



Documentación de NetApp HCI 1,9

HCI

NetApp
September 23, 2024

Tabla de contenidos

Documentación de NetApp HCI 1,9	1
Soluciones NetApp HCI	2
Notas de la versión	3
Novedades en NetApp HCI	3
Información adicional sobre la versión	4
Conceptos	7
Información general del producto NetApp HCI	7
Cuentas de usuario	8
Protección de datos	10
De clúster	14
Nodos	17
Reducida	18
Licencias de NetApp HCI	22
Máximos de configuración del control del cloud híbrido de NetApp	23
Seguridad NetApp HCI	23
Rendimiento y calidad de servicio	25
Requisitos y tareas previas a la implementación	29
Información general sobre los requisitos para la puesta en marcha de NetApp HCI	29
Requisitos del nodo de gestión	29
Requisitos de puerto de red	29
Requisitos de switch y red	35
Requisitos de cables de red	36
Requisitos de dirección IP	37
Configuración de red	38
Requisitos de DNS y de control del tiempo	47
Requisitos ambientales	48
Dominios de protección	48
Requisitos de recursos de nodo de observación para clústeres de almacenamiento de dos nodos	48
Empiece a usar NetApp HCI	50
Información general sobre la instalación y la puesta en marcha de NetApp HCI	50
Instale el hardware H-Series	56
Configure LACP para alcanzar un rendimiento de almacenamiento óptimo	74
Validar su entorno con Active IQ Config Advisor	75
Configure IPMI para cada nodo	77
Ponga en marcha NetApp HCI	81
Acceda al motor de implementación de NetApp	81
Inicie la implementación	84
Importe un perfil de instalación	85
Configure VMware vSphere	85
Configurar las credenciales de NetApp HCI	88
Seleccione una topología de red	89
Selección de inventario	90
Configure los ajustes de red	92

Revisar e implementar la configuración	98
Tareas posteriores a la implementación	100
Gestione NetApp HCI	114
Información general de la gestión de NetApp HCI	114
Configure el acceso completo a la interfaz de usuario web de Nombre de dominio	114
Cambie las credenciales en NetApp HCI y SolidFire de NetApp	119
Actualice las credenciales de vCenter y ESXi	124
Gestione el almacenamiento NetApp HCI	127
Trabaje con el nodo de gestión	150
Apaga o enciende el sistema NetApp HCI	201
Supervise su sistema NetApp HCI con el control del cloud híbrido de NetApp	205
Supervise los recursos de almacenamiento y computación en la consola de control de cloud híbrido	205
Consulte el inventario en la página Nodes	211
Edite la información de conexión de la controladora de gestión de placa base	213
Supervise los volúmenes en el clúster de almacenamiento de	217
Supervise el rendimiento, la capacidad y el estado del clúster con SolidFire Active IQ	218
Recopile registros para solucionar problemas	219
Actualice su sistema NetApp HCI versión 1.9 o 1.9P1	224
Información general sobre la secuencia de actualización	224
Procedimientos de actualización del sistema	226
Actualice los componentes de vSphere para un sistema NetApp HCI con el plugin de Element para vCenter Server	311
Amplíe su sistema NetApp HCI	312
Visión general de la ampliación	312
Amplíe los recursos de almacenamiento de NetApp HCI	313
Amplíe los recursos de computación de NetApp HCI	314
Amplíe los recursos informáticos y de almacenamiento de NetApp HCI al mismo tiempo	317
Quite nodos de testigos después de expandir el clúster	320
Use Rancher en NetApp HCI	323
Descripción general de rancher on NetApp HCI	323
Rancher en conceptos de NetApp HCI	325
Requisitos para Rancher en NetApp HCI	326
Ponga en marcha Rancher en NetApp HCI	329
Tareas posteriores a la implementación	333
Poner en marcha aplicaciones y clústeres de usuarios	339
Administrar Rancher en NetApp HCI	339
Supervisar un Rancher en la implementación de NetApp HCI	340
Actualice Rancher en NetApp HCI	342
Retire una instalación de Rancher en NetApp HCI	348
Mantenimiento de hardware H-Series	351
Descripción general del mantenimiento de hardware H-Series	351
Sustituya el chasis 2U de la serie H	351
Sustituya las unidades de alimentación CC en los nodos H615C y H610S	358
Reemplace los DIMM en los nodos de computación	360
Sustituya las unidades para los nodos de almacenamiento	369

Sustituya los nodos H410C	374
Sustituya los nodos H410S	401
Reemplace los nodos H610C y H615C	408
Sustituya los nodos H610S	414
Sustituya las unidades de alimentación	416
Sustituir los interruptores SN2010, SN2100 y SN2700	419
Sustituya el nodo de almacenamiento en un clúster de dos nodos	427
Versiones anteriores de la documentación de NetApp HCI	429
Avisos legales	430
Derechos de autor	430
Marcas comerciales	430
Estadounidenses	430
Política de privacidad	430
Código abierto	430

Documentación de NetApp HCI 1,9

Soluciones NetApp HCI

Las soluciones de NetApp HCI pueden ayudarle a lograr el rendimiento a escala con varias cargas de trabajo en la misma infraestructura sin ningún tipo de fricción.

NetApp HCI le permite implementar servicios cloud en varios proveedores de cloud público y en las instalaciones. Puede usar NetApp HCI para implementar servicios similares a los que podría hacer con un proveedor de cloud, todo ello en un modo de autoservicio sin involucrar al DEPARTAMENTO DE TI.

Para obtener más información sobre las soluciones NetApp HCI, consulte "[Documentación de las soluciones NetApp HCI](#)".

Obtenga más información

- "[Recursos de NetApp HCI](#)"

Notas de la versión

Novedades en NetApp HCI

NetApp actualiza periódicamente NetApp HCI para ofrecerle nuevas funciones, mejoras y correcciones de errores. NetApp HCI 1,9 P1 incluye el software de NetApp Element 12.3.1 para clústeres de almacenamiento.



Element 12.3.2 contiene la mitigación que cierra la exposición del software Element a la vulnerabilidad Apache Log4j. Los clústeres de almacenamiento de SolidFire de NetApp con la función Virtual Volumes (VVol) habilitada se exponen a esta vulnerabilidad.

Si el clúster de almacenamiento es Element 12.3.1 y la función VVol está habilitada, debe actualizar al software Element 12.3.2.

Si el clúster de almacenamiento es Element 12.3.1 y la función VVol está deshabilitada, la actualización al software Element 12.3.2 es opcional.

NetApp no recomienda ejecutar versiones mixtas de Element en un clúster, a excepción de la duración de la actualización.

- La [NetApp HCI 1.9P1](#) En la sección se describen las nuevas funciones y actualizaciones en la versión 1.9P1 de NetApp HCI.
- La [Elemento 12.3.1](#) La sección describe las nuevas funciones y actualizaciones de NetApp Element 12.3.1.

NetApp HCI 1.9P1

NetApp HCI 1,9 P1 incluye mejoras de seguridad y estabilidad.

Elemento 12.3.1

NetApp HCI 1,9 P1 incluye Element 12.3.1 para los clústeres de almacenamiento.

Paquete de firmware de almacenamiento 2.99.2

La versión 12.3.1 de Element incluye la versión 2.99.2 del paquete de firmware de almacenamiento. Si el clúster de almacenamiento ya está en Element 12.3, tiene la opción de instalar simplemente el nuevo paquete de firmware 2.99.2.

NetApp Bugs Online contiene problemas conocidos y resueltos

Los problemas conocidos y resueltos, figuran en la herramienta NetApp Bugs Online. Puede examinar estos problemas para Element y otros productos en "[NetApp Bugs Online](#)".

Pasos

1. Vaya a "[NetApp Bugs Online](#)".
2. En el campo **Buscar por palabra clave**, escriba el nombre del producto, por ejemplo, "elemento".
- 3.

Seleccione la , Seleccione el filtro **Fixed in Versions** y seleccione **OK**.

Manage Columns

<input checked="" type="checkbox"/>	Fav
<input type="checkbox"/>	Notes
<input checked="" type="checkbox"/>	Title
<input type="checkbox"/>	Summary
<input checked="" type="checkbox"/>	Severity
<input checked="" type="checkbox"/>	Fixed In Versions
<input checked="" type="checkbox"/>	Found In Versions
<input type="checkbox"/>	Workaround
<input type="checkbox"/>	Product ID
<input checked="" type="checkbox"/>	Bug ID
<input type="checkbox"/>	Bug Title
<input type="checkbox"/>	Internal Code Names
<input type="checkbox"/>	Internal Workarounds

[Cancel](#)

4. Seleccione **Nueva búsqueda**.
5. Escriba la versión de versión en el campo **Fixed in Versions**.

Obtenga más información

- ["Notas de la versión de los servicios de gestión y control del cloud híbrido de NetApp"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)
- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Información adicional sobre la versión

Es posible encontrar enlaces a las notas de la versión más reciente y anteriores para varios componentes del entorno de almacenamiento de NetApp HCI y Element.



Se le pedirá que inicie sesión con sus credenciales del sitio de soporte de NetApp.

NetApp HCI

- ["Notas de la versión de NetApp HCI 1.9P1"](#)
- ["Notas de la versión de NetApp HCI 1.9"](#)
- ["Notas de la versión de NetApp HCI 1.8P1"](#)
- ["Notas de la versión de NetApp HCI 1.8"](#)
- ["Notas de la versión de NetApp HCI 1.7P1"](#)

Software NetApp Element

- ["Notas de la versión del software NetApp Element 12.3.2"](#)
- ["Notas de la versión del software NetApp Element 12.3.1"](#)
- ["Notas de la versión del software NetApp Element 12.3"](#)
- ["Notas de la versión del software NetApp Element 12.2.1"](#)
- ["Notas de la versión del software NetApp Element 12.2"](#)
- ["Notas de la versión del software NetApp Element 12.0.1"](#)
- ["Notas de la versión del software NetApp Element 12.0"](#)
- ["Notas de la versión del software NetApp Element 11.8"](#)
- ["Notas de la versión del software NetApp Element 11.7"](#)
- ["Notas de la versión del software NetApp Element 11.5.1"](#)
- ["Notas de la versión del software NetApp Element 11.3P1"](#)

Servicios de gestión

- ["Notas de la versión de los servicios de gestión"](#)

Plugin de NetApp Element para vCenter Server

- ["Notas de la versión del plugin de vCenter 5,3" *NEW*](#)
- ["Notas de la versión del plugin de vCenter 5,2"](#)
- ["Notas de la versión del plugin de vCenter 5.1"](#)
- ["Notas de la versión del plugin de vCenter 5.0"](#)
- ["Notas de la versión del plugin de vCenter 4.10"](#)
- ["Notas de la versión del plugin de vCenter 4.9"](#)
- ["Notas de la versión del plugin de vCenter 4.8"](#)
- ["Notas de la versión del plugin de vCenter 4.7"](#)
- ["Notas de la versión del plugin de vCenter 4.6"](#)
- ["Notas de la versión del plugin de vCenter 4.5"](#)
- ["Notas de la versión del plugin de vCenter 4.4"](#)

- ["Notas de la versión del plugin de vCenter 4.3"](#)

Firmware de computación

- ["Notas de la versión de Compute firmware Bundle 2.146"](#)
- ["Notas de la versión de Compute firmware Bundle 2.76"](#)
- ["Notas de la versión de Compute firmware Bundle 2.27"](#)
- ["Notas de la versión de Compute firmware Bundle 12.2.109"](#)
- ["Versiones de firmware y controlador ESXi compatibles"](#)

Firmware de almacenamiento

- ["Notas de la versión del paquete de firmware de almacenamiento 2.146"](#)
- ["Notas de la versión del paquete de firmware de almacenamiento 2.99.2"](#)
- ["Notas de la versión del paquete de firmware de almacenamiento 2.76"](#)
- ["Notas de la versión del paquete de firmware de almacenamiento 2.27"](#)
- ["Notas de la versión de H610S BMC 3.84.07"](#)
- ["Versiones de firmware y controlador ESXi compatibles"](#)

Conceptos

Información general del producto NetApp HCI

NetApp HCI es un diseño de infraestructura de cloud híbrido de clase empresarial que combina el almacenamiento, la computación, la conexión a redes y el hipervisor, y añade funcionalidades que abarcan los clouds privados y públicos.

La infraestructura de cloud híbrido desagregada de NetApp permite un escalado independiente de la computación y el almacenamiento, adaptándose a las cargas de trabajo con un rendimiento garantizado.

- Satisface la demanda del multicloud híbrido
- Escala los recursos de computación y de almacenamiento de forma independiente
- Simplifica la orquestación de servicios de datos entre multiclouds híbridos

Componentes de NetApp HCI

A continuación se ofrece una descripción general de los distintos componentes del entorno de NetApp HCI:

- NetApp HCI proporciona recursos de almacenamiento e informáticos. Utilice el asistente **Motor de puesta en marcha de NetApp** para implementar NetApp HCI. Después de realizar la implementación correctamente, los nodos de computación se muestran como hosts ESXi y se pueden gestionar en VMware vSphere Web Client.
- **Los servicios de gestión** o microservicios incluyen el recopilador Active IQ, QoSSIOC para el complemento vCenter y el servicio mNode; se actualizan con frecuencia como paquetes de servicio. A partir de la versión Element 11.3, **servicios de administración** se alojan en el nodo de gestión, lo que permite actualizaciones más rápidas de determinados servicios de software fuera de las versiones principales. El **nodo de gestión** (mNode) es una máquina virtual que se ejecuta en paralelo con uno o varios clústeres de almacenamiento basados en software Element. Se utiliza para actualizar y proporcionar servicios del sistema como supervisión y telemetría, gestionar activos y configuraciones del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas.



Más información acerca de "[lanzamientos de servicios de gestión](#)".

- **El control del cloud híbrido de NetApp** le permite gestionar NetApp HCI. Puede actualizar los servicios de gestión, ampliar el sistema, recopilar registros y supervisar la instalación mediante SolidFire Active IQ de NetApp. Para iniciar sesión en NetApp Hybrid Cloud Control, vaya a la dirección IP del nodo de gestión.
- El complemento **NetApp Element para vCenter Server** es una herramienta web integrada con la interfaz de usuario (UI) de vSphere. El complemento es una extensión e interfaz escalable y fácil de usar para VMware vSphere que permite gestionar y supervisar clústeres de almacenamiento que ejecutan **software NetApp Element**. El plugin ofrece una alternativa a la interfaz de usuario de Element. Puede usar la interfaz de usuario del plugin para detectar y configurar clústeres, así como para gestionar, supervisar y asignar almacenamiento de la capacidad del clúster con el fin de configurar almacenes de datos y almacenes de datos virtuales (para volúmenes virtuales). Se muestra un clúster en la red como grupo local único que se representa ante los hosts y administradores mediante direcciones IP virtuales. Adicionalmente, la actividad del clúster se puede supervisar con informes en tiempo real, incluida la mensajería sobre alertas y errores de todo evento que pueda producirse durante la ejecución de varias operaciones.



Más información acerca de "[Plugin de NetApp Element para vCenter Server](#)".

- De forma predeterminada, NetApp HCI envía estadísticas de rendimiento y alerta al servicio **SolidFire Active IQ** de NetApp. Como parte del contrato de soporte normal, el soporte de NetApp supervisa estos datos y alerta al usuario sobre los cuellos de botella de rendimiento o los problemas potenciales del sistema. Si todavía no tiene una cuenta de soporte de NetApp, debe crear una (aunque tenga una cuenta de SolidFire Active IQ existente) para poder aprovechar este servicio.



Más información acerca de "[SolidFire Active IQ de NetApp](#)".

Direcciones URL de NetApp HCI

Estas son las direcciones URL comunes que utiliza con NetApp HCI:

URL	Descripción
<code>https://[IPv4 address of Bond1G interface on a storage node]</code>	Acceda al asistente del motor de implementación de NetApp para instalar y configurar NetApp HCI. " Leer más. "
<code><code>https://&lt;ManagementNodeIP&gt</code></code>	Acceda a Control del cloud híbrido de NetApp para actualizar, ampliar y supervisar su instalación de NetApp HCI, así como actualizar los servicios de gestión. " Leer más. "
<code>https://[IP address]:442</code>	Desde la interfaz de usuario por nodo, acceda a la configuración de red y clúster y utilice pruebas y utilidades del sistema. " Leer más. "
<code>https://[management node IP address]:9443</code>	Registre el paquete del plugin de vCenter en vSphere Web Client.
<code>https://activeiq.solidfire.com</code>	Supervise los datos y reciba alertas sobre los cuellos de botella de rendimiento o los problemas potenciales del sistema.
<code><a href="https://<ManagementNodeIP>/mnode">https://<ManagementNodeIP>/mnode</code>	Actualice manualmente los servicios de gestión mediante la interfaz de usuario de API DE REST desde el nodo de gestión.
<code>https://[storage cluster MVIP address]</code>	Acceda a la interfaz de usuario del software NetApp Element.

Obtenga más información

- "[Plugin de NetApp Element para vCenter Server](#)"
- "[Recursos de NetApp HCI](#)"

Cuentas de usuario

Para acceder a los recursos de almacenamiento del sistema, tendrá que configurar cuentas de usuario.

Gestionar cuentas de usuario

Las cuentas de usuario se utilizan para controlar el acceso a los recursos de almacenamiento en una red basada en software de NetApp Element. Se requiere al menos una cuenta de usuario para poder crear un volumen.

Cuando crea un volumen, este se asigna a una cuenta. Si creó un volumen virtual, la cuenta será el contenedor de almacenamiento.

A continuación, se indican algunas consideraciones adicionales:

- La cuenta contiene la autenticación CHAP que se necesita para acceder a los volúmenes que tiene asignados.
- Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.
- Las cuentas de usuario se pueden gestionar desde el punto de extensión NetApp Element Management.

Con el control del cloud híbrido de NetApp, puede crear y gestionar los siguientes tipos de cuentas:

- Cuentas de usuario de administrador para el clúster de almacenamiento de
- Cuentas de usuario autoritativas
- Cuentas de volúmenes, específicas solo para el clúster de almacenamiento en el que se crearon.

Cuentas de administrador de clúster de almacenamiento

Existen dos tipos de cuentas de administrador que se pueden encontrar en un clúster de almacenamiento donde se ejecuta el software NetApp Element:

- **Cuenta de administrador del clúster principal:** Esta cuenta de administrador se crea cuando se crea el clúster. Es la cuenta administrativa principal con el nivel de acceso al clúster más alto. Esta cuenta es similar a un usuario raíz en un sistema Linux. Puede cambiar la contraseña de esta cuenta de administrador.
- **Cuenta de administrador de clúster:** Puede otorgar a una cuenta de administrador de clúster un rango limitado de acceso administrativo para realizar tareas específicas dentro de un clúster. Las credenciales que se asignan a cada cuenta de administrador de clúster sirven para autenticar las solicitudes de la API y la interfaz de usuario de Element dentro del sistema de almacenamiento.



Se necesita una cuenta de administrador de clúster local (que no sea LDAP) para acceder a los nodos activos en un clúster a través de la interfaz de usuario por nodo. No se necesitan credenciales de cuenta para acceder a un nodo que aún no forme parte de un clúster.

Las cuentas de administrador de clúster se pueden gestionar creando, eliminando y editando las cuentas de administrador de clúster, cambiando la contraseña de administrador de clúster y configurando los ajustes LDAP para gestionar el acceso al sistema para los usuarios.

Cuentas de usuario autoritativas

Las cuentas de usuario con autoridad pueden autenticarse en cualquier activo de almacenamiento asociado con la instancia de Cloud Control de NetApp de los nodos y los clústeres. Con esta cuenta, puede gestionar volúmenes, cuentas, grupos de acceso y mucho más en todos los clústeres.

Las cuentas de usuario autorizadas se gestionan desde la opción de gestión de usuarios del menú superior

derecho del control de cloud híbrido de NetApp.

La "[clúster de almacenamiento fiable](#)" Es el clúster de almacenamiento que utiliza el control del cloud híbrido de NetApp para autenticar usuarios.

