Guía de actualización de NSX para vShield Endpoint

VMware NSX for vSphere 6.2

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

ES-002164-04

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Contenido

Guía de actualización de NSX para vShield Endpoint 1

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

Público objetivo

Este manual está dirigido a quienes utilicen vCloud Networking and Security solamente para la función de Endpoint, y se actualiza a NSX para implementar y administrar vShield Endpoint solo para la capacidad de descarga antivirus. La información de este manual está escrita para administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y con operaciones de centros de datos. Este manual da por sentado que el usuario está familiarizado con VMware vSphere 5.5 o 6.0, incluidos VMware ESXi, vCenter Server y vSphere Web Client.

Si necesita utilizar otras funciones de NSX (por ejemplo, conmutadores y enrutadores lógicos, Distributed Firewall o NSX Edge) consulte la *Guía de actualización de NSX*.

Glosario de publicaciones técnicas de VMware

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

Este capítulo cubre los siguientes temas:

Leer los documentos complementarios

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

Notas de la versión

Antes de comenzar la actualización a NSX 6.2.X, revise las notas de la versión. En ellas se documentan problemas de actualización conocidos y las soluciones correspondientes. Conocer los problemas de actualización antes de comenzar el proceso puede ahorrarle tiempo y esfuerzo. Consulte https://www.vmware.com/support/pubs/nsx_pubs.html.

Matriz de interoperabilidad de productos

Compruebe la interoperabilidad con otros productos de VMware, como vCenter. Consulte la matriz de interoperabilidad de productos (Product Interoperability Matrix) de VMware en la pestaña **Interoperabilidad** (Interoperability) de la página http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Compruebe la compatibilidad de la ruta de acceso de actualización de su versión actual de NSX a la versión a la cual desea actualizar. En la pestaña **Ruta de acceso de actualización** (Upgrade Path), seleccione **VMware NSX** en el menú de productos.

Guía de compatibilidad

Compruebe la compatibilidad de las soluciones de los partners con NSX en la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Secuencia de actualización para productos VMware

Al actualizar otros productos de VMware junto con la actualización de NSX como por ejemplo, vCenter y ESXi, es importante seguir la secuencia de actualización correcta que se documenta en el ejemplo 5 de http://kb.vmware.com/kb/2109760.

Requisitos del sistema para NSX vShield Endpoint

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

Hardware

Tabla 1-1. Requisitos de hardware

Dispositivo	Memoria	vCPU	Espacio en disco
NSX Manager	16 GB (24 GB con ciertos tamaños de implementación de NSX*)	4 GB (8 GB con ciertos tamaños de implementación de NSX*)	60 GB
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 el aumento de la memoria y la asignación de vCPU para los dispositivos virtuales, consulte las páginas de documentación de vSphere siguientes (o las páginas equivalentes para su versión de vSphere):

- vSphere 5.5:
  - Memoria---https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-49D7217C-DB6C-41A6-86B3-7AFEB8BF575F.html
  - vCPU---https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-76FC7E9F-8037-4C8E-BEB9-91C266C1EA9A.html
- vSphere 6.0:
  - Memoria---https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-49D7217C-DB6C-41A6-86B3-7AFEB8BF575F.html
  - vCPU---https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-76FC7E9F-8037-4C8E-BEB9-91C266C1EA9A.html

Software

Estas son las versiones recomendadas de los productos de VMware.

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

Acceso de clientes y usuarios

- Si agregó hosts ESXi por nombre al inventario de vSphere, compruebe que la resolución de nombres directa o inversa está funcionando. De lo contrario, NSX Manager no puede resolver las direcciones IP.
- Permisos para agregar y encender máquinas virtuales.
- Acceda al almacén de datos en el que almacena archivos de máquina virtual y a los permisos de cuenta para copiar los archivos en ese almacén de datos.
- Cookies habilitadas en el explorador web, para acceder a la interfaz de usuario de NSX Manager.
- En NSX Manager, compruebe que se puede acceder al puerto 443 desde el host ESXi, el servidor vCenter Server y los dispositivos NSX que se implementarán. Este puerto debe descargar el archivo OVF en el host ESXi para la implementación.
- Un navegador web que sea compatible con la versión de vSphere Web Client que está utilizando. Para obtener más información, consulte la documentación sobre la *administración de vCenter Server y hosts*:
  - vSphere 5.5: https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html
  - vSphere 6.0: https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-A618EF76-638A-49DA-991D-B93C5AC0E2B1.html

