6.3.x, el modo FIPS estará disponible y desactivado en los dispositivos NSX Edge. No habilite FIPS hasta que se haya completado la actualización de todos los componentes de NSX.
Máquina virtual de servicio de Guest Introspection	Después de actualizar a 6.3.x, la máquina virtual de servicio de Guest Introspection cumple los requisitos de FIPS. Esto no se puede configurar.

Habilitar FIPS

Si actualiza a NSX 6.3 y quiere habilitar FIPS, debe completar los siguientes pasos:

1 Verifique que todas las soluciones de los partners tengan un certificado para el modo FIPS. Consulte la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security. Compruebe la documentación del partner para obtener más información.

2 Actualice NSX Manager a NSX 6.3.0 o versiones posteriores.

3 Actualice el clúster de NSX Controller a NSX 6.3.0 o versiones posteriores.

4 Actualice todos los clústeres de hosts que ejecuten cargas de trabajo de NSX a NSX 6.3.0 o versiones posteriores.

5 Actualice todos los dispositivos NSX Edge a NSX 6.3.0 o versiones posteriores.

6 Si está instalado, actualice Guest Introspection en todos los clústeres de hosts a NSX 6.3.0 o versiones posteriores.

7 Habilite el modo FIPS en los dispositivos NSX Edge. Consulte Cambiar el modo FIPS en NSX Edge en la *Guía de administración de NSX*.

8 Habilite el modo FIPS en los dispositivos NSX Manager. Consulte el documento sobre cómo cambiar la configuración del modo FIPS y TLS en NSX Manager en la *Guía de administración de NSX*.

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

NSX Data Security quedó en desuso en NSX 6.2.3 y se eliminó de NSX 6.3.0. Debe desinstalar NSX Data Security antes de actualizar a NSX 6.3.x.

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.

Copia de seguridad y restauración de NSX Manager

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.

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.

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).

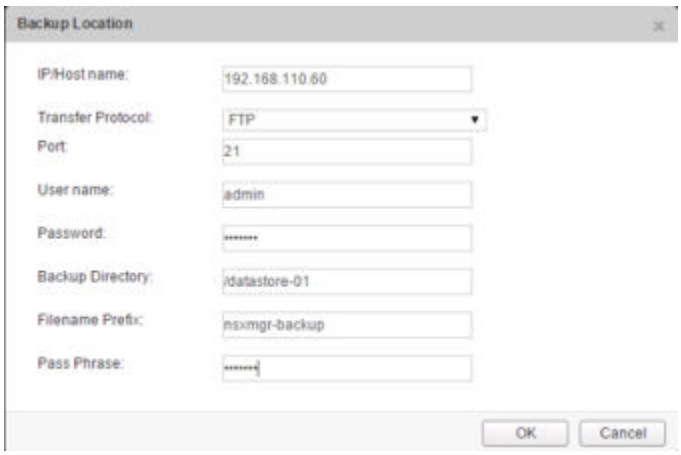
   Este texto se agrega antes del nombre de archivo de cada copia de seguridad para que el sistema de copia de seguridad lo reconozca fácilmente. Por ejemplo, si escribe **ppdb**, la copia de seguridad resultante se denominará `ppdbHH_MM_SS_DayDDMonYYYY`.

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).

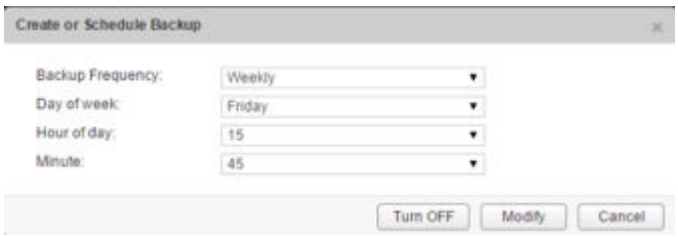
Por ejemplo:



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 se admite. 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 consiste en anotar la configuración actual del dispositivo NSX Manager antiguo para utilizarla en el momento de especificar la información relativa a la dirección IP y a la ubicación de las copias de seguridad del dispositivo NSX Manager recientemente implementado.

Procedimiento

1 Anote toda la configuración del dispositivo NSX Manager existente. Asimismo, anote la configuración del servidor FTP.

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 la configuración del servidor FTP.

   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.

   La sección **Historial de copias de seguridad** (Backup History) muestra la carpeta para las copias de seguridad.

   NOTA: Si la carpeta de copias de seguridad no aparece en la sección **Historial de copias de seguridad**, compruebe la configuración del servidor FTP. Compruebe si puede conectarse al servidor FTP y ver la carpeta de copias de seguridad.

6 En la sección **Historial de copias de seguridad**, seleccione la carpeta de copias de seguridad requerida que desea restaurar y haga clic en **Restaurar** (Restore).

   Comienza el proceso de restauración de los datos de NSX Manager.

La configuración de NSX se restaura a NSX Manager.

ADVERTENCIA: Después de restaurar una copia de seguridad de NSX Manager, es posible que tenga que tomar medidas adicionales para garantizar el funcionamiento correcto de los dispositivos NSX Edge y de los conmutadores lógicos. Consulte Restaurar los NSX Edge y Solucionar errores de sincronización en conmutadores lógicos.

Restaurar los 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.

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

Si tiene una configuración de NSX Manager intacta, puede volver a crear una máquina virtual de dispositivo Edge inaccesible o con errores volviendo a implementar NSX Edge (haga clic en **Volver a implementar NSX Edge [Redeploy NSX Edge] [ ]** en vSphere Web Client). Consulte "Volver a implementar NSX Edge" en la *Guía de administración de NSX*.

ADVERTENCIA: Después de restaurar una copia de seguridad de NSX Manager, es posible que tenga que tomar medidas adicionales para garantizar el funcionamiento correcto de los dispositivos NSX Edge.

- Los dispositivos de Edge que se crearon después de la última copia de seguridad no se eliminan durante la restauración. Debe eliminar la máquina virtual manualmente.
- Los dispositivos de Edge que se eliminaron después de la última copia de seguridad no se restauran a menos que se vuelvan a implementar.
- Si no existen ni las ubicaciones configuradas ni las actuales de un dispositivo NSX Edge almacenadas en la copia de seguridad cuando se restaura la copia de seguridad, se producirán errores en operaciones como la reimplementación, la migración, la habilitación o la deshabilitación de HA. Debe editar la configuración del dispositivo y proporcionar información de ubicación válida. Utilice `PUT /api/4.0/edges/{edgeId}/appliances` para editar la configuración de ubicación del dispositivo (*resourcePoolId*, *datastoreId*, *hostId* y *vmFolderId* según sea necesario). Consulte "Trabajar con la configuración del dispositivo NSX Edge" en la *Guía de NSX API*.

Si se produjo alguno de los siguientes cambios desde la última copia de seguridad de NSX Manager, la configuración restaurada de NSX Manager y la configuración presente en el dispositivo NSX Edge serán diferentes. Debe **Forzar sincronización** (Force Sync) de NSX Edge para revertir estos cambios en el dispositivo y asegurar que NSX Edge funcione correctamente. Consulte "Forzar sincronización de NSX Edge con NSX Manager" en la *Guía de administración de NSX*.

- Cambios realizados a través de Distributed Firewall en preRules del firewall de NSX Edge.
- Cambios en la pertenencia de los objetos de grupo.

Si se produjo alguno de los siguientes cambios desde la última copia de seguridad de NSX Manager, la configuración restaurada de NSX Manager y la configuración presente en el dispositivo NSX Edge serán diferentes. Debe **Volver a implementar** (Redeploy) NSX Edge para revertir los cambios en el dispositivo y asegurar que NSX Edge funcione correctamente. Consulte "Volver a implementar NSX Edge" en la *Guía de administración de NSX*.

- Cambios en la configuración del dispositivo de Edge:
  - HA habilitado o deshabilitado
  - dispositivo que pasó de estado implementado a sin implementar
  - dispositivo que pasó de estado sin implementar a implementado
  - configuración de reserva de recursos cambiada
- Cambios en la configuración de vNic del dispositivo de Edge:
  - agregar, quitar o desconectar vNic
  - grupos de puertos
  - puertos troncales
  - parámetros de contención
  - directiva de catalogación

Solucionar errores de sincronización en conmutadores lógicos

Si se producen cambios en los conmutadores lógicos entre la realización de una copia de seguridad de NSX Manager y la restauración de la misma, es posible que estos conmutadores no se sincronicen correctamente.

Procedimiento

1. Inicie sesión en vSphere Web Client.
2. Vaya a **Redes y seguridad > Conmutadores lógicos** (Networking & Security > Logical Switches).
3. Si esto es así, haga clic en el vínculo **No sincronizado** (Out of sync) de la columna Estado (Status) para mostrar información detallada de los errores.
4. Haga clic en **Resolver** (Resolve) para volver a crear los grupos de puertos de respaldo que faltan para el conmutador lógico.