Todos los usuarios que se creen en el clúster de almacenamiento autorizado pueden iniciar sesión en Hybrid Cloud Control de NetApp. Los usuarios creados en otros clústeres de almacenamiento *no se pueden* iniciar sesión en Hybrid Cloud Control.

- Si su nodo de gestión solo tiene un clúster de almacenamiento, es el clúster autorizado.
- Si su nodo de gestión tiene dos o más clústeres de almacenamiento, uno de esos clústeres se asigna como un clúster autorizado y solo los usuarios de ese clúster pueden iniciar sesión en Hybrid Cloud Control de NetApp.

Aunque muchas de las funciones de control de cloud híbrido de NetApp funcionan con varios clústeres de almacenamiento, la autenticación y la autorización tienen las limitaciones necesarias. La limitación de la autenticación y la autorización consiste en que los usuarios del clúster autorizado pueden ejecutar acciones en otros clústeres vinculados a Hybrid Cloud Control de NetApp incluso si no son usuarios en otros clústeres de almacenamiento. Antes de continuar con la gestión de varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados se hayan definido en todos los demás clústeres de almacenamiento con los mismos permisos. Puede gestionar usuarios desde NetApp Hybrid Cloud Control.

Cuentas de volumen

Las cuentas específicas de cada volumen solo son específicas del clúster de almacenamiento en el que se crearon. Estas cuentas permiten establecer permisos en volúmenes específicos de la red, pero no afectan fuera de dichos volúmenes.

Las cuentas de volumen se gestionan en la tabla volúmenes de control de cloud híbrido de NetApp.

Obtenga más información

- ["Administrar cuentas de usuario"](#)
- ["Obtenga información acerca de los clústeres"](#)
- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Protección de datos

Los términos de protección de datos de NetApp HCI incluyen diferentes tipos de replicación remota, snapshots de volúmenes, clonado de volúmenes, dominios de protección y alta disponibilidad con tecnología Double Helix.

La protección de datos de NetApp HCI incluye los siguientes conceptos:

- [Tipos de replicación remota](#)
- [Snapshots de volumen para proteger los datos](#)
- [Clones de volúmenes](#)
- [Información general sobre el proceso de backup y restauración para el almacenamiento de SolidFire](#)

- [Dominios de protección](#)
- [Alta disponibilidad de Double Helix](#)

Tipos de replicación remota

La replicación remota de datos puede adoptar las siguientes formas:

- [Replicación síncrona y asíncrona entre clústeres](#)
- [Replicación solo de Snapshot](#)
- [Replicación entre clústeres de Element y ONTAP mediante SnapMirror](#)

Consulte "[TR-4741: Replicación remota del software NetApp Element](#)".

Replicación síncrona y asíncrona entre clústeres

En los clústeres que ejecutan el software NetApp Element, la replicación en tiempo real permite la creación rápida de copias remotas de datos de volumen.

Un clúster de almacenamiento se puede emparejar con hasta otros cuatro clústeres de almacenamiento. Es posible replicar datos de volúmenes de forma síncrona o asíncrona desde un clúster de una pareja de clústeres para escenarios de conmutación por error y conmutación tras recuperación.

Replicación síncrona

La replicación síncrona replica continuamente datos del clúster de origen al clúster de destino y se ve afectada por la latencia, la pérdida de paquetes, la fluctuación y el ancho de banda.

La replicación síncrona es adecuada para las siguientes situaciones:

- Replicación de varios sistemas a corta distancia
- Sitio de recuperación ante desastres que sea geográficamente local en el origen
- Las aplicaciones más urgentes y la protección de las bases de datos
- Aplicaciones de continuidad del negocio que requieren que el sitio secundario actúe como el sitio principal cuando el sitio principal esté inactivo

Replicación asíncrona

La replicación asíncrona replica continuamente datos de un clúster de origen a un clúster de destino sin esperar los reconocimientos del clúster de destino. Durante la replicación asíncrona, las escrituras se reconocen en el cliente (aplicación) después de que se aplican en el clúster de origen.

La replicación asíncrona es apropiada para las siguientes situaciones:

- El sitio de recuperación ante desastres está lejos del origen y la aplicación no tolera latencias inducidas por la red.
- La red que conecta los clústeres de origen y destino tiene limitaciones de ancho de banda.

Replicación solo de Snapshot

La protección de datos con Snapshot replica los datos modificados en momentos específicos a un clúster remoto. Solo se replican las copias de Snapshot que se crean en el clúster de origen. No se producen las escrituras activas del volumen de origen.

Puede establecer la frecuencia de las replicaciones de snapshots.

La replicación Snapshot no afecta a la replicación asíncrona o síncrona.

Replicación entre clústeres de Element y ONTAP mediante SnapMirror

Con la tecnología SnapMirror de NetApp, puede replicar copias snapshot realizadas mediante el software NetApp Element en ONTAP con fines de recuperación ante desastres. En una relación de SnapMirror, Element es un extremo y ONTAP es el otro.

SnapMirror es la tecnología de replicación Snapshot™ de NetApp que facilita la recuperación ante desastres, diseñada para la conmutación por error del almacenamiento principal al almacenamiento secundario en un centro geográficamente remoto. La tecnología SnapMirror crea una réplica, o réplica, de los datos del trabajo en almacenamiento secundario desde el cual puede seguir proporcionando datos si se produce una interrupción del servicio en el sitio principal. Los datos se reflejan en el nivel de volumen.

La relación entre el volumen de origen en el almacenamiento primario y el volumen de destino en el almacenamiento secundario se denomina relación de protección de datos. Los clústeres se denominan extremos en los que residen los volúmenes y los volúmenes que contienen los datos replicados deben tener una relación entre iguales. Una relación entre iguales permite que clústeres y volúmenes intercambien datos de forma segura.

SnapMirror se ejecuta de forma nativa en las controladoras ONTAP de NetApp y está integrado en Element, que se ejecuta en clústeres de NetApp HCI y SolidFire. La lógica para controlar SnapMirror reside en el software ONTAP; por tanto, todas las relaciones de SnapMirror deben implicar al menos un sistema ONTAP para realizar las tareas de coordinación. Los usuarios gestionan las relaciones entre los clústeres de Element y ONTAP principalmente mediante la interfaz de usuario de Element; no obstante, algunas tareas de gestión residen en ONTAP System Manager de NetApp. Los usuarios también pueden gestionar SnapMirror mediante la CLI y la API, que están disponibles en ONTAP y Element.

Consulte "[TR-4651: Arquitectura y configuración de SnapMirror para SolidFire de NetApp](#)" (se requiere inicio de sesión).

Es necesario habilitar manualmente la funcionalidad SnapMirror en el nivel de clúster mediante el software Element. La funcionalidad SnapMirror está deshabilitada de forma predeterminada y no se habilita automáticamente como parte de una nueva instalación o actualización.

Después de habilitar SnapMirror, es posible crear relaciones de SnapMirror desde la pestaña Data Protection del software Element.

Snapshots de volumen para proteger los datos

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen que se puede utilizar más adelante para restaurar un volumen a ese momento específico.

Aunque las copias de Snapshot son similares a los clones de volúmenes, las copias de Snapshot son réplicas de los metadatos del volumen, por lo que no se pueden montar ni escribir en ellas. Además, para crear una copia de Snapshot de volumen, solo se requiere una pequeña cantidad de espacio y recursos del sistema, lo cual es más rápido crear una copia de Snapshot que clonar.

Las snapshots se pueden replicar en un clúster de remoto y usarlas como copia de backup del volumen. Gracias a ello, es posible revertir un volumen a un momento específico mediante la copia de Snapshot replicada, así como crear un clon de un volumen a partir de esta copia de Snapshot replicada.

Es posible realizar backups de snapshots de un clúster de SolidFire en un almacén de objetos externo o en

otro clúster de SolidFire. Cuando se crea un backup de una copia de Snapshot en un almacén de objetos externo, debe haber una conexión con el almacén de objetos que permita realizar operaciones de lectura y escritura.

Es posible realizar una copia Snapshot de un volumen individual o varias para la protección de datos.

Clones de volúmenes

Un clon de un solo volumen o de varios volúmenes es una copia puntual de los datos. Cuando se clona un volumen, el sistema crea una copia de Snapshot del volumen y, a continuación, crea una copia de los datos que se indican en la copia de Snapshot.

Este es un proceso asíncrono, y la cantidad de tiempo que requiere el proceso depende del tamaño del volumen que se clona y de la carga del clúster actual.

El clúster admite hasta dos solicitudes de clones en ejecución por volumen a la vez y hasta ocho operaciones de clones de volúmenes activos a la vez. Las solicitudes que superen este límite se pondrán en cola para procesarlas más adelante.

Información general sobre el proceso de backup y restauración para el almacenamiento de SolidFire

Es posible realizar backups y restaurar volúmenes en otro almacenamiento de SolidFire, así como en almacenes de objetos secundarios que sean compatibles con OpenStack Swift o Amazon S3.

Es posible realizar un backup de un volumen en los siguientes casos:

- Un clúster de almacenamiento de SolidFire
- Un almacén de objetos Amazon S3
- Un almacén de objetos OpenStack Swift

Cuando se restauran volúmenes desde OpenStack Swift o Amazon S3, se necesita información de manifiesto desde el proceso de backup original. Si desea restaurar un volumen de del cual se había realizado un backup en un sistema de almacenamiento de SolidFire, no será necesaria ninguna información de manifiesto.

Dominios de protección

Un dominio de protección es un nodo o un conjunto de nodos agrupados, de modo que cualquier parte o incluso todos pueden fallar mientras se mantiene la disponibilidad de los datos. Los dominios de protección permiten que un clúster de almacenamiento se sane automáticamente de la pérdida de un chasis (afinidad de chasis) o de un dominio completo (grupo de chasis).

El diseño de un dominio de protección asigna cada nodo a un dominio de protección específico.

Se admiten dos diseños diferentes de dominios de protección, denominados niveles de dominio de protección.

- En el nivel de nodo, cada nodo está en su propio dominio de protección.
- En el nivel del chasis, solo los nodos que comparten un chasis se encuentran en el mismo dominio de protección.
 - La distribución del nivel de chasis se determina automáticamente desde el hardware cuando el nodo se añade al clúster.
 - En un clúster en el que cada nodo se encuentra en un chasis independiente, estos dos niveles son

funcionalmente idénticos.

Puede hacerlo manualmente "[habilite la supervisión del dominio de protección](#)" Usar el plugin de NetApp Element para vCenter Server. Puede seleccionar un umbral para el dominio de protección a partir de dominios de nodo o de chasis.

Cuando se crea un clúster nuevo, si se utilizan nodos de almacenamiento que residen en un chasis compartido, es posible que desee considerar el diseño de la protección contra fallos en el nivel del chasis mediante la función de dominios de protección.

Se puede definir un diseño de dominio de protección personalizado, donde cada nodo está asociado a un único dominio de protección personalizado. De manera predeterminada, cada nodo se asigna al mismo dominio de protección personalizado predeterminado.

Alta disponibilidad de Double Helix

La protección de datos de Double Helix es un método de replicación que expande al menos dos copias de datos redundantes en todas las unidades de un sistema. El enfoque "sin RAID" permite que un sistema absorba múltiples fallos simultáneos en todos los niveles del sistema de almacenamiento y los repare rápidamente.

Obtenga más información

- "[Recursos de NetApp HCI](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"

De clúster

Un clúster es un grupo de nodos que funciona como un conjunto colectivo, que proporcionan recursos de almacenamiento o de computación. A partir de NetApp HCI 1.8, puede tener un clúster de almacenamiento con dos nodos. Un clúster de almacenamiento aparece en la red como un grupo lógico y se puede acceder a él como almacenamiento basado en bloques.

La capa de almacenamiento de NetApp HCI es proporcionada por el software NetApp Element y el nivel de gestión lo proporciona el plugin de NetApp Element para vCenter Server. Un nodo de almacenamiento de es un servidor que contiene una colección de unidades que se comunican entre sí a través de la interfaz de red Bond10G. Cada nodo de almacenamiento está conectado a dos redes, almacenamiento y gestión, cada una con dos enlaces independientes por motivos de redundancia y rendimiento. Cada nodo requiere una dirección IP en cada red. Es posible crear un clúster con nodos de almacenamiento nuevos o añadir nodos de almacenamiento a un clúster existente para aumentar el rendimiento y la capacidad del almacenamiento.

Clústeres de almacenamiento autoritativos

El clúster de almacenamiento autorizado es el clúster de almacenamiento que utiliza Hybrid Cloud Control de NetApp para autenticar usuarios.

Si su nodo de gestión solo tiene un clúster de almacenamiento, es el clúster autorizado. Si su nodo de gestión tiene dos o más clústeres de almacenamiento, uno de esos clústeres se asigna como un clúster autorizado y solo los usuarios de ese clúster pueden iniciar sesión en Hybrid Cloud Control de NetApp. Para averiguar qué clúster es el clúster autorizado, puede utilizar `GET /mnode/about` API. En la respuesta, la dirección IP de la `token_url` Field es la dirección IP virtual de gestión (MVIP) del clúster de almacenamiento autorizado. Si

intenta iniciar sesión en NetApp Hybrid Cloud Control como usuario que no está en el clúster autorizado, el intento de inicio de sesión fallará.

Muchas funciones de control de cloud híbrido de NetApp están diseñadas para funcionar con varios clústeres de almacenamiento, pero la autenticación y la autorización tienen limitaciones. La limitación de la autenticación y la autorización consiste en que el usuario del clúster autorizado puede ejecutar acciones en otros clústeres vinculados a Hybrid Cloud Control de NetApp incluso si no son usuarios en otros clústeres de almacenamiento. Antes de continuar con la gestión de varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados se hayan definido en todos los demás clústeres de almacenamiento con los mismos permisos.

Puede gestionar usuarios con NetApp Hybrid Cloud Control.

Antes de continuar con la gestión de varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados se hayan definido en todos los demás clústeres de almacenamiento con los mismos permisos. Consulte ["Crear y gestionar activos de clúster de almacenamiento"](#) para obtener más información sobre el trabajo con activos de clústeres de almacenamiento del nodo de gestión.

Capacidad desaprovechada

Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto ocurra. Cuando un nodo se queda sin poner en cadena, se produce un error del clúster adecuado.

Clústeres de almacenamiento de dos nodos

A partir de NetApp HCI 1.8, puede configurar un clúster de almacenamiento con dos nodos de almacenamiento.

- Puede usar ciertos tipos de nodos para formar el clúster de almacenamiento de dos nodos. Consulte ["Notas de la versión de NetApp HCI 1.8"](#).



En un clúster de dos nodos, los nodos de almacenamiento se limitan a los nodos con unidades de 480 GB y 960 GB. Además, los nodos deben ser del mismo tipo de modelo.

- Los clústeres de almacenamiento de dos nodos son ideales para las implementaciones a pequeña escala con cargas de trabajo que no dependen de grandes requisitos de capacidad y alto rendimiento.
- Además de dos nodos de almacenamiento, un clúster de almacenamiento de dos nodos también incluye dos * nodos testigos de NetApp HCI*.



Más información acerca de ["Nodos de testigos."](#)

- Es posible escalar un clúster de almacenamiento de dos nodos a un clúster de almacenamiento de tres nodos. Los clústeres de tres nodos aumentan la resiliencia al proporcionar la capacidad de recuperarse automáticamente de fallos de nodos de almacenamiento.
- Los clústeres de almacenamiento de dos nodos proporcionan las mismas funciones de seguridad y funcionalidades que los clústeres de almacenamiento de cuatro nodos tradicionales.

- Los clústeres de almacenamiento de dos nodos utilizan las mismas redes que los clústeres de almacenamiento de cuatro nodos. Las redes se configuran durante la implementación de NetApp HCI mediante el asistente del motor de puesta en marcha de NetApp.

Quórum del clúster de almacenamiento

El software Element crea un clúster de almacenamiento a partir de los nodos seleccionados, que mantiene una base de datos replicada de la configuración de clúster. Se necesita un mínimo de tres nodos para participar en el conjunto de clústeres a fin de mantener el quórum para la resiliencia del clúster. Los nodos de testigos de un clúster de dos nodos se utilizan para garantizar que haya suficientes nodos de almacenamiento para formar un conjunto de quórum válido. Para la creación del conjunto, los nodos de almacenamiento se prefieren frente a los nodos de testimonio. Para el conjunto mínimo de tres nodos que implica un clúster de almacenamiento de dos nodos, se utilizan dos nodos de almacenamiento y un nodo de testigo.



En un conjunto de tres nodos con dos nodos de almacenamiento y un nodo de testigo, si un nodo de almacenamiento se desconecta, el clúster entra en un estado degradado. De los dos nodos de testigos, solo uno puede estar activo en el conjunto. El segundo nodo de testimonio no se puede añadir al conjunto, ya que ejecuta el rol de backup. El clúster permanece en estado degradado hasta que el nodo de almacenamiento sin conexión vuelve a estar en línea o un nodo de sustitución se une al clúster.

Si se produce un error en un nodo de testigo, el nodo de testigo restante se une al conjunto para formar un conjunto de tres nodos. Puede implementar un nuevo nodo testigo para reemplazar el nodo testigo fallido.

Reparación automática y gestión de fallos en clústeres de almacenamiento de dos nodos

Si un componente de hardware falla en un nodo que forma parte de un clúster tradicional, el clúster puede reequilibrar los datos que se encuentran en el componente que no ha fallado en otros nodos disponibles del clúster. Esta capacidad para recuperarse automáticamente no está disponible en un clúster de almacenamiento de dos nodos, ya que debe haber disponible un mínimo de tres nodos de almacenamiento físico para que el clúster los repare automáticamente. Cuando falla un nodo de un clúster de dos nodos, el clúster de dos nodos no requiere la regeneración de una segunda copia de los datos. Las nuevas escrituras se replican para los datos en bloque en el nodo de almacenamiento activo restante. Cuando el nodo que ha fallado se reemplaza y se une al clúster, los datos se reequilibran entre los dos nodos de almacenamiento físicos.

Clústeres de almacenamiento con tres o más nodos

Al ampliar de dos nodos de almacenamiento a tres nodos de almacenamiento, el clúster será más resiliente gracias a que permite la reparación automática en caso de fallos de nodos y unidades, pero no proporciona capacidad adicional. Puede ampliar utilizando la "[IU de control del cloud híbrido de NetApp](#)". Al expandir un clúster de dos nodos a un clúster de tres nodos, la capacidad se puede dejar sin usar (consulte [Capacidad desaprovechada](#)). El asistente de la interfaz de usuario muestra advertencias sobre la capacidad desaprovechada antes de la instalación. Aún está disponible un único nodo de testigo para mantener el quórum del conjunto en caso de que se produzca un fallo en el nodo de almacenamiento, con un segundo nodo de testigo en espera. Cuando se amplía un clúster de almacenamiento de tres nodos a un clúster de cuatro nodos, la capacidad y el rendimiento aumentan. En un clúster de cuatro nodos, los nodos testigos ya no son necesarios para formar el quórum del clúster. Es posible ampliar hasta 64 nodos de computación y 40 nodos de almacenamiento.

Obtenga más información

- "[Clúster de almacenamiento de dos nodos NetApp HCI | TR-4823](#)"

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Nodos

Los nodos son recursos virtuales o de hardware que se agrupan en un clúster para proporcionar funcionalidades de computación y almacenamiento basado en bloques.

El software NetApp HCI y Element define varios roles de nodo para un clúster. Los cuatro tipos de roles de nodo son: **Nodo de gestión**, **nodo de almacenamiento**, **nodo de computación** y **nodos testigos NetApp HCI**.

Nodo de gestión

El nodo de gestión (a veces abreviado como mNode) interactúa con un clúster de almacenamiento para realizar acciones de gestión, pero no es miembro del clúster de almacenamiento. Los nodos de gestión recopilan información periódicamente sobre el clúster a través de llamadas API e informan a Active IQ para la supervisión remota (si está habilitada). Los nodos de gestión también son responsables de coordinar las actualizaciones de software de los nodos del clúster.