Puertos y protocolos requeridos por NSX

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

Tabla 1-2. Puertos y protocolos requeridos por NSX

Origen	Destino	Puerto	Protocolo	Propósito	Sensible	TLS	Autenticación
PC cliente	NSX Manager	443	TCP	Interfaz administrativa de NSX Manager	No	Sí	Autenticación PAM
PC cliente	NSX Manager	80	TCP	Acceso a VIB de NSX Manager	No	No	Autenticación PAM
Host ESXi	vCenter Server	80	TCP	Preparación del host ESXi	No	No	
vCenter Server	Host ESXi	80	TCP	Preparación del host ESXi	No	No	
Host ESXi	NSX Manager	5671	TCP	RabbitMQ	No	Sí	Usuario/contraseña de Rabbit MQ
Host ESXi	NSX Controller	1234	TCP	Conexión del agente del ámbito del usuario	No	Sí	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Clúster de controladoras, sincronización de estado	No	Sí	IPsec
NSX Controller	NSX Controller	7777	TCP	Puerto RPC entre controladoras	No	Sí	IPsec
NSX Controller	NSX Controller	30865	TCP	Clúster de controladoras, sincronización de estado	No	Sí	IPsec
NSX Controller	Servidor horario NTP	123	TCP	Conexión de cliente NTP	No	Sí	Sin autenticación
NSX Manager	NSX Controller	443	TCP	Comunicación de controladora a Manager	No	Sí	Usuario/contraseña
NSX Manager	vCenter Server	443	TCP	vSphere Web Access TCP	No	Sí	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	No	Sí	
NSX Manager	Host ESXi	443	TCP	Conexión de aprovisionamiento y administración	No	Sí	
NSX Manager	Host ESXi	902	TCP	Conexión de aprovisionamiento y administración	No	Sí	
NSX Manager	Servidor DNS	53	TCP	Conexión de cliente DNS	No	No	
NSX Manager	Servidor syslog	514	TCP	Conexión de Syslog	No	Sí	
NSX Manager	Servidor horario NTP	123	TCP	Conexión de cliente NTP	No	Sí	
vCenter Server	NSX Manager	80	TCP	Preparación del host TCP	No	Sí	

Tabla 1-2. Puertos y protocolos requeridos por NSX (Continua)

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

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

Actualización de vCloud Networking and Security a NSX 2

Este capítulo cubre los siguientes temas:

Preparar la actualización de vCloud Networking and Security a NSX para vShield Endpoint

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

ADVERTENCIA: Las versiones anteriores no son compatibles:

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

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

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

1. Compruebe que la versión de vCloud Networking and Security es la 5.5. Si no es así, consulte la *Guía de instalación y actualización de vShield* (vShield Installation and Upgrade Guide) versión 5.5 para obtener instrucciones sobre cómo realizar la actualización.
2. Compruebe que todos los puertos necesarios están abiertos. Consulte "Puertos y protocolos requeridos por NSX," página 7.
3. Compruebe que vCenter cumple los requisitos del sistema de NSX 6.2.x. Consulte "Requisitos del sistema para NSX vShield Endpoint," página 6.
4. Compruebe que puede recuperar la información del nombre de puerto del enlace de subida de los conmutadores distribuidos de vSphere. Consulte https://kb.vmware.com/kb/2129200.
5. Si se implementa un servicio de partners de vShield Endpoint, compruebe la compatibilidad antes de la actualización:
   - Consulte la Guía de compatibilidad de VMware para Networking and Security. Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

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

6 Si tiene Data Security instalado en el entorno, desinstálelo antes de actualizar vShield Manager. Consulte "Desinstalar vShield Data Security," página 15.

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

8 Compruebe que cuenta con una copia de seguridad actualizada de Manager, vCenter y otros componentes de vCloud Networking and Security. Consulte "Copia de seguridad y restauración de vCloud Networking and Security," página 16.

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

10 Cree un paquete de servicio técnico.

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

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

13 Descargue y organice el paquete de actualización, y valídelo con md5sum. Consulte "Descargar el paquete para actualizar vShield Manager a NSX y comprobar MD5," página 18.

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

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

Impactos operativos de las actualizaciones de vShield Endpoint

El proceso de actualización de vCloud Networking and Security puede tardar algún tiempo. Es importante comprender el estado operativo de los componente de vCloud Networking and Security durante una actualización.