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.

La configuración de conmutador distribuido de vSphere y la configuración del grupo de puertos se incluyen en la importación.

La práctica recomendada consiste en exportar la configuración de conmutador distribuido de vSphere 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 a NSX 6.3.x

Para actualizar a NSX 6.3.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 (consulte Nota)

5 Guest Introspection

NOTA: Las puertas de enlace de servicios de Edge (ESG) se pueden actualizar en cualquier momento después de actualizar NSX Manager. No obstante, los enrutadores lógicos no se pueden actualizar hasta que el clúster de instancias de NSX Controller y los clústeres de hosts se hayan actualizado. Consulte Impactos operativos de las actualizaciones de NSX para obtener más información sobre las dependencias de las actualizaciones.

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.

Si está actualizando de NSX 6.1.x a NSX 6.2.x o una versión posterior, debe actualizar NSX Manager y el clúster NSX Controller en la misma ventana de mantenimiento.

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 ejecute `show filesystems` para mostrar el uso del sistema de archivos.
  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.

- Compruebe que la memoria reservada para el dispositivo virtual de NSX Manager cumpla los requisitos del sistema antes de realizar la actualización.

  Consulte Requisitos del sistema para NSX.
- Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte Desinstalar NSX Data Security. La función Seguridad de datos (Data Security) se eliminó desde la versión NSX 6.3.x.
- 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.
- Descargue el paquete de actualización y compruebe MD5. Consulte Descargar el paquete de actualización de NSX y comprobar MD5.
- 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.

Procedimiento

1. Inicie sesión en el dispositivo virtual NSX Manager.
2. En la página de inicio, 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. Vuelva a iniciar sesión en el dispositivo virtual de NSX Manager y desde la página de inicio haga clic en **Actualizar** (Upgrade). Confirme que el estado de la actualización sea **Completada** (Complete) y que la versión y el número de compilación de la parte superior derecha coincida con el paquete de actualizaciones que acaba de instalar.

Tras la actualización de NSX Manager, debe cerrar sesión y volver a iniciarla en vSphere Web Client.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su explorador. Si no se realiza este paso, es posible que aparezca un mensaje de error que indique que se produjo un error interno, como "An internal error has occurred - Error #1009", cuando se hacen cambios de configuración de NSX en vSphere Web Client.

Si la pestaña Redes y seguridad (Networking and Security) no aparece en vSphere Web Client, restablezca el servidor de vSphere Web Client.

- En vCenter 5.5, abra https://<vcenter-ip>:5480 y reinicie el servidor de vSphere Web Client.
- En vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como usuario 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 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. 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 los controladores durante un período de mantenimiento.

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

Si se implementan controladores nuevos antes de que se actualicen los existentes, se implementan en la versión anterior. Los nodos de controlador deben ser de la misma versión para poder unirse a un clúster.

NOTA: En la versión 6.3.3 de NSX cambia el sistema operativo subyacente de NSX Controller. Esto significa que cuando actualice a la versión 6.3.3 de NSX, en lugar de realizar una actualización de software, los controladores existentes se eliminarán uno a uno y los nuevos controladoras del sistema operativo Photon se implementarán con las mismas direcciones IP.

Prerequisitos

- Asegúrese de que todos los controladores estén en estado normal. La actualización no es posible si uno o varios controladores están en estado desconectado. Para reconectar un controlador desconectado, intente restablecer el dispositivo virtual del controlador. En la vista **Hosts y clústeres** (Hosts and Clusters), haga clic con el botón derecho en el controlador y seleccione **Alimentación > Restablecer** (Power > Reset).
- Un clúster de NSX Controller válido contiene tres nodos de controlador. Inicie sesión en los tres nodos de controlador y ejecute el comando **show control-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 controlador informe sobre el estado Unión completa (Join Complete).
  - En el estado Mayoría (Majority), compruebe que el controlador esté conectado a la mayoría del clúster.
  - En el identificador del clúster, todos los nodos de controlador de un clúster deben tener el mismo identificador de clúster.
  - En los estados Configurado (Configured) y Activo (Active), compruebe que todas las funciones del controlador 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.
- Si va a actualizar a la versión 6.3.3 de NSX, el clúster de NSX Controller debe tener tres nodos de controlador. Si tiene menos de tres, debe agregar nodos adicionales antes de iniciar la actualización. Consulte "Implementar clúster de NSX Controller" en la *Guía de instalación de NSX* si desea saber los pasos necesarios para agregar nodos de controlador.

Procedimiento

- 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 controlador** (Controller Cluster Status).

  Los controladores del entorno se actualizan y se reinician de uno a uno. Después de iniciar la actualización, el sistema descarga el archivo de actualización, actualiza y reinicia cada controlador, y actualiza el estado de actualización de cada controlador. Los siguientes campos muestran el estado del controlador:

  - La columna **Estado de clúster de controlador** (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 todos los controladores del clúster, el estado cambia a **En curso** (In progress). Una vez actualizados todos los controladores del clúster, el estado que aparece es **Finalizado** (Complete) y la columna ya no se muestra.
  - La columna **Estado** (Status) en la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de cada controlador, que es **Conectado** (Connected) o **Normal** (Normal) antes de la actualización, dependiendo de la versión NSX original. Cuando los servicios del controlador se apagan y se reinicia el controlador, el estado cambia a **Desconectado** (Disconnected). Una vez completada la actualización del controlador, el estado es **Conectado** (Connected).
  - La columna **Estado de actualización** (Upgrade Status) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de actualización de cada controlador. 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 el controlador está actualizado, el estado indica **Actualizado** (Upgraded).

    NOTA: Al actualizar de NSX 6.3.2 o versiones anteriores a NSX 6.3.3 o versiones posteriores, el estado **Descargando archivo de actualización** (Downloading upgrade file) se reemplaza por **En cola para actualización** (Queued For Upgrade).

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 **6.3.***buildNumber* para cada controlador. Vuelva a ejecutar el comando **show control-cluster status** para garantizar que los controladores puedan crear una mayoría. Si no se vuelve a formar la mayoría del clúster de NSX Controller, revise los registros del controlador 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 del controlador tiene errores, revise la conectividad entre los controladores y NSX Manager.

Hay casos en los que el primer controlador se actualiza correctamente y el segundo no lo hace. Supongamos que el clúster tiene tres controladores: el primero se actualizó correctamente a la nueva versión y el segundo se está actualizando. Si la actualización del segundo controlador tiene errores, este controlador podría quedar en estado desconectado. Al mismo tiempo, el primer controlador y el tercero 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 otro controlador. El nuevo controlador tendrá la versión anterior (coincidente con el tercer controlador) y, por lo tanto, formará una mayoría con el tercer controlador. En este punto, se puede reiniciar el procedimiento de actualización. Consulte Reimplementar un NSX Controller en la *Guía para solucionar problemas de NSX* para obtener instrucciones sobre la creación de otro controlador.

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, puede actualizar los clústeres correspondientes del entorno.

Al actualizar los clústeres del host, se actualizan los VIB de NSX.

Si va a actualizar de NSX 6.2.x o versiones anteriores, o si está actualizando desde NSX 6.3.0 o versiones posteriores con ESXi 5.5, los hosts se deben reiniciar para completar la actualización.

- Si el clúster tiene DRS habilitado, cuando haga clic en **Resolver todo** (Resolve all), DRS intentará reiniciar los hosts de una forma controlada que permita que las máquinas virtuales continúen en ejecución. Las máquinas virtuales se desplazan a otros hosts en el clúster y los hosts deben entrar en modo de mantenimiento y reiniciarse.
- Si el clúster no tiene DRS habilitado, debe apagar vMotion o las máquinas virtuales manualmente antes de comenzar la actualización. Al hacer clic en **Resolver todo** (Resolve all), los hosts entran en el modo de mantenimiento y se reinician.

Si está actualizando desde NSX 6.3.0 o versiones posteriores con ESXi 6.0 o versiones posteriores, los hosts deben entrar en el modo de mantenimiento para completar la actualización. No es necesario reiniciar.

- Si el clúster tiene DRS habilitado, cuando haga clic en **Resolver todo** (Resolve all), DRS intentará que los hosts entren en modo de mantenimiento de una forma controlada que permita que las máquinas virtuales continúen en ejecución. Las máquinas virtuales se desplazan a otros hosts en el clúster y los hosts deben entrar en modo de mantenimiento.

- Si el clúster no tiene DRS habilitado, debe apagar vMotion o las máquinas virtuales manualmente antes de comenzar la actualización. Debe poner los hosts en modo de mantenimiento de forma manual para completar la actualización.