El nodo de gestión es una máquina virtual (VM) que se ejecuta en paralelo con uno o varios clústeres de almacenamiento basados en el software Element. Además de las actualizaciones, se usa para proporcionar servicios del sistema como supervisión y telemetría, gestionar los activos y las configuraciones del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas. A partir del lanzamiento de Element 11.3, el nodo de gestión funciona como host de microservicio, lo que permite actualizar más rápidamente los servicios de software seleccionados que no se incluyen en las principales versiones. Estos microservicios o servicios de gestión, como el recopilador Active IQ, QoSSIOC para el plugin de vCenter y el servicio de nodos de gestión, se actualizan con frecuencia como paquetes de servicio.

Nodos de almacenamiento

Los nodos de almacenamiento de NetApp HCI son elementos de hardware que proporcionan recursos de almacenamiento para un sistema NetApp HCI. Las unidades de cada nodo contienen espacio de bloques y metadatos para almacenar y gestionar los datos. Cada nodo contiene una imagen de fábrica de software NetApp Element. Los nodos de almacenamiento de NetApp HCI se pueden gestionar mediante el punto de extensión NetApp Element Management.

Nodos de computación

Los nodos de computación NetApp HCI son elementos de hardware que proporcionan recursos de computación, como CPU, memoria y redes, que se necesitan para la virtualización en la instalación de NetApp HCI. Como cada servidor ejecuta VMware ESXi, la gestión de los nodos de computación NetApp HCI (añadir o quitar hosts) debe realizarse fuera del plugin dentro del menú hosts and Clusters de vSphere. Ya sea que se trate de un clúster de almacenamiento de cuatro nodos o de un clúster de almacenamiento de dos nodos, el número mínimo de nodos de computación sigue siendo dos para una implementación de NetApp HCI.

Nodos de testigos

Los nodos de testimonio de NetApp HCI son máquinas virtuales que se ejecutan en nodos de computación en paralelo con un clúster de almacenamiento basado en el software Element. Los nodos de testigos no alojan los servicios de segmentos o bloques. Un nodo testigo habilita la disponibilidad de un clúster de

almacenamiento en caso de que se produzca un fallo en un nodo de almacenamiento. Puede gestionar y actualizar los nodos de testigos de la misma forma que los de otros nodos de almacenamiento. Un clúster de almacenamiento puede tener hasta cuatro nodos testigos. Su propósito principal es garantizar que existan nodos de clúster suficientes para formar un quórum de conjunto válido.

Mejor práctica: Configurar las VM del nodo testigo para utilizar el almacén de datos local del nodo de computación (establecido por NDE de forma predeterminada), no configurarlas en el almacenamiento compartido, como los volúmenes de almacenamiento SolidFire. Para evitar la migración automática de los equipos virtuales, establezca el nivel de automatización del planificador de recursos distribuidos (DRS) del nodo testigo en **Desactivado**. De este modo, se evita que ambos nodos testigos se ejecuten en el mismo nodo de computación y se cree una configuración de parejas que no sea de alta disponibilidad (ha).



Más información acerca de ["Requisitos de recursos del nodo de observación"](#) y ["Requisitos de dirección IP de los nodos de observación"](#).



En un clúster de almacenamiento de dos nodos, se ponen en marcha un mínimo de dos nodos testigos para garantizar la redundancia en caso de que se produzca un fallo en un nodo testigo. Cuando el proceso de instalación de NetApp HCI instala nodos testigo, se almacena una plantilla de máquina virtual en VMware vCenter que puede utilizar para volver a poner en marcha un nodo de testigo en caso de que se elimine, se pierda o se dañe por accidente. También puede utilizar la plantilla para volver a poner en marcha un nodo de testigo si necesita sustituir un nodo de computación con errores que alojaba el nodo de testigo. Para obtener instrucciones, consulte la sección **nodos de testigo de nueva puesta en marcha para clústeres de almacenamiento de dos y tres nodos** ["aquí"](#).

Obtenga más información

- ["Clúster de almacenamiento de dos nodos NetApp HCI | TR-4823"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Reducida

Modo de mantenimiento

Si necesita desconectar un nodo de almacenamiento para realizar tareas de mantenimiento, como actualizaciones de software o reparaciones de host, puede minimizar el impacto de I/O del resto del clúster de almacenamiento habilitando el modo de mantenimiento para ese nodo. Puede utilizar el modo de mantenimiento con los dos nodos de dispositivo, así como los nodos SDS de empresa SolidFire.



Cuando se apaga un nodo de almacenamiento, se muestra como **no disponible** en la columna Estado del nodo de la página almacenamiento en HCC, ya que esta columna muestra el estado del nodo desde la perspectiva del clúster. El estado apagado del nodo se indica mediante el icono **fuera de línea** junto al nombre de host del nodo.

Solo puede realizar la transición de un nodo de almacenamiento al modo de mantenimiento si el estado del nodo es bueno (no tiene fallos de clúster de bloqueo) y el clúster de almacenamiento es tolerante a un único

nodo de fallo. Una vez que se habilita el modo de mantenimiento para un nodo en buen estado y tolerante, el nodo no se realiza la transición de forma inmediata, sino que se supervisa hasta que se cumplen las siguientes condiciones:

- Todos los volúmenes alojados en el nodo se han relevado en caso de fallo
- El nodo ya no aloja como principal de ningún volumen
- Se asigna un nodo en espera temporal para cada volumen que se realiza el relevo de errores

Una vez que se cumplen estos criterios, el nodo pasa al modo de mantenimiento. Si no se cumplen estos criterios en un periodo de 5 minutos, el nodo no entrará en el modo de mantenimiento.

Cuando deshabilita el modo de mantenimiento para un nodo de almacenamiento, el nodo se supervisa hasta que se cumplen las siguientes condiciones:

- Todos los datos se replican completamente en el nodo
- Se resuelven todos los fallos del clúster de bloqueo
- Todas las asignaciones temporales de nodos en espera de los volúmenes alojados en el nodo se han desactivado

Una vez que se cumplen estos criterios, el nodo pasa del modo de mantenimiento. Si no se cumplen estos criterios en una hora, no podrá realizar la transición desde el modo de mantenimiento.

Puede ver los estados de las operaciones en modo de mantenimiento cuando trabaja con el modo de mantenimiento mediante la API de Element:

- **Deshabilitado:** No se ha solicitado ningún mantenimiento.
- **FailedToRecover:** El nodo no pudo recuperarse del mantenimiento.
- **RecoveringFromMaintenance:** El nodo se está recuperando del mantenimiento.
- * **PreparingForMaintenance*:** Se están llevando a cabo acciones para permitir que un nodo realice tareas de mantenimiento.
- **ReadyForMaintenance:** El nodo está listo para realizar el mantenimiento.

Obtenga más información

- ["Habilite el modo de mantenimiento con la API de Element"](#)
- ["Deshabilite el modo de mantenimiento con la API de Element"](#)
- ["Documentación sobre API de NetApp Element"](#)
- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Volúmenes

El almacenamiento se aprovisiona en el sistema NetApp Element como volúmenes. Los volúmenes son dispositivos de bloque a los que se accede a través de la red utilizando clientes iSCSI o Fibre Channel.

El plugin de NetApp Element para vCenter Server permite crear, ver, editar, eliminar, clonar, realice backups o restaure volúmenes para cuentas de usuario. También es posible gestionar cada volumen en un clúster, así como añadir o quitar volúmenes en grupos de acceso de volúmenes.

Volúmenes persistentes

Los volúmenes persistentes permiten que los datos de configuración del nodo de gestión se almacenen en un clúster de almacenamiento especificado, en lugar de localmente con una máquina virtual, de modo que los datos se puedan conservar en caso de pérdida o eliminación del nodo de gestión. Los volúmenes persistentes son una configuración de nodos de gestión opcional pero recomendada.

Si desea poner en marcha un nodo de gestión para NetApp HCI con el motor de puesta en marcha de NetApp, los volúmenes persistentes se habilitan y se configuran automáticamente.

Se incluye una opción para habilitar los volúmenes persistentes en las secuencias de comandos de instalación y actualización cuando se implementa un nuevo nodo de gestión. Los volúmenes persistentes son volúmenes en un clúster de almacenamiento basado en software Element que contienen información de configuración del nodo de gestión para la máquina virtual del nodo de gestión de host que permanece más allá de la vida útil de la máquina virtual. Si se pierde el nodo de gestión, una máquina virtual del nodo de gestión de reemplazo puede volver a conectarse y recuperar los datos de configuración de la máquina virtual perdida.

La funcionalidad de volúmenes persistentes, si se habilita durante la instalación o la actualización, crea automáticamente varios volúmenes con NetApp-HCI, cuyo nombre finaliza previamente al nombre en el clúster asignado. Estos volúmenes, como cualquier volumen basado en el software Element, se pueden ver mediante la interfaz de usuario web del software Element, el plugin de NetApp Element para vCenter Server o la API, según sus preferencias e instalación. Los volúmenes persistentes deben estar activos y en ejecución con una conexión iSCSI al nodo de gestión para mantener los datos de configuración actuales que se pueden usar para la recuperación.



Los volúmenes persistentes asociados con servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada

Obtenga más información

- ["Gestione los volúmenes"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Los grupos de acceso de volúmenes

Un grupo de acceso de volúmenes es una colección de volúmenes a la que los usuarios pueden acceder mediante iniciadores de iSCSI o Fibre Channel.

Mediante la creación y el uso de grupos de acceso de volúmenes, se puede controlar el acceso a un conjunto de volúmenes. Cuando se asocia un conjunto de volúmenes y un conjunto de iniciadores a un grupo de acceso de volúmenes, el grupo de acceso otorga a esos iniciadores acceso al conjunto de volúmenes.

Los grupos de acceso de volúmenes presentan los siguientes límites:

- Un máximo de 128 iniciadores por grupo de acceso de volúmenes.
- Un máximo de 64 grupos de acceso por volumen.
- Un grupo de acceso puede estar formado por un máximo de 2000 volúmenes.
- Un IQN o un WWPN solo pueden pertenecer a un grupo de acceso de volúmenes.

Obtenga más información

- ["Gestione los grupos de acceso de volúmenes"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Iniciadores

Los iniciadores permiten que los clientes externos accedan a los volúmenes de un clúster. Se utilizan como el punto de entrada de la comunicación entre clientes y volúmenes. Es posible usar iniciadores para el acceso basado en CHAP en lugar de acceso basado en la cuenta a los volúmenes de almacenamiento. Cuando se añade un iniciador único a un grupo de acceso de volúmenes, permite que los miembros del grupo de acceso de volúmenes accedan a todos los volúmenes de almacenamiento añadidos al grupo sin necesidad de autenticación. Un iniciador solo puede pertenecer a un grupo de acceso.

Obtenga más información

- ["Gestione los iniciadores"](#)
- ["Los grupos de acceso de volúmenes"](#)
- ["Gestione los grupos de acceso de volúmenes"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Dominios de protección personalizados

Se puede definir un diseño de dominio de protección personalizado, donde cada nodo está asociado a un único dominio de protección personalizado. De manera predeterminada, cada nodo se asigna al mismo dominio de protección personalizado predeterminado.

Si no se asignan dominios de protección personalizados:

- El funcionamiento del clúster no se ve afectado.
- El nivel personalizado no es tolerante ni resiliente.

Si se asigna más de un dominio de protección personalizado, cada subsistema asignará duplicados a distintos dominios de protección personalizados. Si esto no es posible, se revierte a la asignación de duplicados a nodos separados. Cada subsistema (por ejemplo, bandejas, segmentos, proveedores de extremo de protocolo y conjunto) realiza esto de forma independiente.



El uso de dominios de protección personalizados implica que no hay nodos que comparten un chasis.

Los siguientes métodos API de Element exponen estos nuevos dominios de protección:

- `GetProtectionDomainLayout` - muestra en qué chasis y qué dominio de protección personalizado se

encuentra cada nodo.

- SetProtectionDomainLayout - permite asignar un dominio de protección personalizado a cada nodo.

Póngase en contacto con el soporte de NetApp para obtener más información sobre el uso de dominios de protección personalizados.

Obtenga más información

["Gestione el almacenamiento con la API de Element"](#)

Licencias de NetApp HCI

Cuando se usa NetApp HCI, es posible que se necesiten licencias adicionales en función de lo que se esté usando.

Licencias de NetApp HCI y VMware vSphere

Las licencias de VMware vSphere dependen de su configuración:

Opción de red	Licencia
Opción A: Dos cables para nodos de computación mediante el etiquetado de VLAN (todos los nodos de computación)	Se requiere usar vSphere Distributed Switch, que requiere licencia VMware vSphere Enterprise Plus.
Opción B: Seis cables para nodos de computación que utilizan VLAN etiquetadas (nodo de computación de 4 nodos 2RU H410C)	Esta configuración utiliza vSphere Standard Switch como valor predeterminado. El uso opcional de vSphere Distributed Switch requiere la licencia VMware Enterprise Plus.
Opción C: Seis cables para nodos de computación mediante VLAN nativas y etiquetadas (H410C, nodo de computación de 4 nodos de 2RU)	Esta configuración utiliza vSphere Standard Switch como valor predeterminado. El uso opcional de vSphere Distributed Switch requiere la licencia VMware Enterprise Plus.

Licencias de NetApp HCI y ONTAP Select

Si se le proporcionó una versión de ONTAP Select para utilizarla junto con un sistema NetApp HCI adquirido, se aplicarán las siguientes limitaciones adicionales:

- La licencia de ONTAP Select, que se incluye con una venta de sistemas NetApp HCI, solo se puede usar junto con nodos de computación de NetApp HCI.
- El almacenamiento de esas instancias de ONTAP Select solo debe residir en los nodos de almacenamiento de NetApp HCI.

- Está prohibido el uso de nodos de computación de terceros o nodos de almacenamiento de terceros.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Máximos de configuración del control del cloud híbrido de NetApp

NetApp HCI incluye el control del cloud híbrido de NetApp para simplificar la gestión del ciclo de vida de los recursos informáticos y del almacenamiento. Admite actualizaciones del software Element en nodos de almacenamiento para los clústeres de almacenamiento de NetApp HCI y SolidFire de NetApp, así como actualizaciones del firmware para los nodos de computación NetApp HCI en NetApp HCI. De manera predeterminada, está disponible en los nodos de gestión en NetApp HCI.

Además de comunicar los componentes de hardware y software proporcionados por NetApp en una instalación de NetApp HCI, el control de cloud híbrido de NetApp interactúa con componentes de terceros en el entorno del cliente, como VMware vCenter. NetApp califica la funcionalidad de Hybrid Cloud Control de NetApp y su interacción con estos componentes de terceros en el entorno del cliente hasta cierta escala. Para obtener una experiencia óptima con el control de cloud híbrido de NetApp, NetApp recomienda permanecer dentro del rango de los máximos de configuración.

Si supera estos máximos probados, puede que experimente problemas con el control del cloud híbrido de NetApp, como una interfaz de usuario más lenta y respuestas de API o una funcionalidad que no esté disponible. Si colabora con NetApp para obtener soporte para productos con el control de cloud híbrido de NetApp en entornos que estén configurados más allá de los máximos de configuración, el soporte de NetApp le solicitará que cambie la configuración para que esté dentro de los máximos de configuración documentados.

Máximos de configuración

Control del cloud híbrido de NetApp es compatible con entornos VMware vSphere con hasta 500 nodos de computación de NetApp. Admite hasta 20 clústeres de almacenamiento basados en software de NetApp Element con 40 nodos de almacenamiento por clúster.

Seguridad NetApp HCI

Al utilizar NetApp HCI, sus datos están protegidos por protocolos de seguridad estándares del sector.

Cifrado en reposo para nodos de almacenamiento

NetApp HCI le permite cifrar todos los datos almacenados en el clúster de almacenamiento.

Todas las unidades de los nodos de almacenamiento capaces de cifrar utilizan cifrado AES de 256 bits a nivel de la unidad. Cada unidad tiene su propia clave de cifrado, que se crea cuando la unidad se inicializa por primera vez. Cuando habilita la función de cifrado, se crea una contraseña para todo el clúster de almacenamiento y los fragmentos de la contraseña se distribuyen a todos los nodos del clúster. Ningún nodo almacena la contraseña completa. La contraseña se utiliza para proteger todo el acceso a las unidades.

Necesita la contraseña para desbloquear la unidad y, como la unidad está cifrando todos los datos, sus datos estarán protegidos en todo momento.

Cuando habilita el cifrado en reposo, el rendimiento y la eficiencia del clúster de almacenamiento no se ven afectados. Además, si quita un nodo o una unidad habilitados para el cifrado del clúster de almacenamiento con la API de Element o la interfaz de usuario de Element, se deshabilita el cifrado en reposo en las unidades y las unidades se borran de forma segura, lo que protege los datos que se almacenaron previamente en esas unidades. Después de quitar la unidad, puede borrarla de forma segura con el `SecureEraseDrives` Método API. Si quita de forma forzada una unidad o un nodo del clúster de almacenamiento, los datos siguen estando protegidos por la contraseña del clúster y las claves de cifrado individuales de la unidad.

Para obtener información sobre cómo habilitar y deshabilitar el cifrado en reposo, consulte ["Habilitar y deshabilitar el cifrado para un clúster"](#) En el centro de documentación de SolidFire y Element.

Cifrado de software en reposo

El cifrado por software en reposo permite cifrar todos los datos que se escriben en las unidades SSD de un clúster de almacenamiento. Esto proporciona una capa principal de cifrado en los nodos SDS empresariales de SolidFire que no incluyen unidades de cifrado automático (SED).

Gestión de claves externas

Es posible configurar el software Element para utilizar un servicio de gestión de claves (KMS) compatible con KMIP de terceros para gestionar las claves de cifrado de los clústeres de almacenamiento. Cuando habilita esta función, la clave de cifrado de contraseña de acceso a unidades para todo el clúster de almacenamiento se gestiona mediante un KMS que especifique. Element puede usar los siguientes servicios de gestión de claves:

- SafeNet KeySecure de Gemalto
- SafeNet en KeySecure
- Control de claves HyTrust
- Administrador de seguridad de datos de VorMetric
- Administrador de ciclo de vida de claves de seguridad de IBM

Para obtener más información sobre la configuración de la gestión de claves externa, consulte ["Introducción a la gestión de claves externas"](#) En el centro de documentación de SolidFire y Element.

Autenticación de múltiples factores

La autenticación multifactor (MFA) permite requerir que los usuarios presenten múltiples tipos de pruebas para autenticar con la interfaz de usuario web de NetApp Element o la interfaz de usuario del nodo de almacenamiento después del inicio de sesión. Puede configurar el elemento para que acepte sólo la autenticación de múltiples factores para los inicios de sesión que se integran con el sistema de administración de usuarios y el proveedor de identidades existentes. Es posible configurar Element para que se integre con un proveedor de identidades SAML 2.0 existente que pueda aplicar múltiples esquemas de autenticación, como mensajes de texto y contraseña, mensajes de correo electrónico y contraseña, u otros métodos.

Puede emparejar la autenticación de múltiples factores con proveedores de identidades (PDI) compatibles con SAML 2.0 comunes, como Microsoft Active Directory Federation Services (ADFS) y Shibboleth.

Para configurar la MFA, consulte ["Activación de la autenticación multifactor"](#) En el centro de documentación de SolidFire y Element.

FIPS 140-2 para HTTPS y cifrado de datos en reposo

Los clústeres de almacenamiento SolidFire de NetApp y los sistemas NetApp HCI admiten el cifrado conforme a los requisitos de estándar de procesamiento de información federal (FIPS) 140-2 para módulos criptográficos. Es posible habilitar el cumplimiento de la normativa FIPS 140-2 en el clúster NetApp HCI o SolidFire para las comunicaciones HTTPS y el cifrado de unidades.