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

- vShield Manager
- vShield Endpoint

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

Actualización de vCenter

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

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

Actualización de vShield Manager

Durante:

- La configuración de vShield Manager se bloquea. El servicio vShield API no está disponible. No pueden realizarse cambios en la configuración de vShield. La comunicación con las máquinas virtuales existentes sigue funcionando.

Después:

- Se permiten todos los cambios de configuración de NSX y vShield.

vShield Endpoint cambia a Guest Introspection

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

Durante:

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

Después:

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

Comprobar el estado de funcionamiento de vShield Endpoint

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

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

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

Procedimiento

1. Identifique las contraseñas y los identificadores de usuario administrador.
2. Compruebe que la resolución de nombres directa e inversa funciona en todos los componentes.
3. Compruebe que puede iniciar sesión en todos los componentes de vSphere y vShield.
4. Tenga en cuenta las versiones actuales de vShield Manager, vCenter Server y ESXi.
5. Inspeccione visualmente el entorno de vShield para asegurarse de que todos los indicadores de estado estén en color verde, muestren una condición normal y estén implementados.
6. Compruebe que Syslog esté configurado.
7. Compruebe que las soluciones de los partners están en funcionamiento.

   Por ejemplo, puede usar el archivo de prueba antivirus EICAR (EICAR Standard Anti-Virus Test File) para probar la función antivirus: http://www.eicar.org/86-0-Intended-use.html
8. (Opcional) Si cuenta con un entorno de prueba, pruebe que funcionen las opciones de actualización y posteriores a la actualización antes de actualizar el entorno de un producto.

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

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

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

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

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

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

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

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

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

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

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

  Por ejemplo, si se utiliza curl:

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

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

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

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

  - Agregue un nuevo usuario tempadmin con el rol super_user.

    Por ejemplo, si se utiliza curl:

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

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

    Por ejemplo, si se utiliza curl:

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

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

    Por ejemplo, si se utiliza curl:

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

Desinstalar vShield Data Security

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

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

Procedimiento

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

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

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

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

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

Copia de seguridad y restauración de vCloud Networking and Security

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

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

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

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

Recomendamos realizar copias de seguridad en las siguientes situaciones:

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

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

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

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

Procedimiento

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Hacer copias de seguridad de conmutadores distribuidos de vSphere

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

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

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

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

Hacer una copia de seguridad de vCenter

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

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

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

Vínculos útiles para vCenter 5.5:

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

Vínculos útiles para vCenter 6.0:

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

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

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

Prerequisitos

Una herramienta de suma de comprobación de MD5.

Procedimiento

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

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

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

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

Cámbielo a:

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

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

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

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

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

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

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

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

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

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

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

1 vShield Manager a NSX Manager

2 vShield Endpoint a NSX Guest Instrospection

Actualizar vShield Manager a NSX Manager para vShield Endpoint

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

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

Prerequisitos

- Compruebe que realizó todas las tareas de preparación para la actualización que se describen en "Preparar la actualización de vCloud Networking and Security a NSX para vShield Endpoint," página 11.
- Compruebe que vShield Manager disponga de suficiente espacio en disco para realizar la actualización a NSX Manager. Consulte "Requisitos del sistema para NSX vShield Endpoint," página 6.
- Aumente la memoria reservada del dispositivo virtual de vShield Manager como mínimo a 16 GB y asigne 4 vCPU antes de realizar la actualización a NSX 6.2.x.

  Consulte "Requisitos del sistema para NSX vShield Endpoint," página 6.

Procedimiento

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

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

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

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

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

  La subida puede tardar unos minutos.

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

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

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

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

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

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

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

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

Contraseñas de vCloud Networking and Security

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

Contraseñas tas la actualización de NSX

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

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

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

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

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

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

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

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

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

Qué hacer a continuación

Crear una copia de seguridad de NSX Manager. La copia de seguridad anterior de NSX Manager solo es válida para la versión anterior. Consulte "Hacer copias de seguridad de la información de NSX Manager para vShield Endpoint," página 21.

Hacer copias de seguridad de la información de NSX Manager para vShield Endpoint

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

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

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

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

Procedimiento

1 Inicie sesión en el dispositivo virtual de NSX Manager.

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

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

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

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

   c Si es necesario, edite el puerto predeterminado.