Prerequisitos

- 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.
- Asegúrese de 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.
  - 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 anticompatibilidad 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 anticompatibilidad durante la actualización y vuelva a habilitarlas una vez completada la actualización. Para deshabilitar una regla anticompatibilidad, desplácese hasta **Hosts y clústeres (Hosts and Clusters) > *Clúster (Cluster)* > Administrar (Manage) > Configuración (Settings) > Reglas de VM/Host (VM/Host Rules)**. Edite la regla y anule la selección de **Habilitar regla** (Enable rule).
- Inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list`.

  Los VIB presentes dependen de las versiones de ESXi y NSX y, por tanto, pueden cambiar como parte de la actualización. Observe la versión actual de los VIB instalados:

Versión de ESXi	Versión de NSX	VIB instalados
5.5	6.1.x, 6.2.x o 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.2 o anterior	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.3 o posterior	■ esx-nsxv

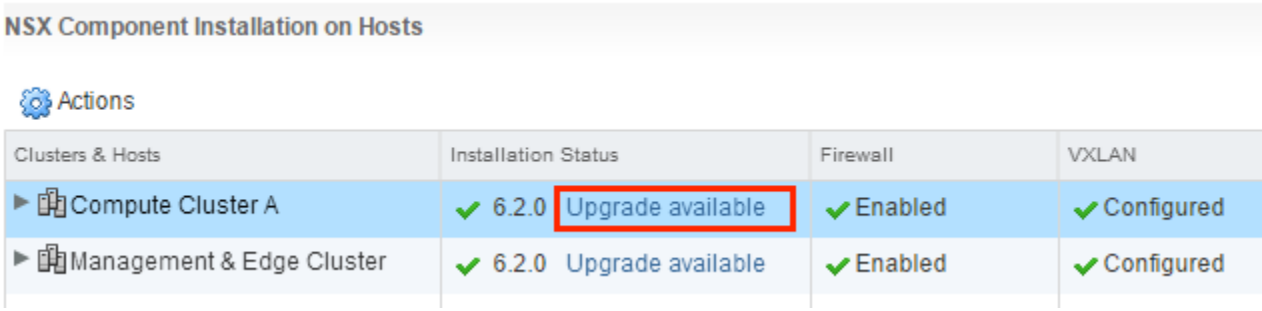
NOTA: Algunas versiones de NSX tienen VIB adicionales que se eliminarán durante la actualización.

- Si va a actualizar desde una versión anterior a NSX 6.2, los hosts preparados tienen un VIB adicional: esx-dvfilter-switch-security.
- Si va a actualizar desde NSX 6.2.x (donde la versión es NSX 6.2.4 o posterior), los hosts preparados tienen un VIB adicional: esx-vdpi.

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 opción Estado de instalación (Installation Status) muestra `Instalando` (Installing).

3 El clúster Estado de instalación (Installation Status) muestra `No está listo` (Not Ready). Haga clic en **No está listo** (Not Ready) para mostrar más información. Haga clic en **Resolver todo** (Resolve all) para intentar completar la instalación de los VIB.

Para completar la actualización, los hosts se deben poner en modo de mantenimiento y, si es necesario, se reiniciarán.

La columna Estado de instalación (Installation Status) muestra `Instalando` (Installing). Una vez completada la actualización, la columna Estado de instalación (Installation Status) muestra una marca de verificación de color verde y la versión NSX actualizada.

4 Si se produce un error en la acción **Resolver** (Resolve) cuando DRS está habilitado, es posible que los hosts requieran una intervención manual para entrar 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 **No está listo** (Not Ready) para mostrar más información. 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).

   La columna Estado de instalación (Installation Status) muestra `Instalando` (Installing). Una vez completada la actualización, la columna Estado de instalación (Installation Status) muestra una marca de verificación de color verde y la versión NSX actualizada.

5 Si se produce un error en la acción **Resolver** (Resolve) cuando DRS está deshabilitado y está actualizando desde NSX 6.3.0 o versiones posteriores con ESXi 6.0 o versiones posteriores, debe poner los hosts en modo de mantenimiento de forma manual para completar la actualización.

   a Ponga los hosts evacuados en modo de mantenimiento.

   b Desplácese a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)**.

      La actualización se inicia automáticamente cuando los hosts entran en modo de mantenimiento. La columna Estado de instalación (Installation Status) muestra `Instalando (Installing)`. Si no ve el estado `Instalando` (Installing), actualice la página.

      Una vez completada la actualización, la columna Estado de instalación (Installation Status) muestra una marca de verificación de color verde y la versión NSX actualizada.

   c Quite los hosts del modo de mantenimiento.

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

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.

Consulte el tema Preparación de host en la *Guía para solucionar problemas de NSX* para ver más pasos de solución de problemas.

Qué hacer a continuación

Actualizar NSX Edge

Actualizar NSX Edge

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 se haya actualizado NSX Manager.
- Compruebe que el clúster de NSX Controller y la preparación del host se hayan actualizado antes de actualizar los enrutadores lógicos.
- 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 los Requisitos del sistema para NSX si desea obtener información sobre los recursos necesarios para el tamaño de cada instancia de NSX Edge.
  - Para una instancia individual de NSX Edge, hay dos dispositivos de NSX Edge del tamaño en el estado encendido (poweredOn) durante la actualización.
  - Para una instancia de NSX Edge con alta disponibilidad, se implementan ambos dispositivos de sustitución antes de reemplazar los antiguos dispositivos. Esto significa que hay cuatro dispositivos NSX Edge del tamaño adecuado en el estado encendido (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.
- Compruebe que los clústeres de host enumerados en la ubicación configurada y la ubicación en vivo para el dispositivo NSX Edge estén preparados para NSX y que el estado de su infraestructura de mensajería sea de color `VERDE`. Si la ubicación configurada no está disponible, por ejemplo, debido a que se quitó el clúster al crearse el dispositivo NSX Edge, compruebe solo la ubicación en vivo.
  - Busque el ID de la ubicación configurada original (*configuredResourcePool* > *id*) y la ubicación en vivo actual (*resourcePoolId*) con la solicitud de la API `GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances`.

- Busque el estado de preparación del host y el estado de la infraestructura de mensajería para los clústeres con la solicitud de la API `GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}`, donde *resourceId* es el ID de la ubicación configurada y en vivo de los dispositivos de NSX Edge que se detectaron anteriormente.
  - Busque el estado correspondiente al *featureId* de `com.vmware.vshield.vsm.nwfabric.hostPrep` en el cuerpo de la respuesta. El estado debe ser de color `VERDE`.

    ```
    <nwFabricFeatureStatus>
      <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
      <featureVersion>6.3.1.5124716</featureVersion>
      <updateAvailable>false</updateAvailable>
      <status>GREEN</status>
      <installed>true</installed>
      <enabled>true</enabled>
      <allowConfiguration>false</allowConfiguration>
    </nwFabricFeatureStatus>
    ```

  - Busque el estado correspondiente al *featureId* de `com.vmware.vshield.vsm.messagingInfra` en el cuerpo de la respuesta. El estado debe ser de color `VERDE`.

    ```
    <nwFabricFeatureStatus>
      <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
      <updateAvailable>false</updateAvailable
      <status>GREEN</status>
      <installed>true</installed>
      <enabled>true</enabled>
      <allowConfiguration>false</allowConfiguration>
    </nwFabricFeatureStatus>
    ```

- 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 en la *Guía de actualización de NSX*.
- Si va a actualizar desde NSX 6.0.x y tiene una VPN de Capa 2 habilitada en una instancia de NSX Edge, debe borrar la configuración de esa conexión antes de realizar la actualización. Después de la actualización, puede volver a configurar la VPN de Capa 2. Consulte "Descripción general de VPN de Capa 2" en la *Guía de instalación de NSX*.

Procedimiento

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

2 Para cada instancia de NSX Edge, seleccione la opción **Actualizar versión** del 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

Tras actualizar NSX Edge 6.2.4 a la versión 6.2.5 u otras posteriores, debe desactivar la opción para iniciar la máquina virtual de vSphere en cada NSX Edge que se encuentre en un clúster en el que esté habilitado vSphere HA y en el que se hayan implementado Edges. Para hacerlo, abra vSphere Web Client y busque el host ESXi en la ubicación de la máquina virtual de NSX Edge. Haga clic en **Administrar (Manage) > Configuración (Settings)** y, en Máquinas virtuales (Virtual Machines), seleccione Encendido/Apagado de VM (VM Startup/Shutdown), haga clic en **Editar** (Edit) y asegúrese de que la máquina virtual esté en modo manual (es decir, asegúrese de que no se haya agregado a la lista de encendido/apagado automático).