Cuando habilita el modo operativo FIPS 140-2 en el clúster, el clúster activa el módulo de seguridad de criptografía de NetApp (NCSM) y utiliza el cifrado certificado FIPS 140-2 de nivel 1 para todas las comunicaciones a través de HTTPS a la interfaz de usuario y la API de NetApp Element. Utilice la `EnableFeature` La API de Element con la `fips` Para habilitar el cifrado HTTPS FIPS 140-2. En los clústeres de almacenamiento con hardware compatible con FIPS, también es posible habilitar el cifrado de unidades FIPS para datos en reposo mediante el `EnableFeature` La API de Element con la `FipsDrives` parámetro.

Para obtener más información sobre cómo preparar un nuevo clúster de almacenamiento para el cifrado FIPS 140-2-2, consulte ["Creación de un clúster compatible con unidades FIPS"](#).

Para obtener más información sobre cómo habilitar FIPS 140-2 en un clúster existente y preparado, consulte ["La API del elemento EnableFeature"](#).

Rendimiento y calidad de servicio

Un clúster de almacenamiento de SolidFire puede proporcionar parámetros de calidad de servicio (QoS) por volumen. Puede garantizar el rendimiento del clúster medido en entradas y salidas por segundo (IOPS) utilizando tres parámetros configurables que definen la calidad de servicio: Min IOPS, Max IOPS y Burst IOPS.



SolidFire Active IQ tiene una página de recomendaciones de calidad de servicio que ofrece asesoramiento sobre la configuración óptima y la configuración de las opciones de calidad de servicio.

Parámetros de calidad de servicio

Los parámetros de IOPS se definen de las siguientes formas:

- **Mínimo de IOPS:** El número mínimo de entradas y salidas sostenidas por segundo (IOPS) que el clúster de almacenamiento proporciona a un volumen. El valor de Min IOPS configurado para un volumen es el nivel garantizado de rendimiento de un volumen. El rendimiento nunca es inferior a este nivel.
- **Maximum IOPS:** El número máximo de IOPS sostenidas que el clúster de almacenamiento proporciona a un volumen. Cuando los niveles de IOPS del clúster son extremadamente altos, este nivel de rendimiento de IOPS nunca se supera.
- **Burst IOPS:** El número máximo de IOPS permitidas en un escenario de ráfaga breve. Si un volumen se ejecuta por debajo del valor Max IOPS, se acumulan créditos de ráfaga. Cuando los niveles de rendimiento llegan a ser muy altos e incluso alcanzan los niveles máximos, se permiten ráfagas breves de IOPS en el volumen.

El software Element usa Burst IOPS cuando un clúster se ejecuta en un estado de bajo uso de IOPS de clúster.

Un solo volumen puede acumular Burst IOPS y usar los créditos para superar su Max IOPS en ráfagas hasta su nivel de Burst IOPS durante un "período de ráfaga" establecido. Un volumen puede usar ráfagas

durante hasta 60 segundos si el clúster tiene la capacidad de acomodar la ráfaga. Un volumen acumula un segundo de crédito de ráfaga (hasta un máximo de 60 segundos) por cada segundo que se ejecuta el volumen por debajo de su límite de Max IOPS.

Burst IOPS se limita de dos formas:

- Un volumen puede usar ráfagas por encima de su Max IOPS durante un número de segundos que sea igual al número de créditos de ráfaga que ha acumulado el volumen.
- Cuando un volumen usa ráfagas por encima de su configuración de Max IOPS, estará limitado por su valor de Burst IOPS. Por ello, la IOPS de ráfaga nunca supera el valor de Burst IOPS del volumen.
- **Ancho de banda máximo efectivo:** El ancho de banda máximo se calcula multiplicando el número de IOPS (en función de la curva QoS) por el tamaño de E/S.

Ejemplo: Una configuración del parámetro de calidad de servicio de 100 Min IOPS, 1000 Max IOPS y 1500 Burst IOPS afectan a la calidad del rendimiento de la siguiente manera:

- Las cargas de trabajo pueden alcanzar y sostener un máximo de 1000 IOPS hasta que la condición de contención de carga de trabajo de IOPS se hace evidente en el clúster. Las IOPS se reducen de forma incremental hasta que las IOPS de todos los volúmenes estén dentro de los rangos de calidad de servicio designados y la contención para el rendimiento mejore.
- El rendimiento de todos los volúmenes se empuja hasta el valor de Min IOPS de 100. Los niveles no se sitúan por debajo del valor de Min IOPS, pero podrían ser superiores a los 100 IOPS cuando la contención de carga de trabajo mejora.
- El rendimiento nunca supera las 1000 IOPS ni es inferior a 100 IOPS durante un período sostenido. Se permite el rendimiento de 1500 IOPS (Burst IOPS), pero solo para esos volúmenes que hayan acumulado créditos de ráfaga al ejecutarse por debajo del valor de Max IOPS y solo se permite durante breves periodos de tiempo. Los niveles de ráfaga nunca son sostenidos.

Límites de valor de calidad de servicio

Estos son los posibles valores mínimos y máximos de la calidad de servicio.

Parámetros	Valor mínimo	Predeterminado	4 4 KB	5 8 KB	6 16 KB	262 KB
IOPS mín	50	50	15,000	9,375*	5556*	385*
Tasa máx. De IOPS	100	15,000	200,000**	125,000	74,074	5128
IOPS de ráfaga	100	15,000	200,000**	125,000	74.074	5128

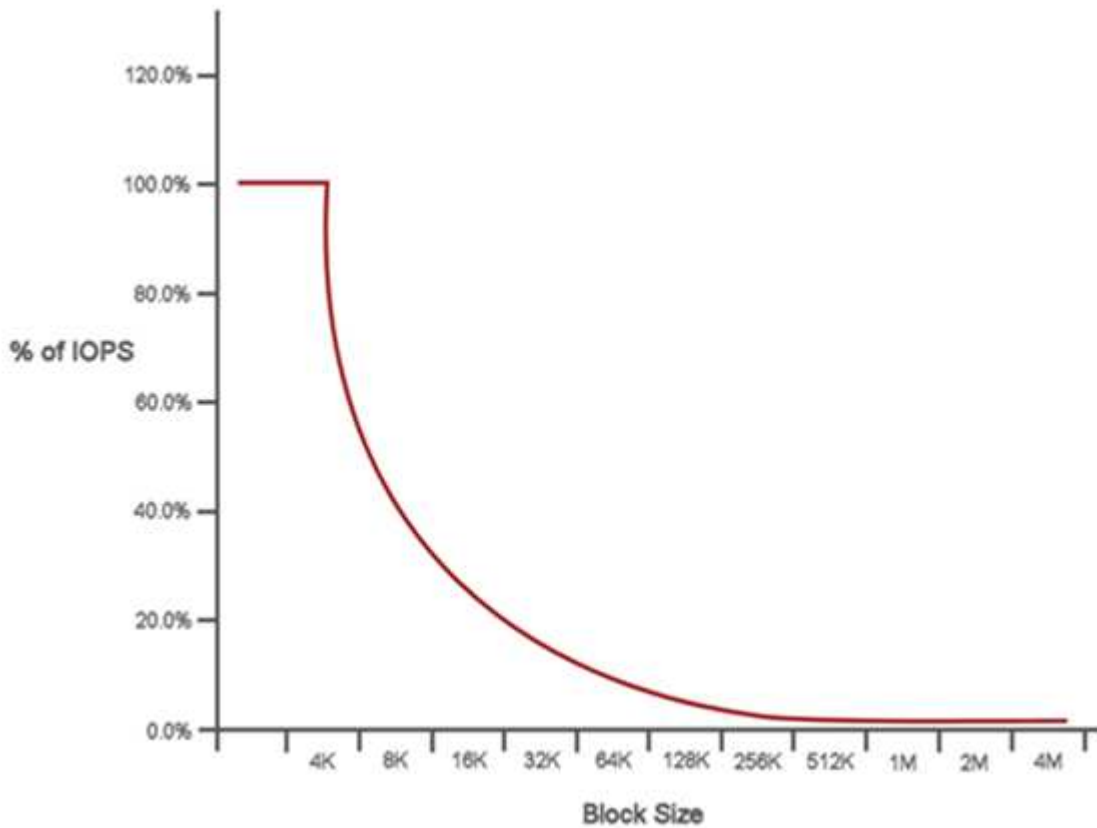
*Estas estimaciones son aproximadas. **Max IOPS y Burst IOPS se pueden establecer con un valor máximo de 200,000 000; sin embargo, este valor solo se permite para destacar de forma efectiva el rendimiento de un volumen. El rendimiento máximo en el mundo real de un volumen está limitado por el uso del clúster y el rendimiento por cada nodo.

Rendimiento de la calidad de servicio

La curva de rendimiento de calidad de servicio muestra la relación entre el tamaño de bloque y el porcentaje de IOPS.

El tamaño de bloque y el ancho de banda repercuten directamente en el número de IOPS que puede obtener una aplicación. El software Element toma en cuenta los tamaños de bloque que recibe definiendo de forma general el tamaño de los bloques en 4k. En función de la carga de trabajo, el sistema podría aumentar los tamaños de bloque. A medida que estos aumenten, el sistema aumentará el ancho de banda hasta el nivel que necesite para procesar los tamaños de bloque más grandes. A medida que aumenta el ancho de banda, se reduce el número de IOPS que el sistema es capaz de conseguir.

La curva de rendimiento de calidad de servicio muestra la relación entre el aumento de los tamaños de bloque y el porcentaje de IOPS en disminución:



A modo de ejemplo, si el tamaño de los bloques es de 4k y el ancho de banda es de 4000 kbps, la IOPS será de 1000. Si el tamaño de los bloques aumenta hasta 8k, el ancho de banda aumentará también hasta los 5000 kbps y la IOPS se reducirá hasta 625. Al tener en cuenta el tamaño de bloque, el sistema garantiza que las cargas de trabajo con prioridad más baja que utilizan tamaños de bloque más altos, como backups y actividades del hipervisor, no necesiten demasiado del rendimiento que necesita el tráfico de mayor prioridad utilizando tamaños de bloque más pequeños.

Políticas de calidad de servicio

Una política de calidad de servicio permite crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes.

Las políticas de calidad de servicio son mejores para los entornos de servicio, por ejemplo, con servidores de bases de datos, aplicaciones o infraestructuras que rara vez se reinician y necesitan igual acceso constante al almacenamiento. La calidad de servicio de un volumen individual es la mejor opción para equipos virtuales de uso reducido, como escritorios virtuales o equipos virtuales especializados de tipo quiosco, que pueden reiniciarse, encenderse o apagarse a diario o varias veces al día.

Las políticas de calidad de servicio y calidad de servicio no se deben utilizar juntas. Si utiliza políticas de

calidad de servicio, no use la calidad de servicio personalizada en un volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.



El clúster seleccionado debe ser Element 10.0 o posterior para usar políticas de calidad de servicio; de lo contrario, las funciones de las políticas de calidad de servicio no estarán disponibles.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Requisitos y tareas previas a la implementación

Información general sobre los requisitos para la puesta en marcha de NetApp HCI

NetApp HCI tiene requisitos físicos y de red específicos para que el centro de datos funcione correctamente. Procure aplicar los requisitos y las recomendaciones siguientes antes de iniciar la implementación.

Antes de recibir el hardware de NetApp HCI, asegúrese de completar los elementos de la lista de comprobación en el libro de trabajo previo a la puesta en marcha de los servicios profesionales de NetApp. Este documento contiene una lista completa de tareas que debe completar para preparar la red y el entorno para una puesta en marcha de NetApp HCI correcta.

A continuación encontrará los enlaces a los requisitos y las tareas previas a la implementación:

- ["Requisitos de puerto de red"](#)
- ["Requisitos de switch y red"](#)
- ["Requisitos de cables de red"](#)
- ["Requisitos de dirección IP"](#)
- ["Configuración de red"](#)
- ["Requisitos de DNS y de control del tiempo"](#)
- ["Requisitos ambientales"](#)
- ["Dominios de protección"](#)
- ["Requisitos de recursos de nodo de observación para clústeres de almacenamiento de dos nodos"](#)

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos del nodo de gestión

Como práctica recomendada, solo asocie un nodo de gestión a una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de gestión. Definir los mismos recursos en varios nodos de gestión puede provocar problemas, como la generación de informes de recursos incorrectos en Active IQ de NetApp.

Requisitos de puerto de red

Es posible que deba permitir los siguientes puertos a través del firewall perimetral del centro de datos para poder gestionar el sistema de forma remota, permitir que los clientes fuera del centro de datos se conecten a los recursos y asegurarse de que los

servicios internos funcionen correctamente. En función de la forma en la que se utilice el sistema, es posible que no sean necesarios algunos puertos, direcciones URL o direcciones IP.

Todos los puertos son TCP a menos que se especifique lo contrario, y todos los puertos TCP deben admitir la comunicación de apretón de manos tripartito entre el servidor de soporte de NetApp, el nodo de gestión y los nodos que ejecutan el software Element. Por ejemplo, el host de un origen del nodo de gestión se comunica con el host en un destino de MVIP del clúster de almacenamiento a través del puerto TCP 443, y el host de destino se vuelve a comunicar al host de origen a través de cualquier puerto.

En la tabla se emplean las siguientes abreviaturas:

- MIP: Dirección IP de gestión, una dirección por nodo
- SIP: Dirección IP de almacenamiento, una dirección por nodo
- MVIP: Dirección IP virtual de gestión
- SVIP: Dirección IP virtual de almacenamiento

Origen	Destino	Puerto	Descripción
Nodo de computación BMC/IPMI	Nodo de gestión	111 TCP/UDP	Comunicación de la API de control de cloud híbrido de NetApp
Nodo de computación BMC/IPMI	Nodo de gestión	137-138 UDP	Comunicación de la API de control de cloud híbrido de NetApp
Nodo de computación BMC/IPMI	Nodo de gestión	445	Comunicación de la API de control de cloud híbrido de NetApp
Nodo de computación BMC/IPMI	Nodo de gestión	623 UDP	Puerto del Protocolo de control de administración remota (RMCP). Necesario para las actualizaciones de firmware de la computación de control de cloud híbrido de NetApp.
Nodo de computación BMC/IPMI	Nodo de gestión	2049 TCP/UDP	Comunicación de la API de control de cloud híbrido de NetApp
Clientes iSCSI	MVIP de clúster de almacenamiento	443	Acceso de interfaz de usuario y API (opcional)
Clientes iSCSI	SVIP de clúster de almacenamiento	3260	Comunicaciones de cliente iSCSI
Clientes iSCSI	SIP de nodo de almacenamiento	3260	Comunicaciones de cliente iSCSI
Nodo de gestión	<code>sfsupport.solidfire.com</code>	22	Túnel SSH inverso para acceso al soporte

Origen	Destino	Puerto	Descripción
Nodo de gestión	MIP de nodo de almacenamiento	22	Acceso SSH para soporte
Nodo de gestión	Servidores DNS	53 TCP/UDP	Búsqueda de DNS
Nodo de gestión	Nodo de computación BMC/IPMI	139	Comunicación de la API de control de cloud híbrido de NetApp
Nodo de gestión	MIP de nodo de almacenamiento	442	Acceso de interfaz de usuario y de API al nodo de almacenamiento y actualizaciones del software Element
Nodo de gestión	MVIP de nodo de almacenamiento	442	Acceso de interfaz de usuario y de API al nodo de almacenamiento y actualizaciones del software Element
Nodo de gestión	23.32.54.122, 216.240.21.15	443	Actualizaciones del software Element
Nodo de gestión	Controlador de administración en placa base (BMC)	443	Supervisión de hardware y conexión de inventario (comandos Redfish e IPMI)
Nodo de gestión	Nodo de computación BMC/IPMI	443	Comunicación HTTPS de control del cloud híbrido de NetApp
Nodo de gestión	monitoring.solidfire.com	443	Informes del clúster de almacenamiento a Active IQ
Nodo de gestión	MVIP de clúster de almacenamiento	443	Acceso de interfaz de usuario y de API al nodo de almacenamiento y actualizaciones del software Element
Nodo de gestión	VMware vCenter	443	Comunicación HTTPS de control del cloud híbrido de NetApp
Nodo de gestión	Nodo de computación BMC/IPMI	623 UDP	Puerto del Protocolo de control de administración remota (RMCP). Necesario para las actualizaciones de firmware de la computación de control de cloud híbrido de NetApp.

Origen	Destino	Puerto	Descripción
Nodo de gestión	BMC/IPMI de nodo de almacenamiento	623 UDP	Puerto RMCP. Esto es necesario para gestionar los sistemas habilitados para IPMI.
Nodo de gestión	VMware vCenter	5988-5989	Comunicación HTTPS de control del cloud híbrido de NetApp
Nodo de gestión	Nodo de testimonio	9442	Servicio API de configuración por nodo
Nodo de gestión	VCenter Server	9443	Registro del plugin de vCenter; El puerto se puede cerrar una vez que se completa el registro.
Servidor SNMP	MVIP de clúster de almacenamiento	161 UDP	Sondeo de SNMP
Servidor SNMP	MIP de nodo de almacenamiento	161 UDP	Sondeo de SNMP
BMC/IPMI de nodo de almacenamiento	Nodo de gestión	623 UDP	Puerto RMCP. Esto es necesario para gestionar los sistemas habilitados para IPMI.
MIP de nodo de almacenamiento	Servidores DNS	53 TCP/UDP	Búsqueda de DNS
MIP de nodo de almacenamiento	Nodo de gestión	80	Actualizaciones del software Element
MIP de nodo de almacenamiento	Extremo de S3/Swift	80	Comunicación HTTP con el extremo de S3/Swift para backup y recuperación (opcional)
MIP de nodo de almacenamiento	Servidor NTP	123 UDP	NTP
MIP de nodo de almacenamiento	Nodo de gestión	162 UDP	(Opcional) capturas SNMP
MIP de nodo de almacenamiento	Servidor SNMP	162 UDP	(Opcional) capturas SNMP
MIP de nodo de almacenamiento	Servidor LDAP	389 TCP/UDP	Búsqueda de LDAP (opcional)
MIP de nodo de almacenamiento	Nodo de gestión	443	Actualizaciones del software Element
MIP de nodo de almacenamiento	MVIP de clúster de almacenamiento remoto	443	Comunicación de emparejamiento de clústeres de replicación remota

Origen	Destino	Puerto	Descripción
MIP de nodo de almacenamiento	MIP de nodo de almacenamiento remoto	443	Comunicación de emparejamiento de clústeres de replicación remota
MIP de nodo de almacenamiento	Extremo de S3/Swift	443	Comunicación HTTPS con el extremo de S3/Swift para backup y recuperación (opcional)
MIP de nodo de almacenamiento	Servidor LDAPS	636 TCP/UDP	Búsqueda LDAPS
MIP de nodo de almacenamiento	Nodo de gestión	10514 TCP/UDP, 514 TCP/UDP	Reenvío de syslog
MIP de nodo de almacenamiento	Servidor de syslog	10514 TCP/UDP, 514 TCP/UDP	Reenvío de syslog
MIP de nodo de almacenamiento	MIP de nodo de almacenamiento remoto	2181	Comunicación entre clústeres para replicación remota
SIP de nodo de almacenamiento	Extremo de S3/Swift	80	Comunicación HTTP con el extremo de S3/Swift para backup y recuperación (opcional)
SIP de nodo de almacenamiento	SIP de nodo de computación	442	API del nodo de computación, configuración y validación y acceso al inventario de software
SIP de nodo de almacenamiento	Extremo de S3/Swift	443	Comunicación HTTPS con el extremo de S3/Swift para backup y recuperación (opcional)
SIP de nodo de almacenamiento	SIP de nodo de almacenamiento remoto	2181	Comunicación entre clústeres para replicación remota
SIP de nodo de almacenamiento	SIP de nodo de almacenamiento	3260	iSCSI entre nodos
SIP de nodo de almacenamiento	SIP de nodo de almacenamiento remoto	4000 hasta 4020	Transferencia de datos nodo a nodo con replicación remota
PC del administrador de sistemas	MIP de nodo de almacenamiento	80	(Solo NetApp HCI) Página de inicio del motor de implementación de NetApp
PC del administrador de sistemas	Nodo de gestión	442	Acceso de interfaz de usuario de HTTPS a nodo de gestión

Origen	Destino	Puerto	Descripción
PC del administrador de sistemas	MIP de nodo de almacenamiento	442	Acceso de API e interfaz de usuario de HTTPS a nodo de almacenamiento, (solo NetApp HCI) Supervisión de configuración y de implementación en el motor de implementación de NetApp
PC del administrador de sistemas	Nodos de computación de las series BMC/IPMI H410 y H600	443	Acceso de API e interfaz de usuario de HTTPS a control remoto de nodos
PC del administrador de sistemas	Nodo de gestión	443	Acceso HTTPS de interfaz de usuario y API al nodo de gestión
PC del administrador de sistemas	MVIP de clúster de almacenamiento	443	Acceso de API e interfaz de usuario de HTTPS a clúster de almacenamiento
PC del administrador de sistemas	Nodos de almacenamiento series BMC/IPMI H410 y H600	443	Acceso de API e interfaz de usuario de HTTPS a control remoto de nodos
PC del administrador de sistemas	MIP de nodo de almacenamiento	443	Creación de clúster de almacenamiento de HTTPS, acceso de interfaz de usuario al clúster de almacenamiento posterior a la implementación
PC del administrador de sistemas	Nodos de computación de las series BMC/IPMI H410 y H600	623 UDP	Puerto RMCP. Esto es necesario para gestionar los sistemas habilitados para IPMI.
PC del administrador de sistemas	Nodos de almacenamiento series BMC/IPMI H410 y H600	623 UDP	Puerto RMCP. Esto es necesario para gestionar los sistemas habilitados para IPMI.
PC del administrador de sistemas	Nodo de testimonio	8080	Interfaz de usuario web de un nodo de testigos por nodo
VCenter Server	MVIP de clúster de almacenamiento	443	Acceso de API de plugin de vCenter
VCenter Server	Plugin remoto	8333	Servicio de complemento de vCenter remoto

Origen	Destino	Puerto	Descripción
VCenter Server	Nodo de gestión	8443	Servicio QoSSIOC del plugin de vCenter (opcional);
VCenter Server	MVIP de clúster de almacenamiento	8444	Acceso del proveedor VASA de vCenter (solo VVol)
VCenter Server	Nodo de gestión	9443	Registro del plugin de vCenter; El puerto se puede cerrar una vez que se completa el registro.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos de switch y red

Los switches que usa para NetApp HCI requieren una configuración específica para garantizar una implementación correcta. Consulte la documentación de su switch para ver instrucciones específicas sobre cómo implementar cada uno de los requisitos siguientes para su entorno.