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

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

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

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

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

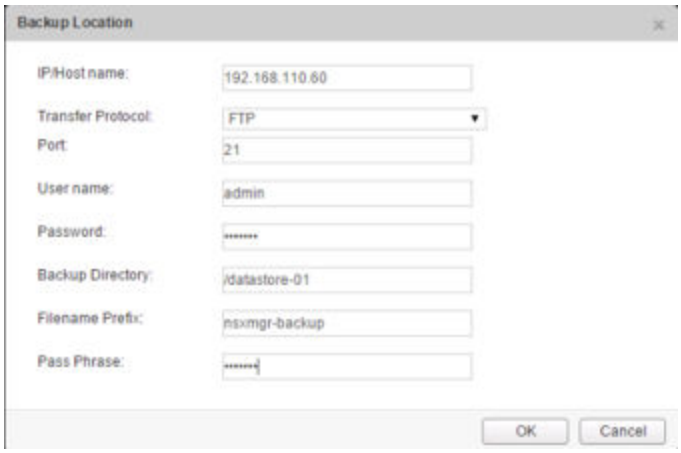
Este texto se agrega antes del nombre de archivo de cada copia de seguridad para que el sistema de copia de seguridad lo reconozca fácilmente. Por ejemplo, si escribe **ppdb**, la copia de seguridad resultante se denominará `ppdbHH_MM_SS_DayDDMonYYYY`.

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

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

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

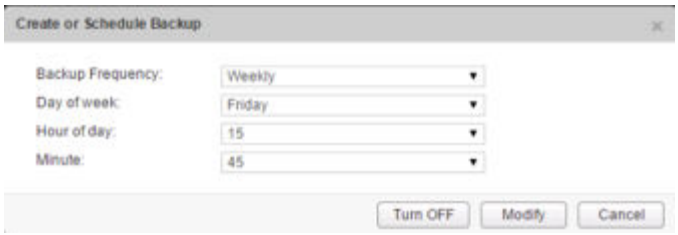
Por ejemplo:



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

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

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



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

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

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

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

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

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

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

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

Qué hacer a continuación

Actualizar vShield Endpoint Consulte "Actualizar a Guest Introspection en NSX para vShield Endpoint," página 23.

Actualizar a Guest Introspection en NSX para vShield Endpoint

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

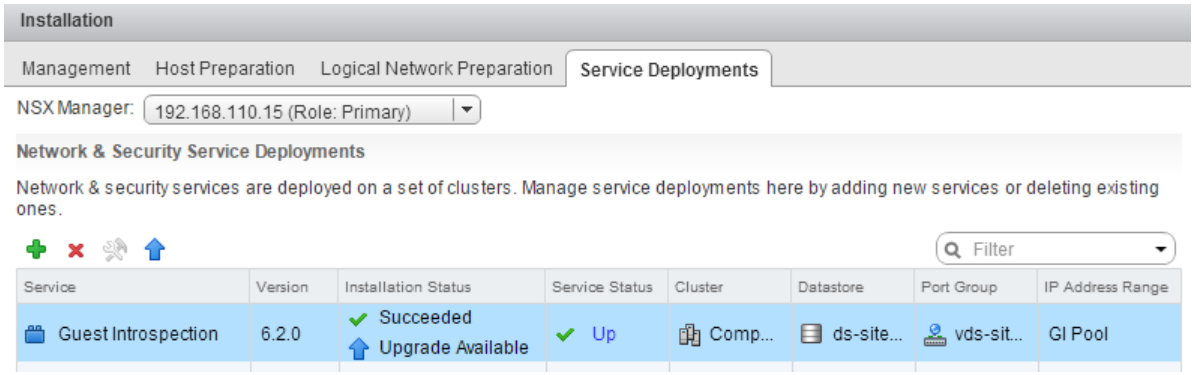
NOTA: Las máquinas virtuales de servicio de Guest Introspection se pueden actualizar desde vSphere Web Client. No es necesario eliminar la máquina virtual de servicio después de la actualización de NSX Manager para que se actualice. Si elimina la máquina virtual de servicio, el estado del servicio (Service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

Compruebe que NSX Manager se actualizó a 6.2.x.

Procedimiento

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

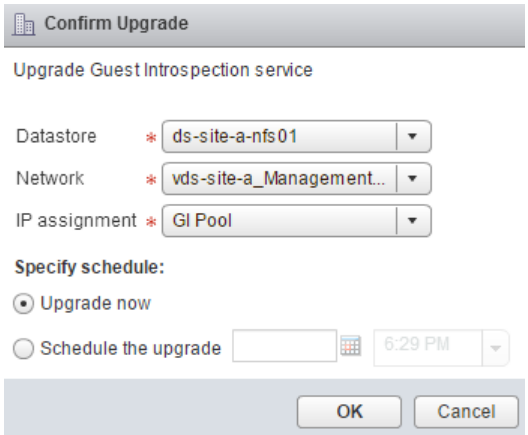


La columna **Estado de instalación** (Installation Status) indica **Actualización disponible** (Upgrade Available).