Actualizar Guest Introspection

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

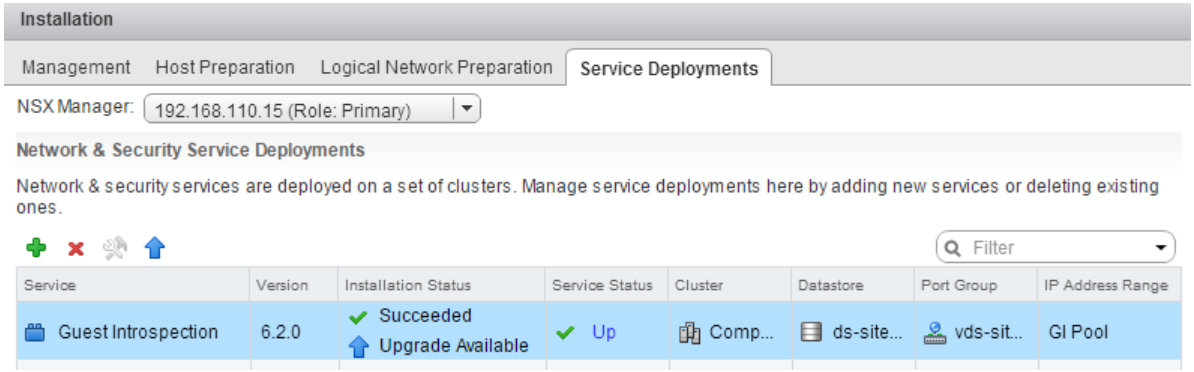
NOTA: Las máquinas virtuales de servicio de Guest Introspection se pueden actualizar desde vSphere Web Client. No es necesario eliminar la máquina virtual de servicio después de la actualización de NSX Manager para que se actualice. Si elimina la máquina virtual de servicio, el estado del servicio (Service 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

Actualizar NSX Manager, controladores, clústeres de hosts preparados e instancias de NSX Edge.

Procedimiento

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

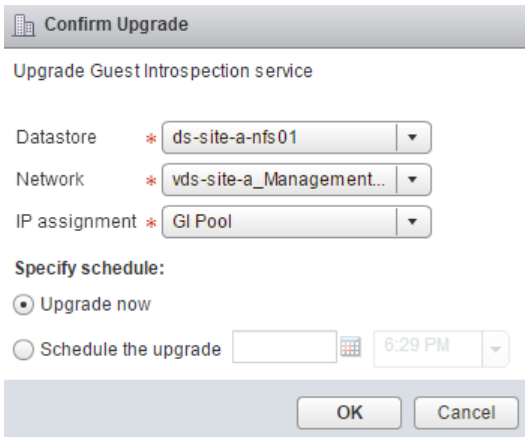


La columna **Estado de instalación** (Installation Status) indica **Actualización disponible** (Upgrade Available).

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

Algunos servicios NSX Services no admiten una actualización directa. En estos casos, debe desinstalar los servicios y volver a instalarlos.

Dispositivos virtuales de seguridad de VMware Partner

Compruebe la documentación de partners para comprobar si se puede actualizar el dispositivo virtual de seguridad para partners.

VPN SSL de NSX

A partir de NSX 6.2, la puerta de enlace de la VPN SSL solo acepta el protocolo TLS. Sin embargo, después de actualizar a NSX 6.2 o una versión posterior, todos los clientes nuevos que cree utilizarán automáticamente el protocolo TLS al establecer la conexión. Además, a partir de NSX 6.2.3, el protocolo TLS 1.0 está obsoleto.

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

Después de la actualización desde NSX 6.0.x, desinstale los clientes de VPN SSL anteriores e instale la versión 6.3.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

No se admite la actualización de NSX Edge si dispone de una VPN de Capa 2 instalado en una instancia de NSX Edge con NSX 6.0.x instalado. La configuración de una VPN de Capa 2 se debe eliminar para poder actualizar NSX Edge.