Una implementación de NetApp HCI requiere al menos tres segmentos de red, uno para cada tipo de tráfico a continuación:

- Gestión
- VMware vMotion
- Almacenamiento/datos

Según los modelos de nodos de almacenamiento y computación de NetApp H-Series, y la configuración de cableado planificada, estas redes se pueden separar mediante switches distintos, o bien mediante VLAN. Para la mayoría de las implementaciones, sin embargo, es necesario separar lógicamente estas redes (y cualquier otra red de máquina virtual adicional) mediante VLAN.

Los nodos de computación y de almacenamiento deben ser capaces de comunicarse antes, durante y después de la implementación. Si va a implementar redes de gestión independientes para los nodos de computación y de almacenamiento, asegúrese de que estas redes de gestión tengan rutas de red entre ellas. Estas redes deben tener puertas de enlace asignadas, y debe existir una ruta entre las puertas de enlace. Asegúrese de que cada nodo nuevo tenga asignada una puerta de enlace para facilitar la comunicación entre nodos y redes de gestión.

NetApp HCI tiene los siguientes requisitos de switch:

- Todos los puertos de switch conectados a los nodos NetApp HCI deben estar configurados como puertos periféricos de árbol de expansión.
 - En los switches Cisco, en función del modelo del switch, la versión del software y el tipo de puerto, puede hacerlo con uno de los siguientes comandos:

- `spanning-tree port type edge`
- `spanning-tree port type edge trunk`
- `spanning-tree portfast`
- `spanning-tree portfast trunk`

◦ En los switches Mellanox, puede hacerlo con `spanning-tree port type edge` comando.

- Los nodos NetApp HCI tienen puertos redundantes para todas las funciones de red, excepto la gestión fuera de banda. Para obtener la mejor resiliencia, divida estos puertos entre dos switches con vínculos superiores redundantes ya sea a una arquitectura jerárquica tradicional o una arquitectura tipo espina de capa 2.
- Los switches que controlan el tráfico de almacenamiento, máquinas virtuales y vMotion deben admitir velocidades de al menos 10 GbE por puerto (se admiten hasta 25 GbE por puerto).
- Los switches que controlan el tráfico de gestión deben admitir velocidades de al menos 1 GbE por puerto.
- Debe configurar tramas gigantes en los puertos del switch que controla el tráfico de vMotion y almacenamiento. Los hosts deben poder enviar paquetes de 9000 bytes de extremo a extremo para una instalación correcta.
- Es necesario configurar los puertos del switch de red de gestión para permitir el tamaño MTU para el que estén configurados los puertos NIC de gestión en cada host. Por ejemplo, si los puertos de red de gestión de host utilizan un tamaño de MTU de 1750 bytes, deben configurarse los puertos del switch de red de gestión para permitir un mínimo de 1750 bytes (la red de gestión no requiere un MTU de 9000 bytes). La configuración de MTU debe ser coherente de extremo a extremo.
- La latencia de red de ida y vuelta entre todos los nodos de computación y almacenamiento no debe exceder los 2 ms.

Todos los nodos NetApp HCI proporcionan funcionalidades de gestión fuera de banda adicionales a través de un puerto de gestión dedicado. NETAPP H300S, H300E, H500S, H500E, H700S, Los nodos H700E y H410C también permiten el acceso de IPMI a través del puerto A. Como práctica recomendada, debe facilitar la gestión remota de NetApp HCI mediante la configuración de la gestión fuera de banda para todos los nodos del entorno.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos de cables de red

Puede utilizar las siguientes pautas para asegurarse de contar con la cantidad suficiente del tipo correcto de cables de red según el tamaño de la implementación. Para los puertos RJ45, debe usar cables con clasificación Cat 5e o Cat 6.

- Configuración de nodos de computación de dos cables: Cada nodo de computación debe estar conectado a una red de 10 GbE a través de dos interfaces SFP+/SFP28 (un cable Cat 5e/6 adicional es opcional para la gestión fuera de banda).
- Configuración de nodos de computación de seis cables: Cada nodo de computación debe estar conectado a una red de 10/25 GbE a través de cuatro interfaces SFP+/SFP28 y a una red de 10 GbE a través de dos cables Cat 5e/6 (un cable Cat 5e/6 adicional es opcional para la gestión fuera de banda).

- Cada nodo de almacenamiento debe estar conectado a una red de 10/25 GbE a través de dos interfaces SFP+/SFP28 y a una red de 10 GbE a través de dos cables Cat 5e/6 (un cable Cat 5e/6 adicional es opcional para la gestión fuera de banda).
- Asegúrese de que los cables de red que utiliza para conectar el sistema NetApp HCI a la red sean lo suficientemente largos como para llegar cómodamente a los switches.

Por ejemplo, una implementación que contiene cuatro nodos de almacenamiento y tres nodos de computación (con la configuración de seis cables) requiere la siguiente cantidad de cables de red:

- (14) cables Cat 5e/6 con conectores RJ45 (más siete cables para tráfico IPMI si se desea)
- (20) cables Twinax con conectores SFP28/SFP+

Esto se debe a las siguientes razones:

- Cuatro nodos de almacenamiento requieren ocho (8) cables Cat 5e/6 y ocho (8) cables Twinax.
- Tres nodos de computación que utilizan una configuración de seis cables requieren seis (6) cables Cat 5e/6 y doce (12) cables Twinax.



En una configuración de seis cables, se reservan dos puertos para VMware ESXi y los configura y gestiona el motor de puesta en marcha de NetApp. No es posible acceder a estos puertos ESXi dedicados ni gestionarlos mediante la TUI de Element o la interfaz gráfica de usuario web de Element.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos de dirección IP

NetApp HCI tiene requisitos de dirección IP específicos que dependen del tamaño de la implementación. Tenga en cuenta que, de forma predeterminada, las direcciones IP que se asignan a cada nodo antes de utilizar el motor de implementación de NetApp para implementar el sistema son temporales y no se pueden reutilizar. Debe separar un segundo conjunto permanente de direcciones IP sin usar que se puedan asignar durante la implementación final.

Número de direcciones IP necesarias por implementación de NetApp HCI

La red de almacenamiento y de gestión de NetApp HCI deben utilizar distintos rangos contiguos de direcciones IP. Utilice la siguiente tabla para determinar cuántas direcciones IP se necesitan en la implementación:

Componente del sistema	Se requieren direcciones IP de red de gestión	Direcciones IP de red de almacenamiento requeridas	Direcciones IP de red de vMotion requeridas	Total de direcciones IP requeridas por componente
Nodo de computación	1	2	1	4

Componente del sistema	Se requieren direcciones IP de red de gestión	Direcciones IP de red de almacenamiento requeridas	Direcciones IP de red de vMotion requeridas	Total de direcciones IP requeridas por componente
Nodo de almacenamiento	1	1		2
Clúster de almacenamiento	1	1		2
VMware vCenter	1			1
Nodo de gestión	1	1		2
Nodo de testimonio	1	1		2 por nodo testigo (se ponen en marcha dos nodos testigos para cada clúster de almacenamiento de dos o tres nodos)

Direcciones IP reservadas por NetApp HCI

NetApp HCI se reserva los siguientes rangos de direcciones IP para los componentes del sistema. Cuando planifique la red, evite el uso de estas direcciones IP:

Rango de direcciones IP	Descripción
10.0.0.0/24	Red de superposición de Docker
10.0.1.0/24	Red de superposición de Docker
10.255.0.0/16	Red de entrada de Docker Swarm/Datacenter
169.254.100.1/22	Red puente Docker
169.254.104.0/22	Red puente Docker

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configuración de red

Configuración de red

NetApp HCI puede utilizar varias configuraciones de VLAN y cableado de red distintas. Es importante planificar la configuración de red para garantizar una correcta implementación.

Segmentos de red requeridos

NetApp HCI requiere tres segmentos de red como mínimo: Tráfico de gestión, almacenamiento y virtualización (que incluye máquinas virtuales y tráfico de vMotion de VMware). También es posible separar el tráfico de la máquina virtual y de vMotion. Estos segmentos de red, en general, existen como VLAN separadas en la infraestructura de red de NetApp HCI.

El modo en que los nodos de computación y almacenamiento se conectan a estas redes depende de cómo se diseñan y se cablean los nodos. Las ilustraciones de red de ejemplo incluidas en esta guía suponen las siguientes redes:

Nombre de la red	ID DE VLAN
Gestión	100
Reducida	105
vMotion	107
Equipos virtuales	200, 201

Para la detección y configuración automática de los nodos NetApp HCI en el motor de implementación de NetApp, debe tener un segmento de red que esté disponible como VLAN sin etiquetas o nativa en todos los puertos del switch que se utilizan para las interfaces SFP+/SFP28 de los nodos. De este modo, se proporcionará comunicación de capa 2 entre todos los nodos para su detección y puesta en marcha. Sin una VLAN nativa, debe configurar las interfaces SFP+/SFP28 de todos los nodos manualmente con una dirección VLAN y IPv4 para que se puedan detectar. En los ejemplos de configuración de red de este documento, la red de gestión (VLAN ID 100) se utiliza con este propósito.

El motor de implementación de NetApp permite configurar rápidamente las redes para los nodos de computación y almacenamiento durante la implementación inicial. Puede colocar algunos componentes de gestión incorporados, como vCenter y el nodo de gestión, en su propio segmento de red. Estos segmentos de red requieren enrutamiento para permitir que vCenter y el nodo de gestión se comuniquen con las redes de gestión de almacenamiento y computación. En la mayoría de las implementaciones, esos componentes utilizan la misma red de gestión (ID de VLAN 100 en este ejemplo).



Las redes de máquina virtual se configuran con vCenter. La red de máquina virtual predeterminada (grupo de puertos "VM_Network") en las implementaciones de NetApp HCI se configura sin un identificador de VLAN. Si planea utilizar varias redes de máquina virtual etiquetadas (VLAN 200 y 201 en el ejemplo anterior), asegúrese de incluirlas en la planificación de red inicial.

Opciones de configuración y cableado de red

Se puede usar una configuración de red de dos cables para los nodos de computación H410C, lo cual simplifica el enrutamiento de los cables. Esta configuración utiliza dos interfaces SFP+/SFP28 más una interfaz RJ45 opcional para la comunicación IPMI. Estos nodos también pueden usar una configuración de seis cables con dos interfaces RJ45 y cuatro SFP28/SFP+.

Los nodos de almacenamiento H410S y H610S admiten una topología de red que utiliza cuatro puertos de red (puertos A a D).

Los nodos de computación admiten tres topologías de red, según la plataforma de hardware:

Opción de configuración	Cableado para nodos H410C	Cableado para nodos H610C	Cableado para nodos H615C
Opción A	Dos cables con los puertos D y E	Dos cables con los puertos C y D	Dos cables que utilizan los puertos A y B
Opción B	Seis cables con los puertos A a F	No disponible	No disponible
Opción C	Similar a la opción B, pero con VLAN nativas (o "puertos de acceso") en el switch para las redes de gestión, almacenamiento y vMotion		

Los nodos que no tienen el número correcto de cables conectados no pueden participar en la implementación. Por ejemplo, no se puede implementar un nodo de computación en una configuración de seis cables si solo tiene conectados los puertos D y E.



Es posible ajustar la configuración de red NetApp HCI después de la implementación para satisfacer las necesidades de infraestructura. Sin embargo, al ampliar los recursos de NetApp HCI, recuerde que los nodos nuevos deben tener la misma configuración de cables que los nodos de computación y de almacenamiento existentes.

Si el motor de puesta en marcha de NetApp falla porque su red no admite tramas gigantes, puede realizar una de las siguientes soluciones alternativas:



- Use una dirección IP estática y establezca manualmente una unidad de transmisión máxima (MTU) de 9000 bytes en la red Bond10G.
- Configure el Protocolo de configuración dinámica de host para anunciar una MTU de interfaz de 9000 bytes en la red Bond10G.

Opciones de configuración de red

- ["Opción de configuración de red A"](#)
- ["Opción de configuración de red B"](#)
- ["Opción de configuración de red C"](#)

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configuración de red

NetApp HCI puede utilizar varias configuraciones de VLAN y cableado de red distintas. La primera configuración, la opción A, utiliza dos cables de red para cada nodo de computación.

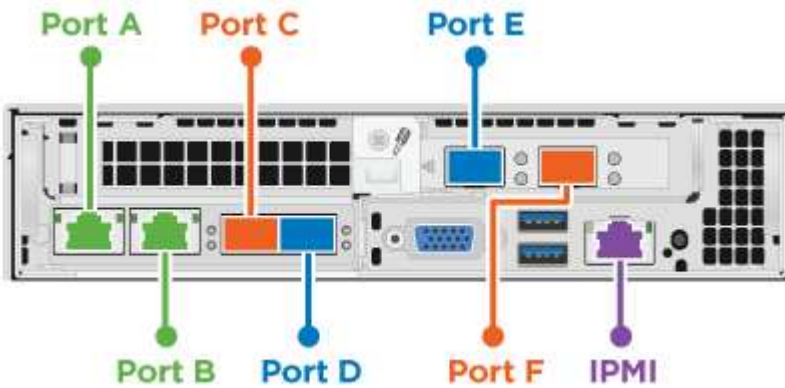
Opción de configuración A: Dos cables para nodos de computación

Los nodos de computación NetApp H410C, H610C y H615C admiten el uso de dos cables de red para conectividad a todas las redes NetApp HCI. Esta configuración requiere que las redes de almacenamiento, vMotion y máquina virtual utilicen el etiquetado de VLAN. Todos los nodos de computación y de almacenamiento deben usar el mismo esquema de ID de VLAN. Esta configuración utiliza switches

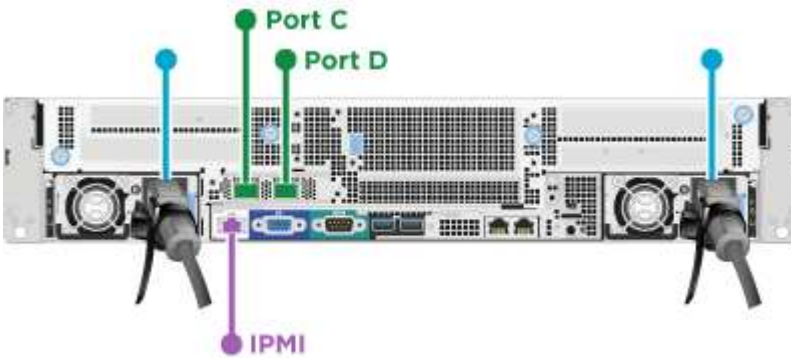
distribuidos de vSphere que requieren licencia VMware vSphere Enterprise Plus.

La documentación de NetApp HCI utiliza letras para hacer referencia a los puertos de red en el panel posterior de los nodos H-Series.

Aquí se muestran los puertos de red y las ubicaciones en el nodo de almacenamiento H410C:



Aquí están los puertos de red y las ubicaciones en el nodo de computación H610C:



A continuación, se muestran los puertos de red y las ubicaciones en el nodo de computación H615C:



Esta configuración utiliza los siguientes puertos de red en cada nodo:

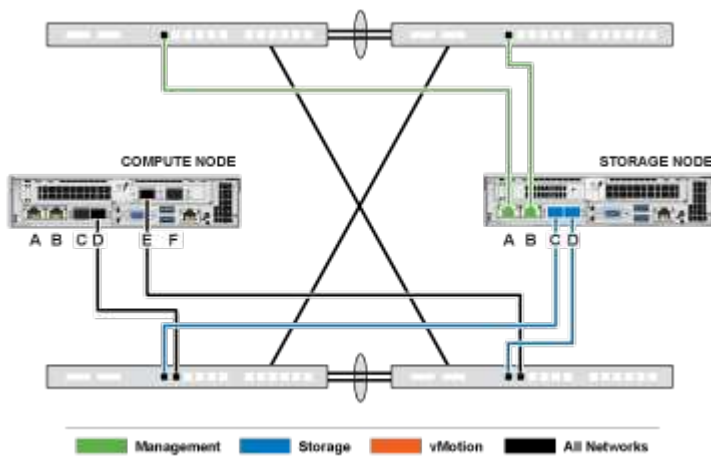
Nodo	Puertos de red utilizados
H410C	D y E
H610C	C y D
H615C	A y B

Configuración de VLAN

Una práctica recomendada es configurar los segmentos de red necesarios en todos los puertos del switch que usen los nodos. Por ejemplo:

Nombre de la red	ID DE VLAN	Configuración de puertos del switch
Gestión	100	Nativo
Reducida	105	Etiquetada
VMotion	107	Etiquetada
Equipos virtuales	200, 201	Etiquetada

En la siguiente ilustración, se muestra la configuración de cableado recomendada para los nodos de computación H410C de dos cables y los nodos de almacenamiento H410S de cuatro cables. Todos los puertos del switch de este ejemplo comparten la misma configuración.



Comandos del switch de ejemplo

Es posible usar los siguientes comandos de ejemplo a fin de configurar todos los puertos del switch utilizados para los nodos de NetApp HCI. Estos comandos se basan en una configuración de Cisco, pero podrían requerir únicamente pequeños cambios para aplicarlos a los switches Mellanox. Consulte en la documentación de su switch los comandos específicos que necesita para implementar esta configuración. Reemplace el nombre de la interfaz, la descripción y las VLAN por los valores para su entorno.

```
interface {interface name, such as EthernetX/Y or GigabitEthernetX/Y/Z}
description {desired description, such as NetApp-HCI-NodeX-PortY}
mtu 9216
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 105,107,200,201
spanning-tree port type edge trunk
```



Algunos switches pueden requerir la inclusión de la VLAN nativa en la lista de VLAN permitidas. Consulte la documentación de su modelo de switch y versión de software específicos.