2 Seleccione la implementación de Guest Introspection que desea actualizar.

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

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



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

Qué hacer a continuación

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

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

Lista de comprobación tras la actualización

Cuando la actualización finalice, siga estos pasos.

Procedimiento

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

2 Realice una copia de seguridad actualizada tras la actualización.

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

NSX Instala los siguientes VIB:

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

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

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

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

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

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

Utilizar los servicios de partners en NSX para vShield Endpoint 3

Guest Introspection le permite usar los servicios de partners en su implementación de NSX.

Este capítulo cubre los siguientes temas:

Actualizar el servicio de partners en NSX para vShield Endpoint

Una vez que actualice de vCloud Networking and Security a NSX, es posible que necesite actualizar el servicio de partners.

Prerequisitos

Consulte la documentación del servicio de partners para obtener más detalles sobre compatibilidad y actualización.

Procedimiento

1 Actualice la solución de administración de partner.

2 Registre el servicio de partners con NSX Manager en la consola del proveedor.

Si necesita instrucciones, consulte la documentación del servicio de partners.

3 Apague y elimine las máquinas virtuales de los servicio de partners antiguos.

Qué hacer a continuación

"Implementar un servicio de partner," página 27

Implementar un servicio de partner

Si la solución del partner incluye un dispositivo virtual host-residente, podrá implementar el servicio una vez que la solución esté registrada en NSX Manager.

Prerequisitos

Asegúrese de que:

- La solución del partner se registra en NSX Manager.
- NSX Manager puede acceder a la consola de administración de la solución del partner.

Procedimiento

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

2 Haga clic en la pestaña **Implementaciones de servicios** (Service Deployments) y haga clic en el icono **Nueva implementación de servicios** (New Service Deployments) ( ).

3 En el cuadro de diálogo Implementar servicios de red y seguridad (Deploy Network and Security Services), seleccione las soluciones adecuadas.

4 En **Especificar programación** (Specify schedule) (en la parte inferior del cuadro de diálogo), seleccione **Implementar ahora** (Deploy now) para implementar la solución inmediatamente o seleccionar una fecha y una hora de implementación.

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

6 Seleccione el centro de datos y los clústeres en los que desea implementar la solución y haga clic en **Siguiente** (Next).

7 Seleccione el almacén de datos en el que desea agregar el almacenamiento de máquinas virtuales del servicio de soluciones o bien seleccione **Especificado en el host** (Specified on host).

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

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

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

Si la red está establecida en **Especificado en el host** (Specified on host), la red que se utilizará debe especificarse en la propiedad **Configuración de máquina virtual agente > Red** (Agent VM Settings > Network) de cada host del clúster. Consulte la *documentación de vSphere API/SDK*.

Debe establecer la propiedad de la red de la máquina virtual de agente en un host antes de agregarlo a un clúster. Acceda a **Administrar > Configuración > Configuración de máquina virtual agente > Red** (Manage > Settings > Agent VM Settings > Network) y haga clic en **Editar** (Edit) para establecer la red de la máquina virtual de agente.

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

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

Seleccionar	Para
DHCP	Asigne una dirección IP a la máquina virtual de servicios a través del protocolo Dynamic Host Configuration Protocol (DHCP).
Grupo de direcciones IP	Asigne una dirección IP a la máquina virtual de servicios desde el grupo de direcciones IP seleccionado.

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

11 Supervise la implementación hasta que **Estado de instalación** (Installation Status) muestre Correcto (Successful). Si el estado muestra Con errores (Failed), haga clic en el icono junto a Con errores (Failed) y complete las acciones necesarias para solucionar el error.

Qué hacer a continuación

Ahora puede consumir el servicio del partner a través de la interfaz de usuario de NSX o NSX API.

Utilizar Service Composer en NSX para vShield Endpoint

Service Composer permite aprovisionar y asignar los servicios de red y seguridad a las aplicaciones en una infraestructura virtual.

Service Composer se utiliza para crear grupos y directivas de seguridad. Los grupos de seguridad pueden contener definiciones de afiliación a grupos dinámicas y estáticas. Las directivas de seguridad aplican servicios a los grupos de seguridad.

Consulte la documentación de Service Composer en la *Guía de administración de NSX* para obtener información e instrucciones.

Índice