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

1. Realice una copia de seguridad actualizada tras la actualización.
2. 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
```

3 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 6.3.x con Cross-vCenter NSX

Para actualizar a NSX 6.3.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.

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.

Durante la actualización de NSX Manager en un entorno de Cross-vCenter NSX, no realice ningún cambio en los objetos universales hasta que el NSX Manager principal y todos los secundarios se actualicen. Esto incluye crear, actualizar o eliminar objetos universales y realizar operaciones relativas a objetos universales (por ejemplo, aplicar una etiqueta de seguridad universal a una máquina virtual).

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 ejecute `show filesystems` para mostrar el uso del sistema de archivos.
  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.
- Compruebe que la memoria reservada para el dispositivo virtual de NSX Manager cumpla los requisitos del sistema antes de realizar la actualización.

  Consulte Requisitos del sistema para NSX.
- Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte Desinstalar NSX Data Security. La función Seguridad de datos (Data Security) se eliminó desde la versión NSX 6.3.x.
- 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.
- Descargue el paquete de actualización y compruebe MD5. Consulte Descargar el paquete de actualización de NSX y comprobar MD5.
- 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.

Procedimiento

1. Inicie sesión en el dispositivo virtual NSX Manager.
2. En la página de inicio, 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 Vuelva a iniciar sesión en el dispositivo virtual de NSX Manager y desde la página de inicio haga clic en **Actualizar** (Upgrade). Confirme que el estado de la actualización sea **Completada** (Complete) y que la versión y el número de compilación de la parte superior derecha coincida con el paquete de actualizaciones que acaba de instalar.

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.

Tras la actualización de NSX Manager, debe cerrar sesión y volver a iniciarla en vSphere Web Client.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su explorador. Si no se realiza este paso, es posible que aparezca un mensaje de error que indique que se produjo un error interno, como "An internal error has occurred - Error #1009", cuando se hacen cambios de configuración de NSX en vSphere Web Client.

Si la pestaña Redes y seguridad (Networking and Security) no aparece en vSphere Web Client, restablezca el servidor de vSphere Web Client.

- En vCenter 5.5, abra https://<vcenter-ip>:5480 y reinicie el servidor de vSphere Web Client.
- En vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como usuario 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 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. 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 de NSX Manager en un entorno de Cross-vCenter NSX, no realice ningún cambio en los objetos universales hasta que el NSX Manager principal y todos los secundarios se actualicen. Esto incluye crear, actualizar o eliminar objetos universales y realizar operaciones relativas a objetos universales (por ejemplo, aplicar una etiqueta de seguridad universal a una máquina virtual).

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 ejecute `show filesystems` para mostrar el uso del sistema de archivos.
  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.
- Compruebe que la memoria reservada para el dispositivo virtual de NSX Manager cumpla los requisitos del sistema antes de realizar la actualización.

  Consulte Requisitos del sistema para NSX.
- Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar NSX Manager. Consulte Desinstalar NSX Data Security. La función Seguridad de datos (Data Security) se eliminó desde la versión NSX 6.3.x.
- 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.
- Descargue el paquete de actualización y compruebe MD5. Consulte Descargar el paquete de actualización de NSX y comprobar MD5.

- 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.

Procedimiento

1. Inicie sesión en el dispositivo virtual NSX Manager.
2. En la página de inicio, 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. Vuelva a iniciar sesión en el dispositivo virtual de NSX Manager y desde la página de inicio haga clic en **Actualizar** (Upgrade). Confirme que el estado de la actualización sea **Completada** (Complete) y que la versión y el número de compilación de la parte superior derecha coincida con el paquete de actualizaciones que acaba de instalar.

Tras la actualización de NSX Manager, debe cerrar sesión y volver a iniciarla en vSphere Web Client.

Si el complemento de NSX no se muestra correctamente en vSphere Web Client, limpie la caché y el historial de su explorador. Si no se realiza este paso, es posible que aparezca un mensaje de error que indique que se produjo un error interno, como "An internal error has occurred - Error #1009", cuando se hacen cambios de configuración de NSX en vSphere Web Client.

Si la pestaña Redes y seguridad (Networking and Security) no aparece en vSphere Web Client, restablezca el servidor de vSphere Web Client.

- En vCenter 5.5, abra https://<vcenter-ip>:5480 y reinicie el servidor de vSphere Web Client.
- En vCenter Server Appliance 6.0, inicie sesión en el shell de vCenter Server como usuario 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 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. 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

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 los controladores durante un período de mantenimiento.

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

Si se implementan controladores nuevos antes de que se actualicen los existentes, se implementan en la versión anterior. Los nodos de controlador deben ser de la misma versión para poder unirse a un clúster.

NOTA: En la versión 6.3.3 de NSX cambia el sistema operativo subyacente de NSX Controller. Esto significa que cuando actualice a la versión 6.3.3 de NSX, en lugar de realizar una actualización de software, los controladores existentes se eliminarán uno a uno y los nuevos controladoras del sistema operativo Photon se implementarán con las mismas direcciones IP.

Prerequisitos

- Asegúrese de que todos los controladores estén en estado normal. La actualización no es posible si uno o varios controladores están en estado desconectado. Para reconectar un controlador desconectado, intente restablecer el dispositivo virtual del controlador. En la vista **Hosts y clústeres** (Hosts and Clusters), haga clic con el botón derecho en el controlador y seleccione **Alimentación > Restablecer** (Power > Reset).

- Un clúster de NSX Controller válido contiene tres nodos de controlador. Inicie sesión en los tres nodos de controlador y ejecute el comando **show control-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 controlador informe sobre el estado Unión completa (Join Complete).
  - En el estado Mayoría (Majority), compruebe que el controlador esté conectado a la mayoría del clúster.
  - En el identificador del clúster, todos los nodos de controlador de un clúster deben tener el mismo identificador de clúster.
  - En los estados Configurado (Configured) y Activo (Active), compruebe que todas las funciones del controlador 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.
- Si va a actualizar a la versión 6.3.3 de NSX, el clúster de NSX Controller debe tener tres nodos de controlador. Si tiene menos de tres, debe agregar nodos adicionales antes de iniciar la actualización. Consulte "Implementar clúster de NSX Controller" en la *Guía de instalación de NSX* si desea saber los pasos necesarios para agregar nodos de controlador.

Procedimiento

- 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 controlador** (Controller Cluster Status).

  Los controladores del entorno se actualizan y se reinician de uno a uno. Después de iniciar la actualización, el sistema descarga el archivo de actualización, actualiza y reinicia cada controlador, y actualiza el estado de actualización de cada controlador. Los siguientes campos muestran el estado del controlador:

  - La columna **Estado de clúster de controlador** (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 todos los controladores del clúster, el estado cambia a **En curso** (In progress). Una vez actualizados todos los controladores del clúster, el estado que aparece es **Finalizado** (Complete) y la columna ya no se muestra.
  - La columna **Estado** (Status) en la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de cada controlador, que es **Conectado** (Connected) o **Normal** (Normal) antes de la actualización, dependiendo de la versión NSX original. Cuando los servicios del controlador se apagan y se reinicia el controlador, el estado cambia a **Desconectado** (Disconnected). Una vez completada la actualización del controlador, el estado es **Conectado** (Connected).
  - La columna **Estado de actualización** (Upgrade Status) de la sección Nodos de NSX Controller (NSX Controller nodes) muestra el estado de actualización de cada controlador. 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 el controlador está actualizado, el estado indica **Actualizado** (Upgraded).

    NOTA: Al actualizar de NSX 6.3.2 o versiones anteriores a NSX 6.3.3 o versiones posteriores, el estado **Descargando archivo de actualización** (Downloading upgrade file) se reemplaza por **En cola para actualización** (Queued For Upgrade).

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 **6.3.***buildNumber* para cada controlador. Vuelva a ejecutar el comando **show control-cluster status** para garantizar que los controladores puedan crear una mayoría. Si no se vuelve a formar la mayoría del clúster de NSX Controller, revise los registros del controlador 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 del controlador tiene errores, revise la conectividad entre los controladores y NSX Manager.

Hay casos en los que el primer controlador se actualiza correctamente y el segundo no lo hace. Supongamos que el clúster tiene tres controladores: el primero se actualizó correctamente a la nueva versión y el segundo se está actualizando. Si la actualización del segundo controlador tiene errores, este controlador podría quedar en estado desconectado. Al mismo tiempo, el primer controlador y el tercero 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 otro controlador. El nuevo controlador tendrá la versión anterior (coincidente con el tercer controlador) y, por lo tanto, formará una mayoría con el tercer controlador. En este punto, se puede reiniciar el procedimiento de actualización. Consulte Reimplementar un NSX Controller en la *Guía para solucionar problemas de NSX* para obtener instrucciones sobre la creación de otro controlador.

Qué hacer a continuación

Actualizar los clúster del host en Cross-vCenter NSX.

Actualizar los clúster del host en Cross-vCenter NSX

Una vez actualizados todos los dispositivos NSX Manager y el clúster de NSX Controller, debe actualizar todos los clústeres de los hosts en el entorno cross-vCenter NSX.

Al actualizar los clústeres del host, se actualizan los VIB de NSX.

Si va a actualizar de NSX 6.2.x o versiones anteriores, o si está actualizando desde NSX 6.3.0 o versiones posteriores con ESXi 5.5, los hosts se deben reiniciar para completar la actualización.

- Si el clúster tiene DRS habilitado, cuando haga clic en **Resolver todo** (Resolve all), DRS intentará reiniciar los hosts de una forma controlada que permita que las máquinas virtuales continúen en ejecución. Las máquinas virtuales se desplazan a otros hosts en el clúster y los hosts deben entrar en modo de mantenimiento y reiniciarse.