Obtenga más información

- "Recursos de NetApp HCI"
- "Plugin de NetApp Element para vCenter Server"

Configuración de red

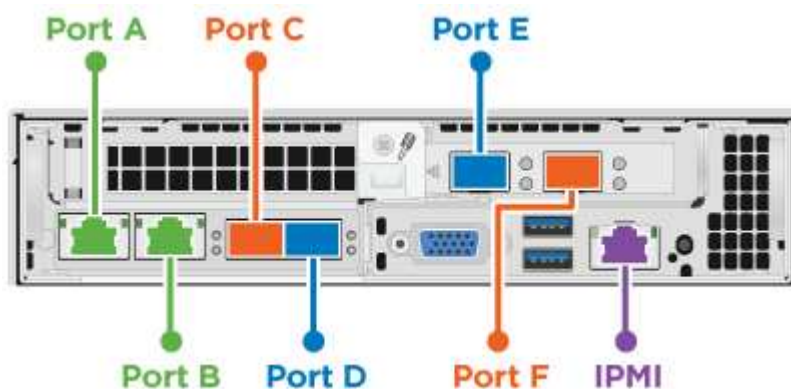
NetApp HCI puede utilizar varias configuraciones de VLAN y cableado de red distintas. La primera configuración, la opción B, utiliza seis cables de red para cada nodo de computación.

Opción de configuración B: Seis cables para nodos de computación

Como una opción de configuración de red secundaria, los nodos de computación H410C admiten el uso de seis cables de red para la conectividad a todas las redes NetApp HCI. Esta configuración requiere que las redes de almacenamiento, vMotion y máquina virtual utilicen el etiquetado de VLAN. Se puede usar esta configuración con switches estándar de vSphere o switches distribuidos de vSphere (que requieren licencia de VMware vSphere Enterprise Plus).

La documentación de NetApp HCI utiliza letras para hacer referencia a los puertos de red en el panel posterior de los nodos H-Series.

Aquí se muestran los puertos de red y las ubicaciones del nodo de computación H410C:

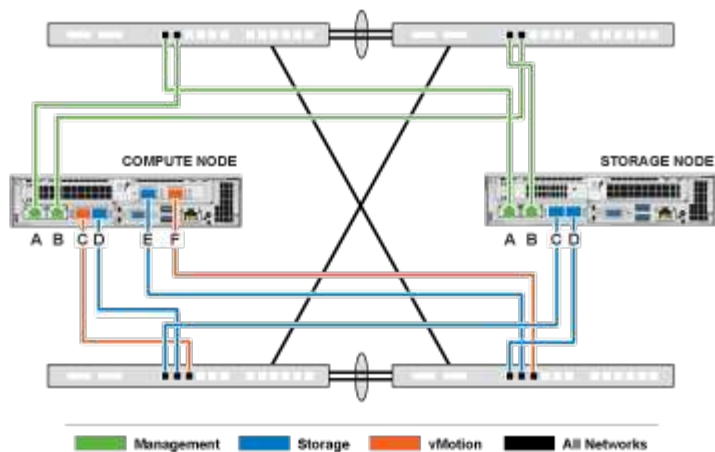


Configuración de VLAN

Cuando se implementan los nodos de computación mediante seis cables y los nodos de almacenamiento mediante cuatro cables, una práctica recomendada es configurar los segmentos de red necesarios en todos los puertos del switch que usen los nodos. Por ejemplo:

Nombre de la red	ID DE VLAN	Configuración de puertos del switch
Gestión	100	Nativo
Reducida	105	Etiquetada
VMotion	107	Etiquetada
Equipos virtuales	200, 201	Etiquetada

En la siguiente ilustración, se muestra la configuración de cableado recomendada para los nodos de computación de seis cables y los nodos de almacenamiento de cuatro cables. Todos los puertos del switch de este ejemplo comparten la misma configuración.



Comandos del switch de ejemplo

Es posible usar los siguientes comandos de ejemplo a fin de configurar todos los puertos del switch utilizados para los nodos de NetApp HCI. Estos comandos se basan en una configuración de Cisco, pero podrían requerir únicamente pequeños cambios para aplicarlos a los switches Mellanox. Consulte en la documentación de su switch los comandos específicos que necesita para implementar esta configuración. Reemplace el nombre de la interfaz, la descripción y las VLAN por los valores para su entorno.

```
interface {interface name, such as EthernetX/Y or GigabitEthernetX/Y/Z}
description {desired description, such as NetApp-HCI-NodeX-PortY}
mtu 9216
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 105,107,200,201
spanning-tree port type edge trunk
```



Algunos switches pueden requerir la inclusión de la VLAN nativa en la lista de VLAN permitidas. Consulte la documentación de su modelo de switch y versión de software específicos.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configuración de red

NetApp HCI puede utilizar varias configuraciones de VLAN y cableado de red distintas. La tercera configuración, la opción C, utiliza seis cables de red para cada nodo de computación con VLAN nativas.

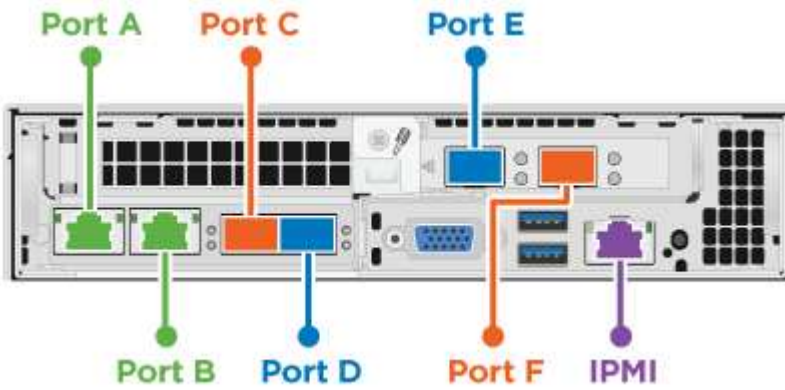
Opción de configuración C: Seis cables para nodos de computación con VLAN nativas

Es posible implementar NetApp HCI sin utilizar VLAN etiquetadas para el tráfico de almacenamiento y virtualización y, en su lugar, basarse en la configuración del switch para separar los segmentos de red. Se puede usar esta configuración con switches estándar de vSphere o switches distribuidos de vSphere (que requieren licencia de VMware vSphere Enterprise Plus).

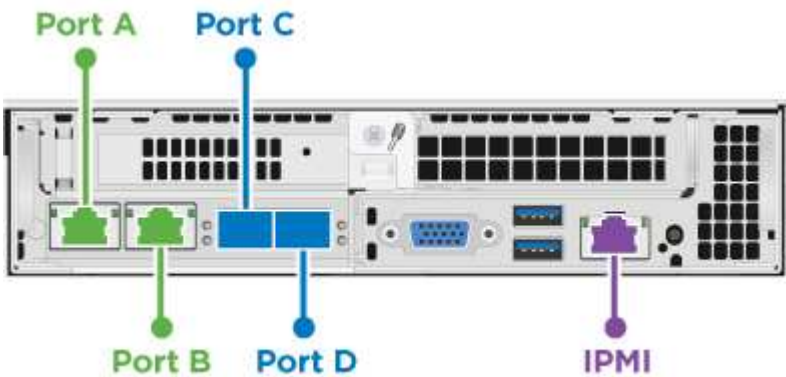
La documentación de NetApp HCI utiliza letras para hacer referencia a los puertos de red en el panel posterior

de los nodos H-Series.

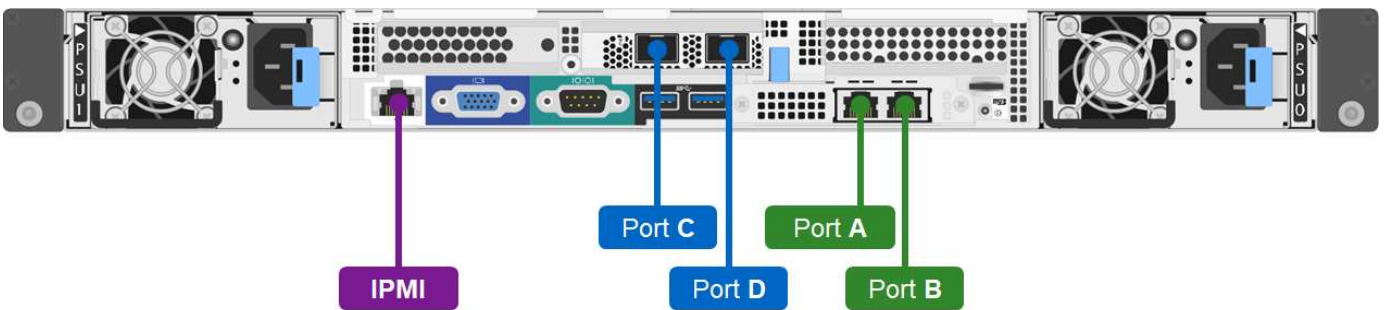
Aquí se muestran los puertos de red y las ubicaciones en el nodo de almacenamiento H410C:



A continuación, se muestran los puertos de red y las ubicaciones en el nodo de almacenamiento H410S:



A continuación, se muestran los puertos de red y las ubicaciones del nodo de almacenamiento H610S:



Configuración de VLAN para nodos H410C, H410S y H610S

Esta opción de topología utiliza la siguiente configuración de VLAN en nodos H410C, H410S y H610S:

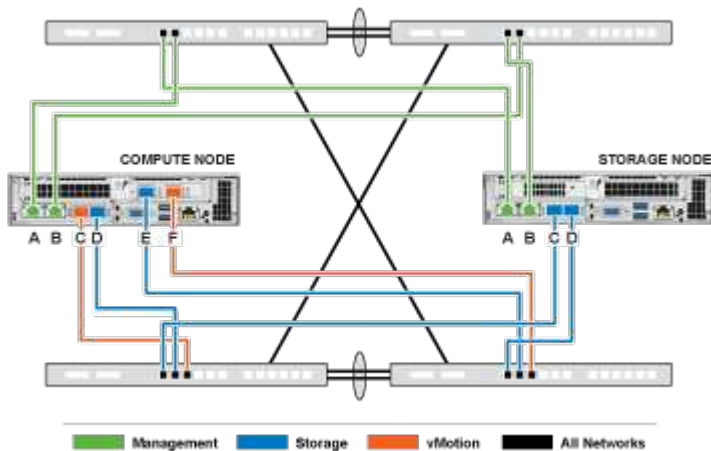
Puertos de nodo utilizados	Nombre de la red	ID DE VLAN	Configuración de puertos del switch conectados
Puertos A y B en nodos de computación y de almacenamiento	Gestión	100	Nativo

Puertos de nodo utilizados	Nombre de la red	ID DE VLAN	Configuración de puertos del switch conectados
Puertos D y E en nodos de computación	Reducida	105	Nativo
Puertos C y D en nodos de almacenamiento	Reducida	105	Nativo
Puertos C y F en nodos de computación	VMotion	107	Nativo
Puertos C y F en nodos de computación	Equipos virtuales	200, 201	Etiquetada



Tenga cuidado al configurar los puertos del switch al implementar esta configuración. Los errores de configuración en esta topología de red pueden provocar problemas de implementación difíciles de diagnosticar.

En la siguiente ilustración, se muestra información general de la configuración de red para esta opción de topología. En el ejemplo, los puertos del switch individuales se configuraron con un segmento de red apropiado como la red nativa.



Comandos del switch de ejemplo

Es posible usar los siguientes comandos del switch de ejemplo a fin de configurar los puertos del switch utilizados para los nodos de NetApp HCI. Estos comandos se basan en una configuración de Cisco, pero podrían requerir cambios mínimos para aplicarse a los switches Mellanox. Consulte en la documentación de su switch los comandos específicos que necesita para implementar esta configuración.

Es posible usar los siguientes comandos de ejemplo a fin de configurar los puertos del switch utilizados para la red de gestión. Reemplace el nombre de la interfaz, la descripción y las VLAN por los valores para su configuración.

```
switchport access vlan 100
spanning-tree port type edge
```

Es posible usar los siguientes comandos de ejemplo a fin de configurar los puertos del switch utilizados para la red de almacenamiento. Reemplace el nombre de la interfaz, la descripción y las VLAN por los valores para

su configuración.

```
mtu 9216
switchport access vlan 105
spanning-tree port type edge
```

Es posible usar los siguientes comandos de ejemplo a fin de configurar los puertos del switch utilizados para la red de máquinas virtuales y de vMotion. Reemplace el nombre de la interfaz, la descripción y las VLAN por los valores para su configuración.

```
interface {interface name, such as EthernetX/Y or GigabitEthernetX/Y/Z}
description {desired description, such as NetApp-HCI-NodeX-PortC|F}
mtu 9216
switchport mode trunk
switchport trunk native vlan 107
switchport trunk allowed vlan 200,201
spanning-tree port type edge trunk
```



Algunos switches pueden requerir la inclusión de la VLAN nativa en la lista de VLAN permitidas. Consulte la documentación de su modelo de switch y versión de software específicos.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos de DNS y de control del tiempo

Antes de la implementación, debe preparar registros del sistema de nombres de dominio (DNS) para el sistema NetApp HCI y recopilar información del servidor NTP. NetApp HCI requiere un servidor DNS con las entradas DNS correctas y un servidor NTP para conseguir una implementación correcta.

Realice las siguientes preparaciones para el servidor de tiempo y DNS antes de implementar NetApp HCI:

- Cree todas las entradas de DNS necesarias para los hosts (como nodos de computación o almacenamiento individuales) y documente cómo se asignan las entradas de host a las direcciones IP respectivas. Durante la implementación, deberá asignar un prefijo al clúster de almacenamiento que se aplicará a cada host; para evitar confusiones, tenga en cuenta sus planes de nomenclatura de DNS al elegir un prefijo.
- Si va a implementar NetApp HCI con una instalación nueva de VMware vSphere mediante un nombre de dominio completo, debe crear un registro de puntero (PTR) y un registro de dirección (A) para vCenter Server en cualquier servidor DNS que se utilice antes de la implementación.
- Si va a implementar NetApp HCI con una nueva instalación de vSphere usando solo direcciones IP, no es necesario crear nuevos registros de DNS para vCenter.
- NetApp HCI requiere un servidor NTP válido para controlar el tiempo. Se puede usar un servidor de tiempo disponible públicamente si no se dispone de uno en el entorno.
- Compruebe que todos los relojes de nodos de almacenamiento y computación estén sincronizados entre sí y que los relojes de los dispositivos que se utilizan para iniciar sesión en NetApp HCI estén sincronizados con los nodos NetApp HCI.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos ambientales

Compruebe que se suministre alimentación desde los tomas de alimentación de CA al rack utilizado para instalar NetApp HCI, y que el centro de datos proporcione refrigeración adecuada para el tamaño de la instalación de NetApp HCI.

Para obtener capacidades detalladas de cada componente de NetApp HCI, consulte el NetApp HCI ["ficha técnica"](#) .



El nodo de computación H410C solo funciona con tensión de línea alta (200-240 V CA). Debe asegurarse de que se cumplan los requisitos de alimentación cuando añada nodos H410C a una instalación existente de NetApp HCI.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Dominios de protección

Compatibilidad con el software NetApp Element ["dominios de protección"](#) funcionalidad, que optimiza la distribución de datos en nodos de almacenamiento para obtener la mejor disponibilidad de datos. Para usar esta función, debe dividir la capacidad de almacenamiento de manera uniforme en tres o más chasis de NetApp H-Series para una fiabilidad de almacenamiento óptima. En este escenario, el clúster de almacenamiento habilita automáticamente los dominios de protección.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Requisitos de recursos de nodo de observación para clústeres de almacenamiento de dos nodos

NetApp HCI admite un tamaño de instalación mínimo de dos nodos de almacenamiento y dos nodos de computación. Al instalar NetApp HCI mediante un clúster de almacenamiento de dos o tres nodos, debe tener en cuenta los requisitos de los nodos de testigos de NetApp HCI y sus recursos de máquinas virtuales (VM).

Cuando un clúster de almacenamiento utiliza dos o tres nodos, también pone en marcha un par de nodos testigos junto a cada clúster de almacenamiento. Los nodos de observación tienen los siguientes requisitos de

recursos de máquina virtual:

Recurso	Requisito
VCPU	4
Memoria	12 GB
Tamaño de disco	67 GB

NetApp HCI solo admite determinados modelos de nodo de almacenamiento en clústeres de almacenamiento de dos o de tres nodos. Para obtener más información, consulte las notas de la versión de su versión de NetApp HCI.

Mejor práctica: Configurar las VM del nodo testigo para utilizar el almacén de datos local del nodo de computación (establecido por NDE de forma predeterminada), no configurarlas en el almacenamiento compartido, como los volúmenes de almacenamiento SolidFire. Para evitar la migración automática de los equipos virtuales, establezca el nivel de automatización del planificador de recursos distribuidos (DRS) del nodo testigo en **Desactivado**. De este modo, se evita que ambos nodos testigos se ejecuten en el mismo nodo de computación y se cree una configuración de parejas que no sea de alta disponibilidad (ha).



Cuando el proceso de instalación de NetApp HCI instala nodos testigo, se almacena una plantilla de máquina virtual en VMware vCenter que puede utilizar para volver a poner en marcha un nodo de testigo en caso de que se elimine, se pierda o se dañe por accidente. También puede utilizar la plantilla para volver a poner en marcha un nodo de testigo si necesita sustituir un nodo de computación con errores que alojaba el nodo de testigo. Para obtener instrucciones, consulte la sección **nodos de testigo de nueva puesta en marcha para clústeres de almacenamiento de dos y tres nodos** ["aquí"](#).

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)



Su topología de red puede diferir de lo que se muestra aquí. Esto es sólo un ejemplo.

Esta configuración utiliza dos cables de red en los nodos de computación para la conectividad a todas las redes NetApp HCI.

Lea estos recursos:

- Utilice el *Manual de instalación de NetApp HCI* para configurar la red antes de la instalación.
- Para obtener más detalles y otras configuraciones compatibles, consulte "[TR-4820: Guía de planificación rápida de redes de NetApp HCI](#)" y la "[Instrucciones de instalación y configuración de NetApp HCI](#)".
- Para obtener más información sobre las configuraciones de NetApp HCI menores de cuatro nodos de almacenamiento, consulte "[TR-4823: Clúster de almacenamiento de 2 nodos de NetApp HCI](#)".
- Para obtener detalles sobre la configuración del protocolo de control de agregación de enlaces (LACP) en los puertos del switch que se utilizan para cada nodo de almacenamiento, consulte "[Configurar LCAP para obtener un rendimiento óptimo del almacenamiento](#)".

Esta configuración consolida todo el tráfico en dos puertos físicos y redundantes, lo que reduce el cableado y optimiza la configuración de red. Esta configuración requiere que los segmentos de red de almacenamiento, vMotion y máquina virtual utilicen el etiquetado de VLAN. El segmento de red de gestión puede utilizar VLAN nativa o etiquetadas; sin embargo, la VLAN nativa es el modo preferido para que el motor de puesta en marcha de NetApp (NDE) pueda asignar recursos de red de forma automatizada (Zero Conf).

Este modo requiere switches distribuidos de vSphere (VDS), donde se requiere la licencia de VMware vSphere Enterprise Plus.

Requisitos de red antes de comenzar

Aquí están los aspectos más destacados de los requisitos previos.

Para obtener detalles sobre los requisitos previos, consulte "[Información general sobre los requisitos para la puesta en marcha de NetApp HCI](#)".

- Bond1G es una interfaz lógica que combina puertos de red de 1 GbE en nodos de almacenamiento y una interfaz de gestión en nodos de computación. Esta red se utiliza para el tráfico de API NDE. Todos los nodos deben poder comunicarse a través de la interfaz de gestión en la misma red L2.
- Bond10G es una interfaz lógica que combina puertos de 10 GbE y NDE utiliza para la balizas e inventario. Todos los nodos deben ser capaces de comunicarse a través de la interfaz Bond10G con tramas gigantes no fragmentadas.
- Nde requiere como mínimo una dirección IP asignada manualmente en la interfaz de Bond1G en un nodo de almacenamiento. Se ejecutará NDE a partir de este nodo.
- Todos los nodos tendrán direcciones IP temporales asignadas por el descubrimiento de NDE, que se realiza mediante el direccionamiento IP privado automático (APIPA).



Durante el proceso del NDE, a continuación, se asignarán todas las direcciones IP permanentes a todos los nodos y se lanzarán todas las IP temporales asignadas por APIPA.

- Nde requiere redes independientes para gestión, iSCSI y vMotion que están preconfigurados en la red del switch.

Validación de la preparación de la red con Active IQ Config Advisor de NetApp

Para garantizar la preparación de la red para NetApp HCI, instale Active IQ Config Advisor 5.8.1 o posterior de NetApp. Esta herramienta de validación de red se encuentra junto con otra "[Herramientas de soporte de NetApp](#)". Utilice esta herramienta para validar la conectividad, los identificadores de VLAN, los requisitos de dirección IP, la conectividad de switch y mucho más.

Para obtener más información, consulte "[Validar su entorno con Active IQ Config Advisor](#)".

Trabaje con su equipo de NetApp

Su equipo de NetApp usa el informe Active IQ Config Advisor y el *Manual de recuperación* para validar que el entorno de red está listo.

Instale el hardware de NetApp HCI

NetApp HCI puede instalarse con distintas configuraciones:

- Nodos de computación H410C: Configuración de dos cables o configuración de seis cables
- Nodo de computación H610C: Configuración de dos cables
- Nodo de computación H615C: Configuración de dos cables
- Nodo de almacenamiento H410S
- Nodo de almacenamiento H610S



Para conocer las precauciones y los detalles, consulte "[Instale el hardware H-Series](#)".

Pasos

1. Instale los rieles y el chasis.
2. Instale los nodos en el chasis e instale las unidades para los nodos de almacenamiento. (Se aplica solo si se instalan H410C y H410S en un chasis de NetApp H-Series).
3. Instale los interruptores.
4. Cablee el nodo de computación.
5. Cablee el nodo de almacenamiento.
6. Conecte los cables de alimentación.
7. Encienda los nodos NetApp HCI.

Complete tareas opcionales tras instalar el hardware

Después de instalar el hardware de NetApp HCI, debe realizar algunas tareas opcionales y recomendadas.

Gestione la capacidad de almacenamiento en todos los chasis

Asegúrese de que la capacidad de almacenamiento esté dividida uniformemente en todos los chasis que contienen nodos de almacenamiento.

Configure IPMI para cada nodo

Después de haber montado en rack, cableado y encendido el hardware de NetApp HCI, es posible configurar

el acceso de la interfaz de gestión de plataforma inteligente (IPMI) para cada nodo. Asigne una dirección IP a cada puerto IPMI y cambie la contraseña IPMI predeterminada del administrador en cuanto tenga acceso IPMI remoto al nodo.

Consulte "[Configure IPMI](#)".

Puesta en marcha de NetApp HCI con el motor de puesta en marcha de NetApp (NDE)

La interfaz de usuario de NDE es la interfaz del asistente de software que se usa para instalar NetApp HCI.

Inicie la interfaz de usuario de NDE

NetApp HCI utiliza una dirección IPv4 de red de gestión de nodos de almacenamiento para el acceso inicial a NDE. Como práctica recomendada, conéctese desde el primer nodo de almacenamiento.

Requisitos previos

- Ya asignó la dirección IP de red de gestión del nodo de almacenamiento inicial de forma manual o mediante DHCP.
- Debe tener acceso físico a la instalación de NetApp HCI.

Pasos

1. Si no conoce la IP de red de gestión del nodo de almacenamiento inicial, use la interfaz de usuario de terminal (TUI), a la que se accede a través del teclado y monitor en el nodo de almacenamiento o. "[Utilice un dispositivo USB](#)".

Para obtener más información, consulte "[Acceder al motor de puesta en marcha de NetApp](#)".

2. Si conoce la dirección IP, desde un explorador web, conéctese a la dirección Bond1G del nodo primario a través de HTTP, no de HTTPS.

Ejemplo: http://<IP_address>:442/nde/

Ponga en marcha NetApp HCI con la IU de NDE

1. En el NDE, acepte los requisitos previos, marque el uso de Active IQ y acepte los acuerdos de licencia.
2. De manera opcional, habilite Data Fabric File Services por ONTAP Select y acepte la licencia de ONTAP Select.
3. Configure una puesta en marcha de vCenter nueva. Haga clic en **Configurar usando un nombre de dominio completo** e introduzca el nombre de dominio de vCenter Server y la dirección IP del servidor DNS.



Se recomienda usar el enfoque de FQDN para la instalación de vCenter.

4. Revise que la evaluación del inventario de todos los nodos se haya completado correctamente.

Ya se ha comprobado el nodo de almacenamiento que ejecuta NDE.

5. Seleccione todos los nodos y haga clic en **continuar**.
6. Configure los ajustes de red. Consulte *Manual de instalación de NetApp HCI* para obtener información sobre los valores que se deben utilizar.

7. Haga clic en el cuadro azul para iniciar el formulario sencillo.

Network Settings

Provide the network settings that will be used for your installation.

Live network validation is: **On** ?

Infrastructure Services

DNS Server IP Address 1

DNS Server IP Address 2 (Optional)

NTP Server Address 1 ? ✓

NTP Server Address 2 (Optional)

To save time, launch the easy form to enter fewer network settings. > ?

vCenter Networking

VLAN ID	Subnet ?	Default Gateway	FQDN	IP Address
Untagged Network	xxx.xxx.xxx.xxx/n	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. En el formulario sencillo Configuración de red:

- Escriba el prefijo de nombre. (Consulte los detalles del sistema del *NetApp HCI Installation Discovery Workbook*.)
- Haga clic en **no** para ¿asignará identificadores de VLAN? (Se asignan posteriormente en la página principal Network Settings).
- Escriba la subred CIDR, la puerta de enlace predeterminada y la dirección IP de inicio para las redes de gestión, vMotion e iSCSI según el libro. (Consulte la sección método de asignación IP del *NetApp HCI Installation Discovery Workbook* para obtener información sobre estos valores).
- Haga clic en **aplicar a Configuración de red**.

9. Únase a un "vCenter existente" (opcional).

10. Registre los números de serie del nodo en el *NetApp HCI Installation Discovery Workbook*.

11. Especifique un ID de VLAN para la red de vMotion y toda la red que requiera el etiquetado de VLAN. Consulte *Manual de instalación de NetApp HCI*.

12. Descargue la configuración como un archivo .CSV.

13. Haga clic en **Iniciar implementación**.

14. Copie y guarde la URL que aparece.



La puesta en marcha puede tardar unos 45 minutos en completarse.

Compruebe la instalación con vSphere Web Client

1. Inicie vSphere Web Client y inicie sesión con las credenciales especificadas durante el uso de NDE.

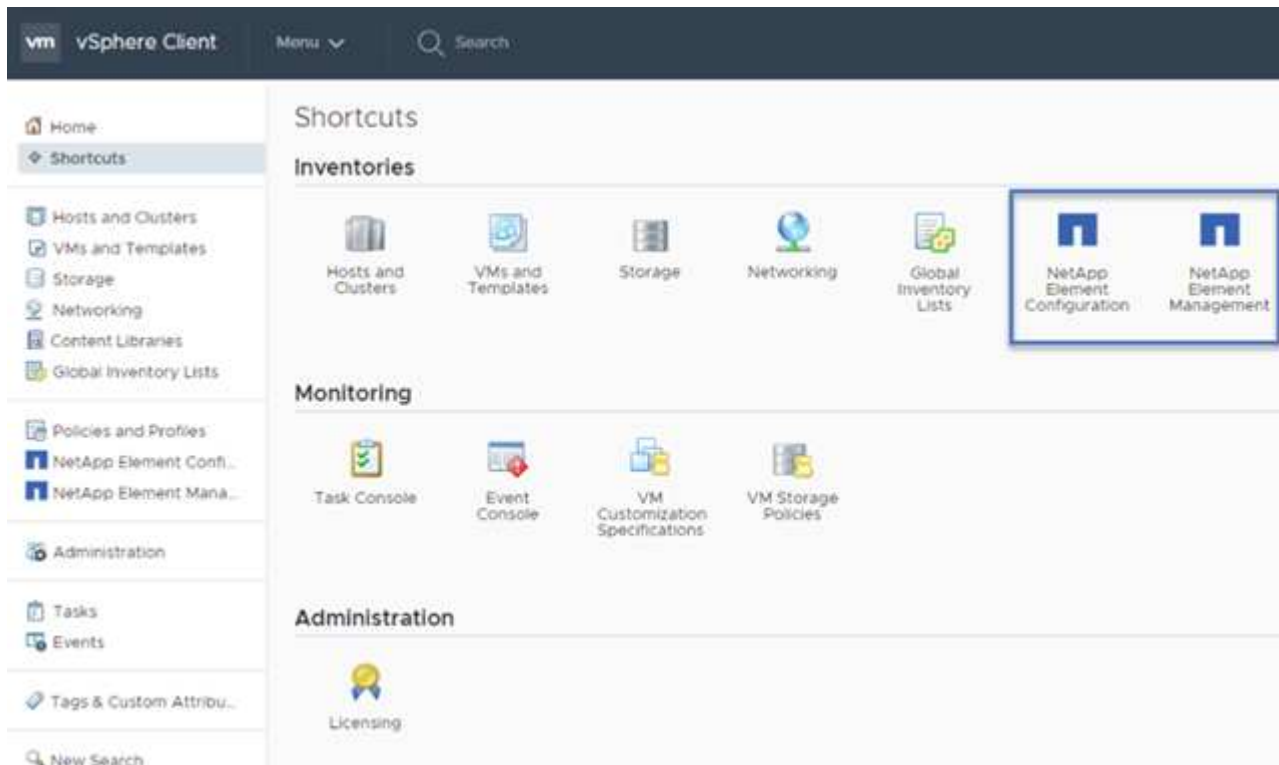
Debe añadir `@vsphere.local` al nombre de usuario.

2. Compruebe que no hay alarmas.
3. Verifique que los dispositivos de vCenter, mNode y ONTAP Select (opcionales) se ejecuten sin iconos de advertencia.
4. Observe que se crean los dos almacenes de datos predeterminados (NetApp-HCI-Datastore_01 y 02).
5. Seleccione cada almacén de datos y compruebe que todos los nodos de computación aparezcan en la pestaña hosts.
6. Valide vMotion y Datastore-02.
 - a. Migre vCenter Server a NetApp-HCI-Datastore-02 (solo almacenamiento vMotion).
 - b. Migre vCenter Server a cada uno de los nodos de computación (solo vMotion).
7. Vaya al plugin de NetApp Element para vCenter Server y compruebe que el clúster esté visible.
8. Asegúrese de que no aparece ninguna alerta en el panel.

Gestione NetApp HCI mediante el plugin de vCenter

Después de instalar NetApp HCI, puede configurar clústeres, volúmenes, almacenes de datos, registros, grupos de acceso, Iniciadores y políticas de calidad de servicio (QoS) mediante el plugin de NetApp Element para vCenter Server.

Para obtener más información, consulte ["Documentación del plugin de NetApp Element para vCenter Server"](#).



Supervise o actualice NetApp HCI con el control del cloud híbrido

Opcionalmente, puede utilizar el control del cloud híbrido de NetApp HCI para supervisar, actualizar o ampliar su sistema.

Para iniciar sesión en NetApp Hybrid Cloud Control, vaya a la dirección IP del nodo de gestión.

Con el control del cloud híbrido, puede hacer lo siguiente:

- ["Supervise la instalación de NetApp HCI"](#)
- ["Actualice su sistema NetApp HCI"](#)
- ["Amplíe sus recursos de computación o almacenamiento de NetApp HCI"](#)
- Pasos*

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.

Aparece la interfaz de control del cloud híbrido de NetApp.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Instrucciones de instalación y configuración de NetApp HCI"](#)
- ["TR-4820: Guía para la planificación rápida de redes de NetApp HCI"](#)
- ["Documentación del plugin de NetApp Element para vCenter Server"](#)
- ["Asesor de configuración de NetApp" 5.8.1 o posterior herramienta de validación de red](#)
- ["Documentación de SolidFire Active IQ de NetApp"](#)

Instale el hardware H-Series

Antes de empezar a usar NetApp HCI, debe instalar los nodos de computación y almacenamiento correctamente.



Consulte ["cartel"](#) para una representación visual de las instrucciones.

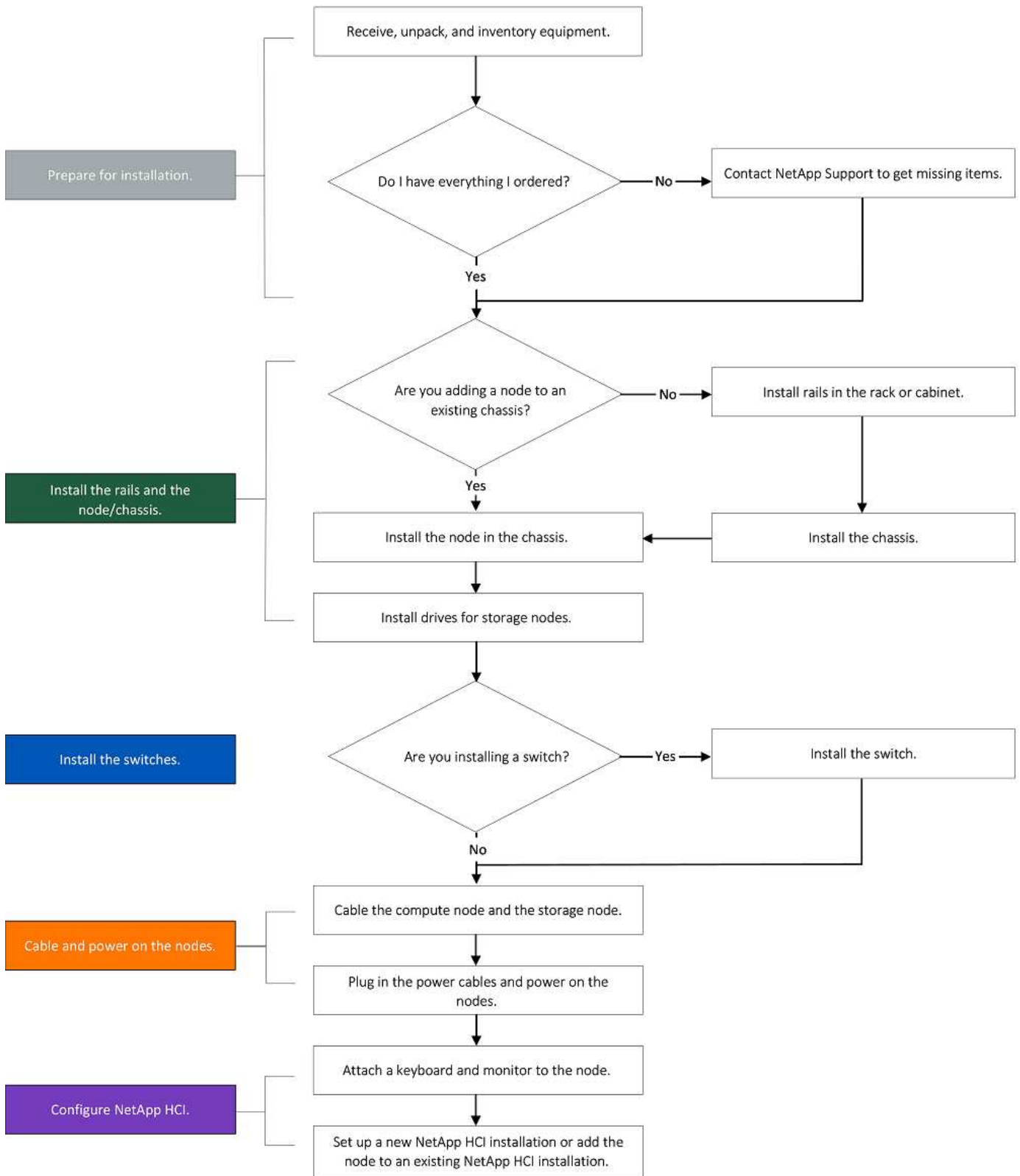
- [Diagramas de flujo de trabajo](#)
- [Preparación de la instalación](#)
- [Instale los rieles](#)
- [Instale el nodo/chasis](#)
- [Instale los interruptores](#)
- [Cablee los nodos](#)
- [Encienda los nodos](#)
- [Configure NetApp HCI](#)
- [Realice tareas posteriores a la configuración](#)

Diagramas de flujo de trabajo

Los diagramas de flujo de trabajo aquí proporcionan una descripción general de alto nivel de los pasos de la instalación. Los pasos varían ligeramente según el modelo de la serie H.

- [H410C y H410S](#)
- [H610C y H615C](#)
- [\[H610S\]](#)