- Si el clúster no tiene DRS habilitado, debe apagar vMotion o las máquinas virtuales manualmente antes de comenzar la actualización. Al hacer clic en **Resolver todo** (Resolve all), los hosts entran en el modo de mantenimiento y se reinician.

Si está actualizando desde NSX 6.3.0 o versiones posteriores con ESXi 6.0 o versiones posteriores, los hosts deben entrar en el modo de mantenimiento para completar la actualización. No es necesario reiniciar.

- Si el clúster tiene DRS habilitado, cuando haga clic en **Resolver todo** (Resolve all), DRS intentará que los hosts entren en modo de mantenimiento de una forma controlada que permita que las máquinas virtuales continúen en ejecución. Las máquinas virtuales se desplazan a otros hosts en el clúster y los hosts deben entrar en modo de mantenimiento.
- Si el clúster no tiene DRS habilitado, debe apagar vMotion o las máquinas virtuales manualmente antes de comenzar la actualización. Debe poner los hosts en modo de mantenimiento de forma manual para completar la actualización.

Prerequisitos

- 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.
- Asegúrese de 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.
  - 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 anticompatibilidad 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 anticompatibilidad durante la actualización y vuelva a habilitarlas una vez completada la actualización. Para deshabilitar una regla anticompatibilidad, desplácese hasta **Hosts y clústeres (Hosts and Clusters) > *Clúster (Cluster)* > Administrar (Manage) > Configuración (Settings) > Reglas de VM/Host (VM/Host Rules)**. Edite la regla y anule la selección de **Habilitar regla** (Enable rule).
- Inicie sesión en uno de los hosts del clúster y ejecute el comando `esxcli software vib list`.

Los VIB presentes dependen de las versiones de ESXi y NSX y, por tanto, pueden cambiar como parte de la actualización. Observe la versión actual de los VIB instalados:

Versión de ESXi	Versión de NSX	VIB instalados
5.5	6.1.x, 6.2.x o 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.2 o anterior	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.3 o posterior	■ esx-nsxv

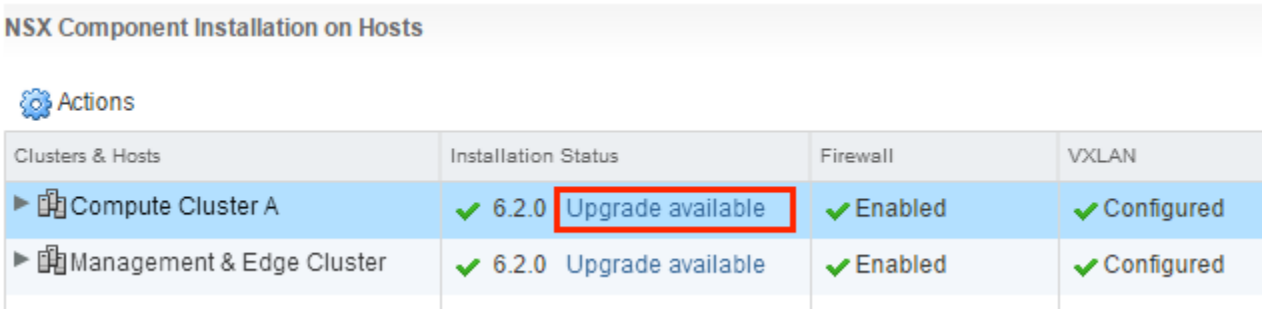
NOTA: Algunas versiones de NSX tienen VIB adicionales que se eliminarán durante la actualización.

- Si va a actualizar desde una versión anterior a NSX 6.2, los hosts preparados tienen un VIB adicional: esx-dvfilter-switch-security.
- Si va a actualizar desde NSX 6.2.x (donde la versión es NSX 6.2.4 o posterior), los hosts preparados tienen un VIB adicional: esx-vdpi.

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 opción Estado de instalación (Installation Status) muestra `Instalando` (Installing).

3 El clúster Estado de instalación (Installation Status) muestra `No está listo` (Not Ready). Haga clic en **No está listo** (Not Ready) para mostrar más información. Haga clic en **Resolver todo** (Resolve all) para intentar completar la instalación de los VIB.

Para completar la actualización, los hosts se deben poner en modo de mantenimiento y, si es necesario, se reiniciarán.

La columna Estado de instalación (Installation Status) muestra `Instalando` (Installing). Una vez completada la actualización, la columna Estado de instalación (Installation Status) muestra una marca de verificación de color verde y la versión NSX actualizada.

4 Si se produce un error en la acción **Resolver** (Resolve) cuando DRS está habilitado, es posible que los hosts requieran una intervención manual para entrar 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 **No está listo** (Not Ready) para mostrar más información. 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).

   La columna Estado de instalación (Installation Status) muestra `Instalando` (Installing). Una vez completada la actualización, la columna Estado de instalación (Installation Status) muestra una marca de verificación de color verde y la versión NSX actualizada.

5 Si se produce un error en la acción **Resolver** (Resolve) cuando DRS está deshabilitado y está actualizando desde NSX 6.3.0 o versiones posteriores con ESXi 6.0 o versiones posteriores, debe poner los hosts en modo de mantenimiento de forma manual para completar la actualización.

   a Ponga los hosts evacuados en modo de mantenimiento.

   b Desplácese a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)**.

      La actualización se inicia automáticamente cuando los hosts entran en modo de mantenimiento. La columna Estado de instalación (Installation Status) muestra `Instalando (Installing)`. Si no ve el estado `Instalando` (Installing), actualice la página.

      Una vez completada la actualización, la columna Estado de instalación (Installation Status) muestra una marca de verificación de color verde y la versión NSX actualizada.

   c Quite los hosts del modo de mantenimiento.

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

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.

Consulte el tema Preparación de host en la *Guía para solucionar problemas de NSX* para ver más pasos de solución de problemas.

Qué hacer a continuación

Actualizar NSX Edge en Cross-vCenter NSX

Actualizar NSX Edge en 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.

Actualizar todas las instancias de NSX Edge en todas las instalaciones de NSX en el entorno de cross-vCenter NSX.

Prerequisitos

- Compruebe que se haya actualizado NSX Manager.
- Compruebe que el clúster de NSX Controller y la preparación del host se hayan actualizado antes de actualizar los enrutadores lógicos.
- 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 los Requisitos del sistema para NSX si desea obtener información sobre los recursos necesarios para el tamaño de cada instancia de NSX Edge.
  - Para una instancia individual de NSX Edge, hay dos dispositivos de NSX Edge del tamaño en el estado encendido (poweredOn) durante la actualización.
  - Para una instancia de NSX Edge con alta disponibilidad, se implementan ambos dispositivos de sustitución antes de reemplazar los antiguos dispositivos. Esto significa que hay cuatro dispositivos NSX Edge del tamaño adecuado en el estado encendido (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.
- Compruebe que los clústeres de host enumerados en la ubicación configurada y la ubicación en vivo para el dispositivo NSX Edge estén preparados para NSX y que el estado de su infraestructura de mensajería sea de color `VERDE`. Si la ubicación configurada no está disponible, por ejemplo, debido a que se quitó el clúster al crearse el dispositivo NSX Edge, compruebe solo la ubicación en vivo.
  - Busque el ID de la ubicación configurada original (*configuredResourcePool* > *id*) y la ubicación en vivo actual (*resourcePoolId*) con la solicitud de la API `GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances`.

- Busque el estado de preparación del host y el estado de la infraestructura de mensajería para los clústeres con la solicitud de la API `GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}`, donde *resourceId* es el ID de la ubicación configurada y en vivo de los dispositivos de NSX Edge que se detectaron anteriormente.
  - Busque el estado correspondiente al *featureId* de `com.vmware.vshield.vsm.nwfabric.hostPrep` en el cuerpo de la respuesta. El estado debe ser de color `VERDE`.

    ```
    <nwFabricFeatureStatus>
      <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
      <featureVersion>6.3.1.5124716</featureVersion>
      <updateAvailable>false</updateAvailable>
      <status>GREEN</status>
      <installed>true</installed>
      <enabled>true</enabled>
      <allowConfiguration>false</allowConfiguration>
    </nwFabricFeatureStatus>
    ```

  - Busque el estado correspondiente al *featureId* de `com.vmware.vshield.vsm.messagingInfra` en el cuerpo de la respuesta. El estado debe ser de color `VERDE`.

    ```
    <nwFabricFeatureStatus>
      <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
      <updateAvailable>false</updateAvailable
      <status>GREEN</status>
      <installed>true</installed>
      <enabled>true</enabled>
      <allowConfiguration>false</allowConfiguration>
    </nwFabricFeatureStatus>
    ```

- 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 en la *Guía de actualización de NSX*.
- Si va a actualizar desde NSX 6.0.x y tiene una VPN de Capa 2 habilitada en una instancia de NSX Edge, debe borrar la configuración de esa conexión antes de realizar la actualización. Después de la actualización, puede volver a configurar la VPN de Capa 2. Consulte "Descripción general de VPN de Capa 2" en la *Guía de instalación de NSX*.

Procedimiento

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

2 Para cada instancia de NSX Edge, seleccione la opción **Actualizar versión** del 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

Tras actualizar NSX Edge 6.2.4 a la versión 6.2.5 u otras posteriores, debe desactivar la opción para iniciar la máquina virtual de vSphere en cada NSX Edge que se encuentre en un clúster en el que esté habilitado vSphere HA y en el que se hayan implementado Edges. Para hacerlo, abra vSphere Web Client y busque el host ESXi en la ubicación de la máquina virtual de NSX Edge. Haga clic en **Administrar (Manage) > Configuración (Settings)** y, en Máquinas virtuales (Virtual Machines), seleccione Encendido/Apagado de VM (VM Startup/Shutdown), haga clic en **Editar** (Edit) y asegúrese de que la máquina virtual esté en modo manual (es decir, asegúrese de que no se haya agregado a la lista de encendido/apagado automático).

Actualizar Guest Introspection en Cross-vCenter NSX

Actualizar Guest Introspection en Cross-vCenter NSX

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

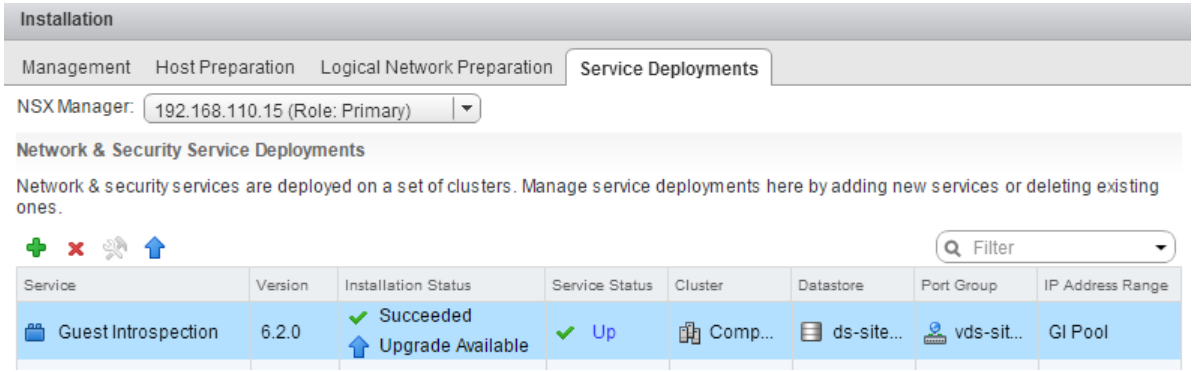
NOTA: Las máquinas virtuales de servicio de Guest Introspection se pueden actualizar desde vSphere Web Client. No es necesario eliminar la máquina virtual de servicio después de la actualización de NSX Manager para que se actualice. Si elimina la máquina virtual de servicio, el estado del servicio (Service 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

Actualizar NSX Manager, controladores, clústeres de hosts preparados e instancias de NSX Edge.

Procedimiento

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

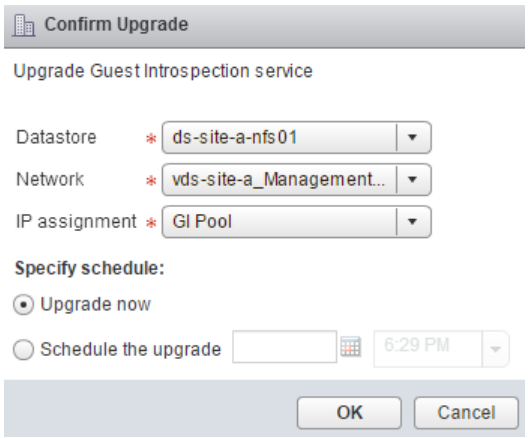


La columna **Estado de instalación** (Installation Status) indica **Actualización disponible** (Upgrade Available).

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

Algunos servicios NSX Services no admiten una actualización directa. En estos casos, debe desinstalar los servicios y volver a instalarlos.

Dispositivos virtuales de seguridad de VMware Partner

Compruebe la documentación de partners para comprobar si se puede actualizar el dispositivo virtual de seguridad para partners.

VPN SSL de NSX

A partir de NSX 6.2, la puerta de enlace de la VPN SSL solo acepta el protocolo TLS. Sin embargo, después de actualizar a NSX 6.2 o una versión posterior, todos los clientes nuevos que cree utilizarán automáticamente el protocolo TLS al establecer la conexión. Además, a partir de NSX 6.2.3, el protocolo TLS 1.0 está obsoleto.

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

Después de la actualización desde NSX 6.0.x, desinstale los clientes de VPN SSL anteriores e instale la versión 6.3.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

No se admite la actualización de NSX Edge si dispone de una VPN de Capa 2 instalado en una instancia de NSX Edge con NSX 6.0.x instalado. La configuración de una VPN de Capa 2 se debe eliminar para poder actualizar NSX Edge.

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

1. Realice una copia de seguridad actualizada tras la actualización.
2. 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
```

3 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 vSphere en un entorno NSX

2

Si necesita actualizar NSX y vSphere, VMware recomienda completar primero la actualización de NSX y, a continuación, la de vSphere.

Compruebe la matriz de interoperabilidad de productos de VMware para verificar qué versiones de vSphere y ESXi son compatibles con su instalación de NSX. Consulte http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Consulte la versión adecuada de la documentación de vSphere para obtener instrucciones detalladas sobre cómo actualizar vSphere, entre las que se incluyen la *Guía de actualización de vSphere* y la *Guía sobre cómo instalar y administrar VMware vSphere Update Manager*.

Cuando se actualiza ESXi en un host, también debe instalar nuevos VIB de NSX en el host para que sea compatible con la nueva versión de ESXi. Las cargas de trabajo de NSX no se pueden ejecutar en el host actualizado hasta que se actualicen los VIB de NSX.

El procedimiento para actualizar ESXi cuando NSX 6.3.x esté instalado varía según la versión de ESXi a la que esté actualizando o desde la que realice la actualización.

Tabla 2-1. Procedimiento de actualización de ESXi cuando NSX 6.3.x esté instalado

Tipo de actualización del host	Requisitos del modo de mantenimiento del host	Requisitos de reinicio del host
ESXi 5.5 a ESXi 6.0. Consulte Actualizar a ESXi 6.0 en un entorno de NSX.	El host debe permanecer en el modo de mantenimiento hasta que la actualización de ESXi y la posterior actualización de los VIB de NSX se hayan completado.	Es necesario realizar un reinicio durante la actualización de ESXi. Durante la posterior actualización de los VIB de NSX, es necesario llevar a cabo un reinicio.
De ESXi 5.5 a ESXi 6.5. Consulte Actualizar a ESXi 6.5 en un entorno de NSX.	El host puede salir del modo de mantenimiento después de realizar la actualización de ESXi. Se bloqueará vMotion de las máquinas virtuales para los conmutadores distribuidos de vSphere preparados de VXLAN en el host actualizado hasta que la posterior actualización de los VIB de NSX se haya completado.	Es necesario realizar un reinicio durante la actualización de ESXi. Durante la posterior actualización de los VIB de NSX, es necesario llevar a cabo un reinicio.
ESXi 6.0 a ESXi 6.5 Consulte Actualizar a ESXi 6.5 en un entorno de NSX.	El host puede salir del modo de mantenimiento después de realizar la actualización de ESXi. Se bloqueará vMotion de las máquinas virtuales para los conmutadores distribuidos de vSphere preparados de VXLAN en el host actualizado hasta que la posterior actualización de los VIB de NSX se haya completado.	Es necesario realizar un reinicio durante la actualización de ESXi. Durante la posterior actualización de los VIB de NSX, no es necesario realizar un reinicio.

Este capítulo cubre los siguientes temas:

- Actualizar a ESXi 6.0 en un entorno de NSX
- Actualizar a ESXi 6.5 en un entorno de NSX
- Volver a implementar Guest Introspection tras la actualización de ESXi

Actualizar a ESXi 6.0 en un entorno de NSX

Los VIB de NSX son específicos para la versión de ESXi que está instalada en el host. Si actualiza el ESXi, debe instalar los nuevos VIB de NSX adecuados para la nueva versión de ESXi.

Los VIB de NSX instalados dependen de las versiones de ESXi y NSX. Si tiene instalada la versión NSX 6.3.3 o posterior y actualiza de ESXi 5.5 a 6.0, los VIB esx-vsip y esx-vxlan se eliminarán y serán reemplazados por el VIB esx-nsxv.

Versión de ESXi	Versión de NSX	VIB instalados
5.5	Cualquier versión 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.2 o anterior	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.3 o posterior	■ esx-nsxv

IMPORTANTE: Debe asegurarse de que el host siga en modo de mantenimiento durante todo el proceso de actualización para evitar que DRS o vMotion muevan las VM al host antes de que se complete la actualización.

Prerequisitos

- Compruebe la matriz de interoperabilidad de productos de VMware para verificar qué versiones de vSphere y ESXi son compatibles con su instalación de NSX. Consulte http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Consulte la versión adecuada de la documentación de vSphere para obtener instrucciones detalladas sobre cómo actualizar vSphere, entre las que se incluyen la *Guía de actualización de vSphere* y la *Guía sobre cómo instalar y administrar VMware vSphere Update Manager*.
- Verifique que los sistemas de Platform Services Controller y vCenter Server estén actualizados a la nueva versión de vSphere.
- Asegúrese de 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.
  - 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 anticompatibilidad 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 anticompatibilidad durante la actualización y vuelva a

habilitarlas una vez completada la actualización. Para deshabilitar una regla anticompatibilidad, desplácese hasta **Hosts y clústeres (Hosts and Clusters) > *Clúster (Cluster)* > Administrar (Manage) > Configuración (Settings) > Reglas de VM/Host (VM/Host Rules)**. Edite la regla y anule la selección de **Habilitar regla** (Enable rule).

Procedimiento

- Por cada host que deba actualizar, complete los siguientes pasos.
  a. Ponga el host en modo de mantenimiento.

     Si el clúster tiene DRS habilitado, DRS intentará mover las VM a otros hosts. Si DRS falla por alguna razón, puede que necesite mover las VM manualmente y, a continuación, poner el host en modo de mantenimiento.

  b. Actualice ESXi en el host.

     Reinicie el host una vez que se haya completado la actualización de ESXi.

  c. Si el host tiene el estado `No conectado` (Not connected) después del reinicio, conecte el host. Haga clic con el botón secundario del mouse en el host y seleccione **Conexión (Connection) > Conectar (Connect)**.

  d. Desplácese a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)**.

  e. Seleccione el host en el que desea ubicar la versión actualizada de ESXi. El estado de instalación muestra **No está listo** (Not Ready).

  f. Haga clic en **Acciones (Actions) > Resolver (Resolve)** para completar la actualización de los VIB de NSX.

     Los VIB de NSX se actualizan en el host y el host se reiniciará.

  g. Una vez que el host haya completado el reinicio, salga del modo de mantenimiento.

Para verificar que los VIB estén actualizados, ejecute el comando `esxcli software vib list` en la línea de comandos del host. La primera parte de la versión del VIB muestra la versión de ESXi para el VIB.

Por ejemplo, tras actualizar a ESXi 6.0 con la versión 6.3.2 de NSX o versiones anteriores:

```
[root@host-1:~] esxcli software vib list
...
esx-vsip    6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
...
```

Tras actualizar a ESXi 6.0 con la versión 6.3.3 de NSX o versiones posteriores:

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv    6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-08-10
...
```

Actualizar a ESXi 6.5 en un entorno de NSX

Los VIB de NSX son específicos para la versión de ESXi que está instalada en el host. Si actualiza el ESXi, debe instalar los nuevos VIB de NSX adecuados para la nueva versión de ESXi.

Cuando actualice a ESXi 6.5 con NSX 6.3.x instalado, se bloqueará vMotion de las máquinas virtuales para los conmutadores distribuidos de vSphere preparados de VXLAN en el host actualizado hasta que los nuevos VIB de NSX se hayan instalado.

VMware recomienda el uso de vSphere Upgrade Manager para actualizar los hosts ESXi 6.5 en un entorno de NSX 6.3.x.

Independientemente del método que use para actualizar ESXi, debe seguir este flujo de trabajo. En un host cada vez, realice las siguientes acciones:

1 Actualizar ESXi

   Una vez que se haya completado la actualización de ESXi, el host saldrá del modo de mantenimiento. No obstante, no podrá mover al host las máquinas virtuales conectadas a los conmutadores lógicos hasta que se haya completado el siguiente paso.

2 Actualizar los VIB de NSX

   Una vez que los VIB se hayan actualizado y el host haya salido del modo de mantenimiento, puede mover al host las máquinas virtuales conectadas a los conmutadores lógicos.

IMPORTANTE: Debe actualizar un solo host a la vez. Cuando actualice a ESXi, no debe seleccionar un clúster o un centro de datos para corregirlo.

Los VIB de NSX instalados dependen de las versiones de ESXi y NSX. Si tiene instalada la versión NSX 6.3.3 o posterior y actualiza de ESXi 5.5 a 6.5, los VIB esx-vsip y esx-vxlan se eliminarán y serán reemplazados por el VIB esx-nsxv.

Versión de ESXi	Versión de NSX	VIB instalados
5.5	Cualquier versión 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.2 o anterior	■ esx-vsip ■ esx-vxlan
6.0 o posterior	6.3.3 o posterior	■ esx-nsxv

Prerequisitos

- Compruebe que NSX 6.3 esté instalado.
- Compruebe la matriz de interoperabilidad de productos de VMware para verificar qué versiones de vSphere y ESXi son compatibles con su instalación de NSX. Consulte http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

  IMPORTANTE: NSX 6.3.x no es interoperable con la versión inicial de ESXi 6.5. Debe actualizar a ESXi 6.5.0a o una versión posterior para que sea compatible con NSX 6.3.0. Compruebe la matriz de interoperabilidad para obtener la última información de interoperabilidad.

- Consulte la versión adecuada de la documentación de vSphere para obtener instrucciones detalladas sobre cómo actualizar vSphere, entre las que se incluyen la *Guía de actualización de vSphere* y la *Guía sobre cómo instalar y administrar VMware vSphere Update Manager*.
- Verifique que los sistemas de Platform Services Controller y vCenter Server estén actualizados a la nueva versión de vSphere.
- Verifique que vSphere Update Manager esté instalado y configurado.
- Asegúrese de 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.
  - 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 anticompatibilidad 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 anticompatibilidad durante la actualización y vuelva a habilitarlas una vez completada la actualización. Para deshabilitar una regla anticompatibilidad, desplácese hasta **Hosts y clústeres (Hosts and Clusters) > *Clúster (Cluster)* > Administrar (Manage) > Configuración (Settings) > Reglas de VM/Host (VM/Host Rules)**. Edite la regla y anule la selección de **Habilitar regla** (Enable rule).

Procedimiento

1 En vSphere Web Client, diríjase a **Update Manager >** ***Objeto de Update Manager (Update Manager Object)*** **> Administrar (Manage)**.

2 Siga las instrucciones sobre *cómo importar las imágenes de actualización del host y cómo crear líneas de base de actualización del host* para proceder a realizar estas acciones.

   a Haga clic en la pestaña **Imágenes de ESXi** (ESXi Images), en **Importar imagen de ESXi** (Import ESXi Image) y desplácese hasta la imagen que desee cargar.

   b En la pestaña **Líneas base de host** (Host Baselines), haga clic en **Nueva línea base** (New Baseline). Use el asistente Nueva línea de base (New Baseline) para crear una nueva línea de base. Para ello, debe seleccionar **Actualización de host** (Host Upgrade) como tipo de línea de base.

3 Actualice un solo host a la vez. Repita estos pasos para cada uno de los hosts.

   a Desplácede hasta **Hosts y clústeres** (Hosts and Clusters) y seleccione el host que desea actualizar. No seleccione un clúster ni un centro de datos.

   b Haga clic con el botón secundario en el host y seleccione **Update Manager (Update Manager) > Adjuntar línea de base (Attach Baseline...)**. Use el asistente Adjuntar línea de base (Attach Baseline) o Grupo de líneas de base (Baseline Group) para seleccionar una línea de base. Consulte información sobre *cómo adjuntar líneas de base y grupos de líneas de base a objetos* en la documentación de vSphere para encontrar instrucciones completas.

   c Haga clic con el botón secundario en el host y seleccione **Update Manager (Update Manager) > Corregir (Remediate...)**. Use el asistente Corregir (Remediate) para seleccionar una línea de base. Consulte información sobre cómo *corregir hosts en una línea de base de actualización* en la documentación de vSphere para encontrar instrucciones completas.

   d Si el host tiene el estado `No conectado` (Not connected) después del reinicio, conecte el host. Haga clic con el botón secundario del mouse en el host y seleccione **Conexión (Connection) > Conectar (Connect)**.

   e Para verificar si la actualización se completó, haga clic con el botón secundario en el host y seleccione **Update Manager (Update Manager) > Analizar para buscar actualizaciones (Scan for Updates...)**. Seleccione la casilla de verificación **Actualizaciones** (Upgrades) para que se puedan buscar actualizaciones. Si el estado de cumplimiento es Compatible (Compliant), la actualización se habrá completado.

      Consulte información sobre *cómo iniciar manualmente un análisis de hosts de ESXi* en la documentación de vSphere para encontrar instrucciones completas.

   f Desplácese a **Redes y seguridad (Networking & Security) > Instalación (Installation) > Preparación del host (Host Preparation)**.

g Localice el host en el que actualizó el ESXi. El estado de instalación muestra **No está listo** (Not Ready).

Haga clic en **No está listo** (Not Ready) para obtener más información.

h Seleccione el host y haga clic en **Acciones (Actions) > Resolver (Resolve)** para activar la instalación de los VIB de NSX.

Si va a actualizar desde ESXi 5.5 y el clúster tiene DRS habilitado, el DRS intenta reiniciar el host de manera controlada para que las máquinas virtuales continúen en ejecución. Si se produce un error en el DRS por cualquier motivo, se detiene la acción **Resolver** (Resolve). En este caso, es posible que deba mover las máquinas virtuales manualmente y, a continuación, volver a intentar la acción **Resolver** (Resolve) o poner el host en el modo de mantenimiento y reiniciarlo de forma manual.

Si va a actualizar desde ESXi 6.0 y el clúster tiene DRS habilitado, el DRS intentará poner el host en el modo de mantenimiento de manera controlada para que las máquinas virtuales continúen en ejecución. Si se produce un error en el DRS por cualquier motivo, se detiene la acción **Resolver** (Resolve). En este caso, es posible que deba mover las máquinas virtuales manualmente y, a continuación, volver a intentar la acción **Resolver** (Resolve) o poner el host en el modo de mantenimiento de forma manual.

IMPORTANTE: Si va a actualizar desde ESXi 6.0 y pone un host en modo de mantenimiento de forma manual para instalar los VIB del host, debe comprobar que la instalación de los VIB del host se ha completado antes de que el host salga del modo de mantenimiento. La opción **Preparación del host** (Host Preparation) mostrará el estado de instalación en `Instalando` (Installing) aunque se haya completado la instalación.

1 Compruebe el panel Tareas recientes (Recent Tasks) en vSphere Web Client y verifique que todas las tareas de instalación se hayan completado.

2 Conéctese a la línea de comandos del host y ejecute el comando `esxcli software vib list`. La primera parte de la versión del VIB muestra la versión de ESXi para el VIB.

Por ejemplo, tras actualizar a ESXi 6.5 con la versión 6.3.2 de NSX o versiones anteriores:

```
[root@host-1:~] esxcli software vib list
...
esx-vsip    6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
...
```

Tras actualizar a ESXi 6.5 con la versión 6.3.3 de NSX o versiones posteriores:

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv    6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-08-10
...
```

Volver a implementar Guest Introspection tras la actualización de ESXi

Si actualiza ESXi en un clúster donde se implementa Guest Introspection, debe comprobar la pestaña Implementaciones de servicios (Service Deployments) para ver si Guest Introspection se debe volver a implementar.

IMPORTANTE: Debe completar la actualización de ESXi y la actualización de los VIB de NSX asociados antes de volver a implementar Guest Introspection.

Prerequisitos

- Complete la actualización de ESXi.
- Complete la actualización de los VIB de NSX (Preparación de host) después de la actualización de ESXi.

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 **Implementaciones de servicios** (Service Deployments).
4. Si la columna Estado de instalación (Installation Status) muestra `Correcto` (Succeeded), no se requiere una nueva implementación.
5. Si la columna Estado de instalación (Installation Status) muestra No está listo (Not Ready), haga clic en el vínculo **No está listo** (Not Ready). Haga clic en **Resolver todo** (Resolve all) para volver a implementar Guest Introspection.