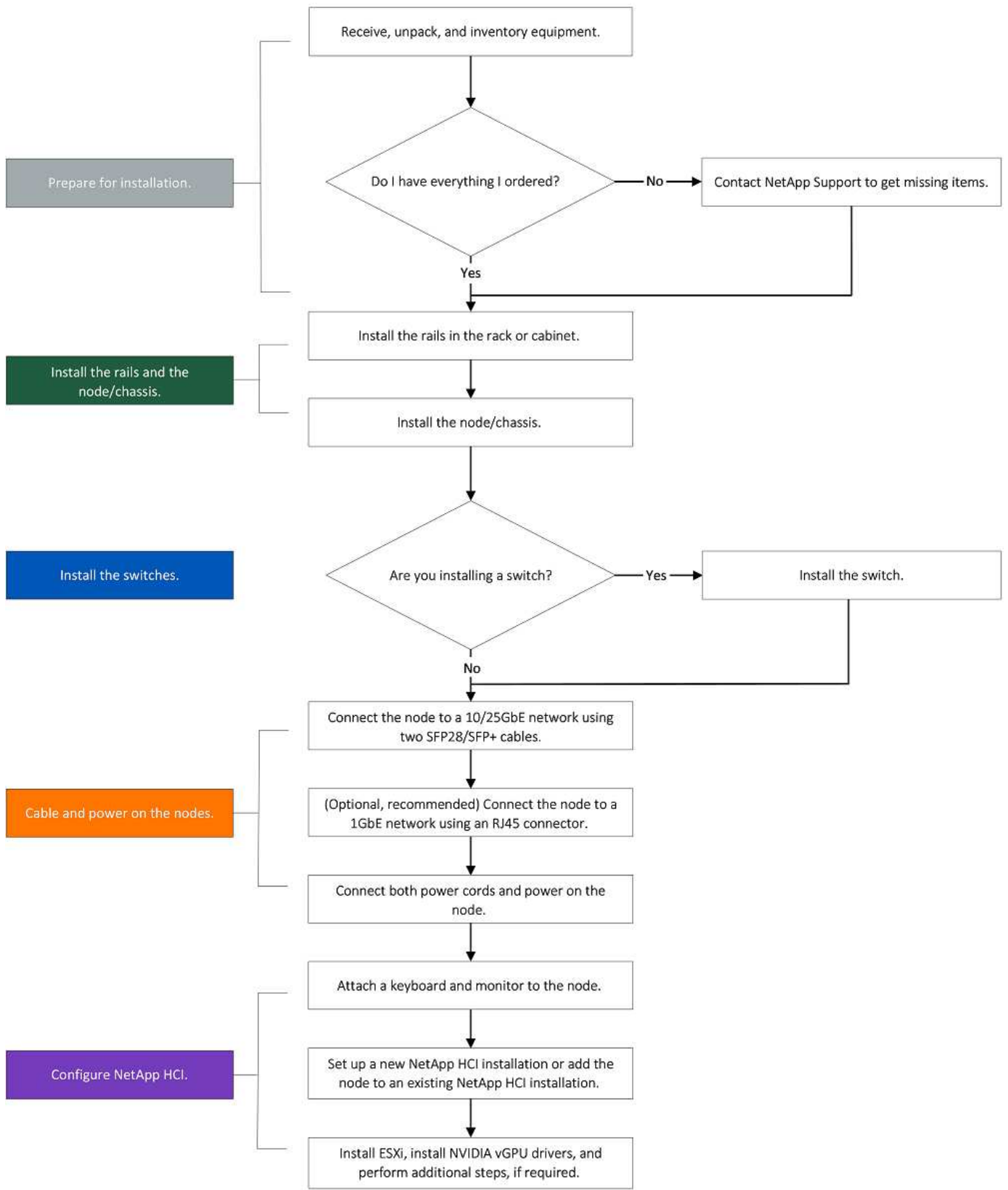
H410C y H410S



H610C y H615C



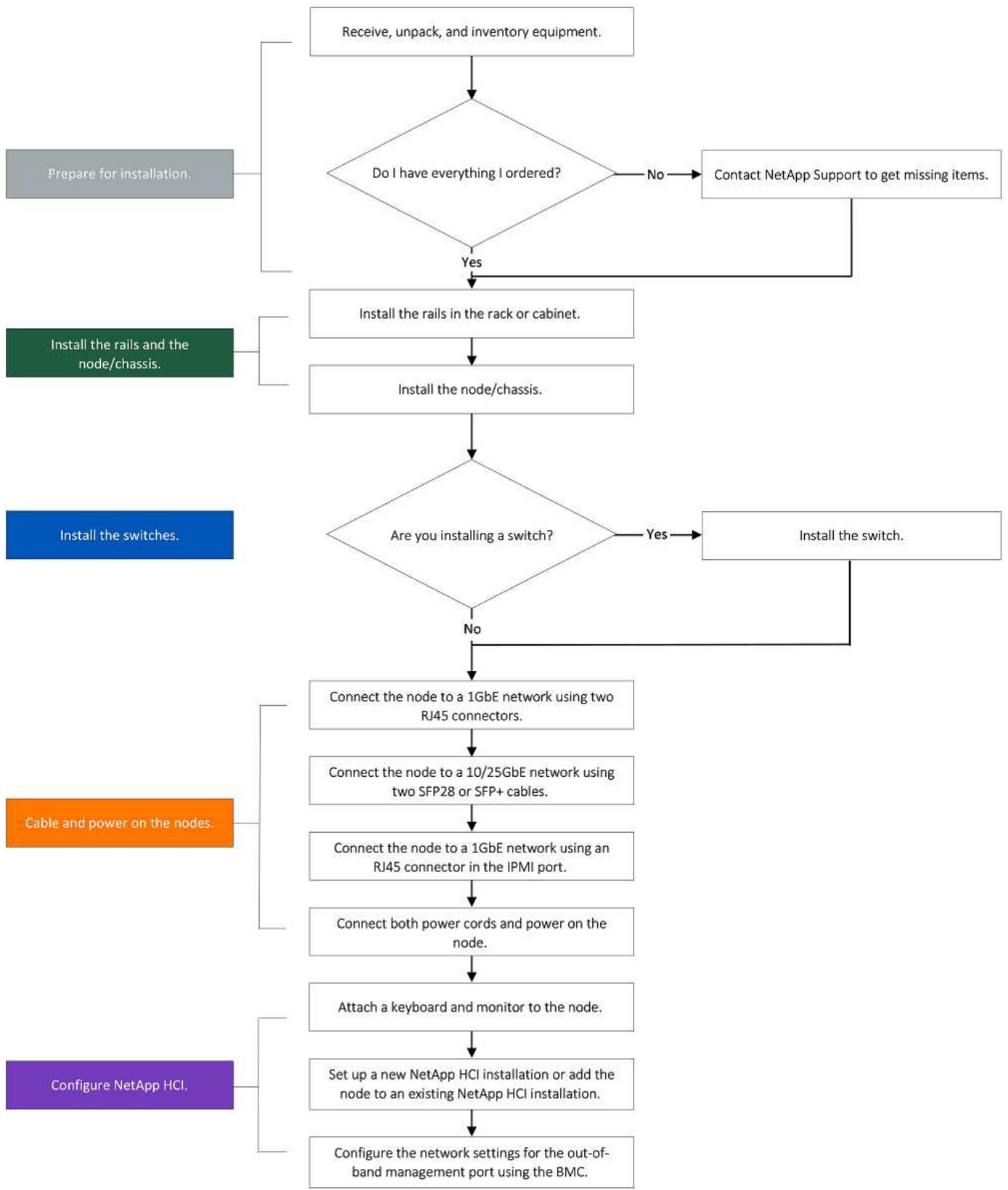
Los términos "nodo" y "chasis" se utilizan indistintamente en el caso de H610C y H615C, porque los componentes de nodo y chasis no están separados, a diferencia del caso de un chasis 2U de cuatro nodos.



H610S



Los términos "nodo" y "chasis" se utilizan indistintamente en el caso de H610C y H615C, porque los componentes de nodo y chasis no están separados, a diferencia del caso de un chasis 2U de cuatro nodos.



Preparación de la instalación

Durante la preparación para la instalación, realice el inventario del hardware que recibió y póngase en contacto con el soporte de NetApp en caso de que falte algún artículo.

Asegúrese de tener los siguientes elementos en su ubicación de instalación:

- Espacio en rack para el sistema.

Tipo de nodo	Espacio de rack
Nodos H410C y H410S	Dos unidades de rack (2U)
Nodo H610C	2 U
Los nodos H615C y H610S	Una unidad de rack (1U)

- Cables o transceptores de conexión directa SFP28/SFP+
- Cables CAT5e o superiores con conector RJ45
- Un switch de teclado, vídeo y ratón (KVM) para configurar el sistema
- Stick USB (opcional)



El hardware que se le envía depende de lo que realice su pedido. Un nuevo pedido de 2U de cuatro nodos incluye el chasis, el panel frontal, el kit de rieles deslizantes, unidades para nodos de almacenamiento, nodos de computación y almacenamiento, y cables de alimentación (dos por chasis). Si solicita nodos de almacenamiento H610S, las unidades se instalan en el chasis.



Durante la instalación de la tornillería, asegúrese de retirar todo el material de embalaje y el embalaje de la unidad. Esto evitará que los nodos se sobrecalienten y se apaguen.

Instale los rieles

El orden de hardware que se le envió incluye un conjunto de rieles deslizantes. Necesitará un destornillador para completar la instalación del riel. Los pasos de instalación varían ligeramente para cada modelo de nodo.



Instale la tornillería desde la parte inferior del bastidor hasta la parte superior para evitar que el equipo se caiga. Si el rack incluye dispositivos estabilizadores, instálelos antes de instalar el hardware.

- [H410C y H410S](#)
- [\[H610C\]](#)
- [H610S y H615C](#)

H410C y H410S

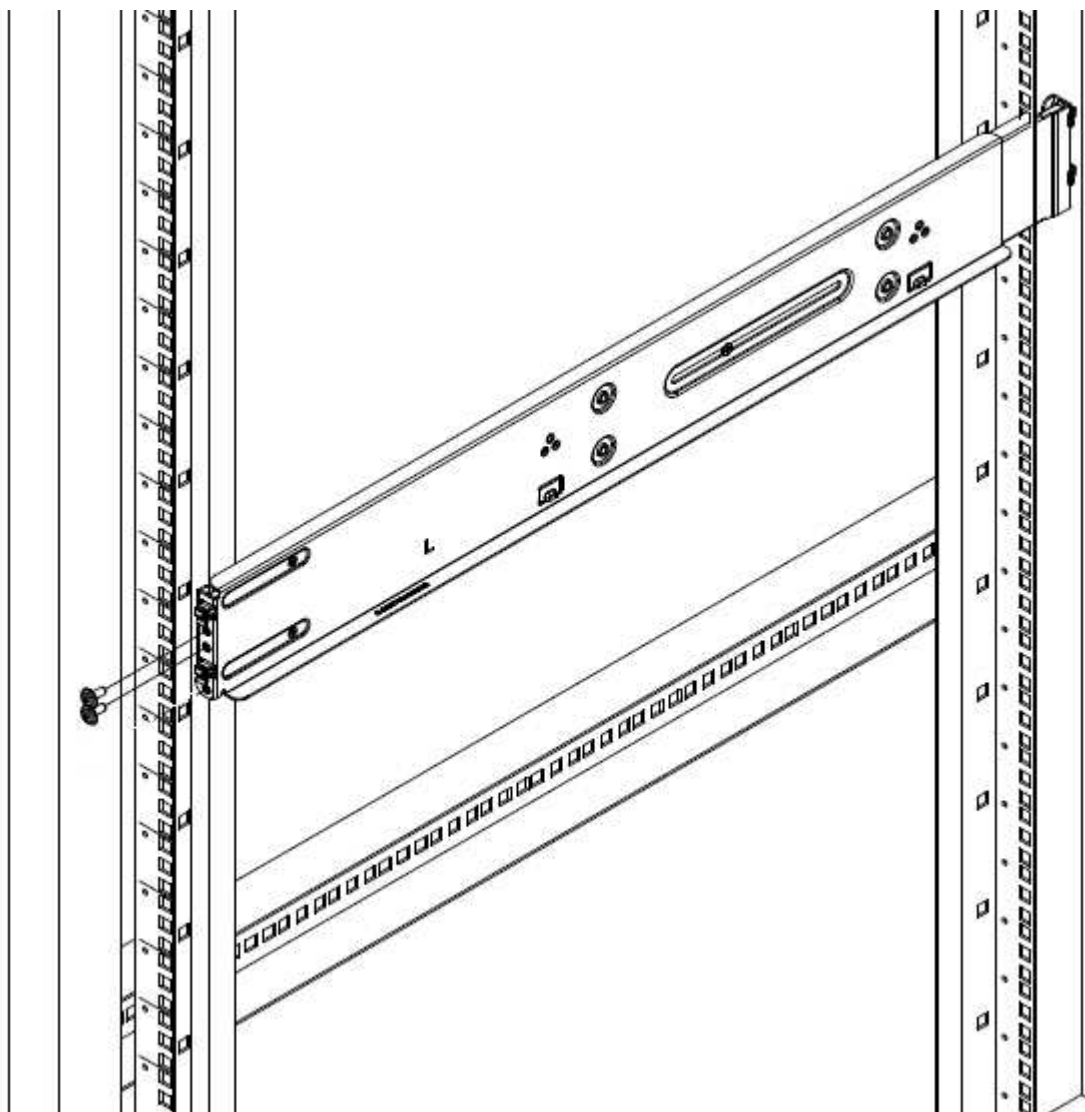
Los nodos H410C y H410S se instalan en chasis 2U de cuatro nodos H-Series, que se envía con dos conjuntos de adaptadores. Si desea instalar el chasis en un rack con orificios redondos, utilice los adaptadores adecuados para un rack con orificios redondos. Los rieles para nodos H410C y H410S encajan en un rack de entre 29 pulgadas y 33.5 pulgadas de profundidad. Cuando el riel está totalmente contrapuesto, tiene 28 pulgadas de largo, y las secciones delantera y trasera del riel se mantienen Unidas sólo con un tornillo.



Si instala el chasis en un riel totalmente contratado, es posible que las secciones delantera y trasera del riel se separen.

Pasos

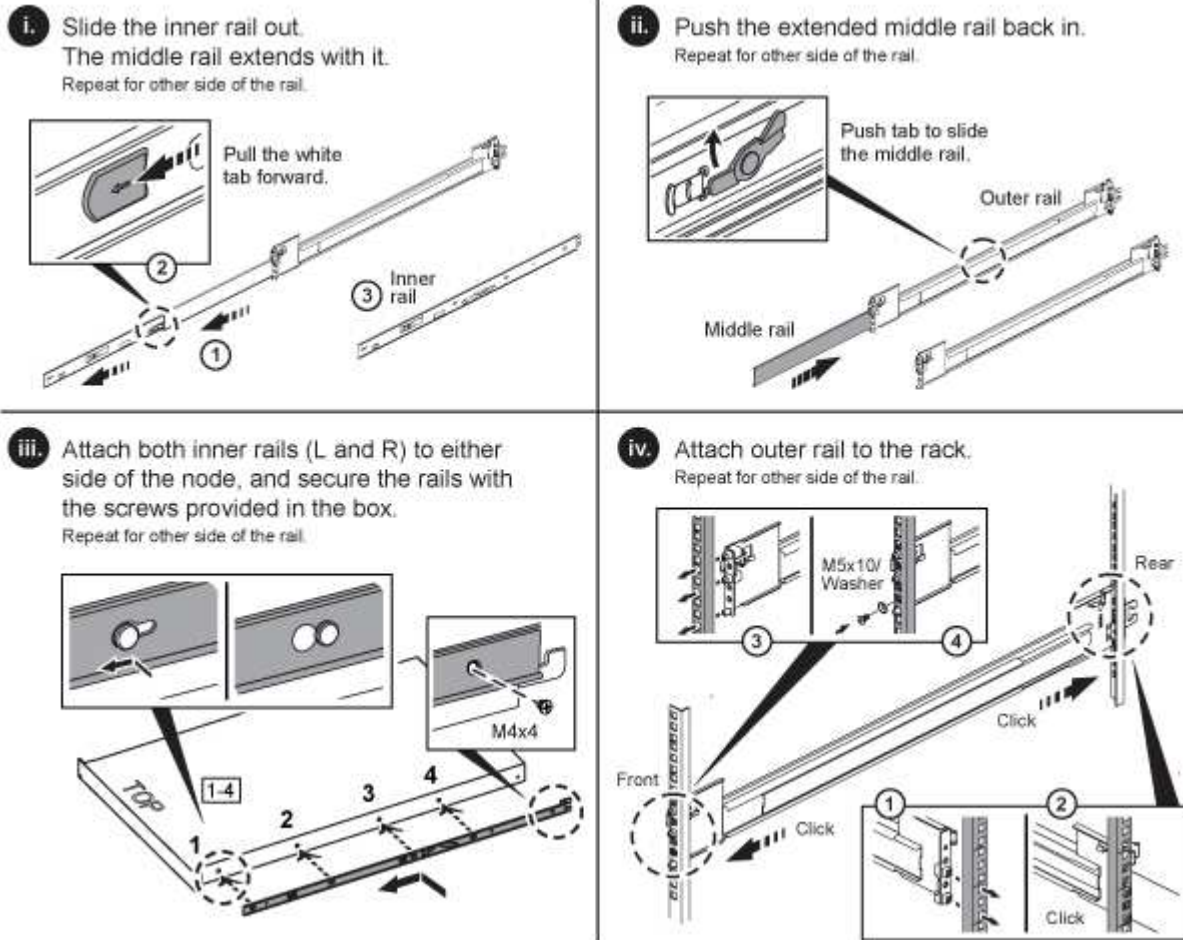
1. Alinee la parte frontal del raíl con los orificios del poste delantero del rack.
2. Empuje los ganchos de la parte frontal del raíl hacia los orificios del poste delantero del rack y, a continuación, hacia abajo hasta que las clavijas cargadas por resorte encajen en los orificios del rack.
3. Fije el riel al rack con tornillos. A continuación, se muestra una ilustración del raíl izquierdo conectado a la parte frontal del rack:



4. Extienda la sección trasera del raíl al poste trasero del bastidor.
5. Alinee los ganchos de la parte trasera del raíl con los orificios adecuados del poste trasero, asegurándose de que la parte delantera y posterior del raíl estén al mismo nivel.
6. Monte la parte posterior del raíl en el rack y fije el riel con tornillos.
7. Realice todos los pasos anteriores para el otro lado del rack.

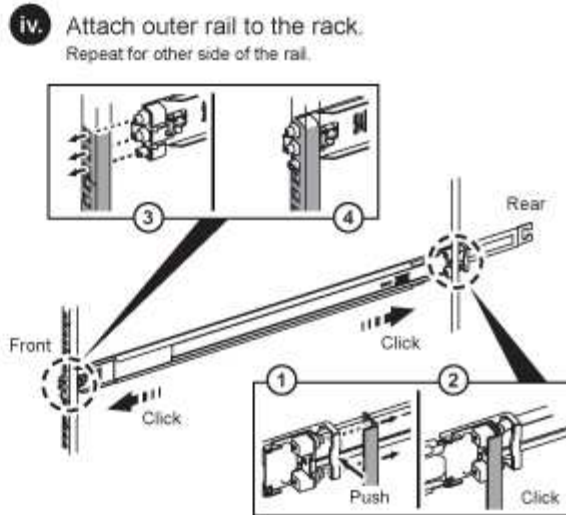
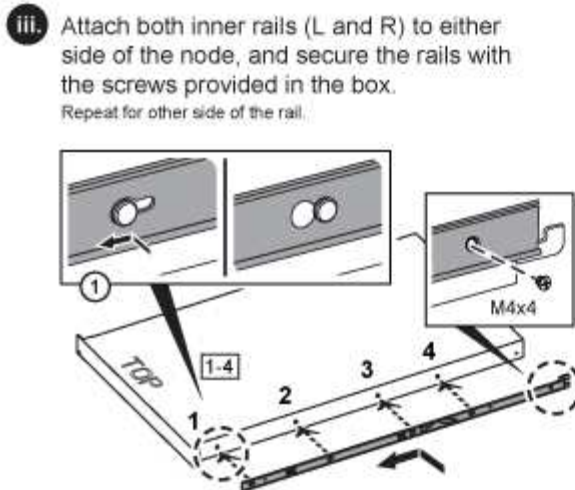
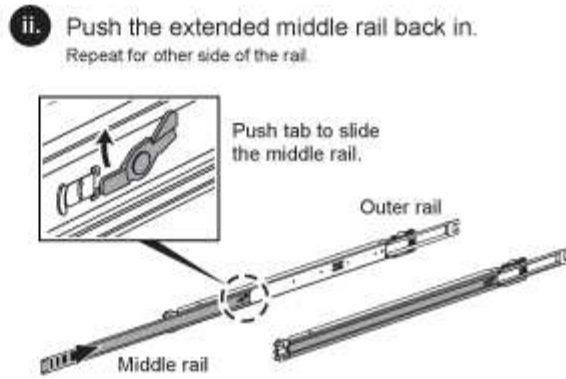
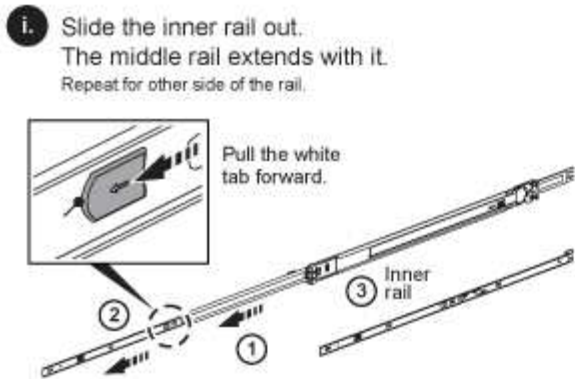
H610C

A continuación encontrará una ilustración de la instalación de rieles para un nodo de computación H610C:



H610S y H615C

A continuación, se muestra una ilustración para la instalación de rieles para un nodo de almacenamiento H610S o un nodo de computación H615C:



Hay rieles izquierdo y derecho en H610S y H615C. Coloque el orificio del tornillo hacia la parte inferior de modo que el tornillo de ajuste manual H610S/H615C pueda fijar el chasis al raíl.

Instale el nodo/chasis

Se instala el nodo de computación H410C y el nodo de almacenamiento H410S en un chasis 2U de cuatro nodos. Para H610C, H615C y H610S, instale el chasis/nodo directamente en los rieles del rack.



A partir de NetApp HCI 1.8, puede configurar un clúster de almacenamiento con dos o tres nodos de almacenamiento.



Retire todo el material de embalaje y el embalaje de la unidad. Esto evita que los nodos se sobrecalienten y se apaguen.

- [Nodos H410C y H410S](#)
- [Nodo/chasis H610C](#)
- [nodo/chasis](#)

Nodos H410C y H410S

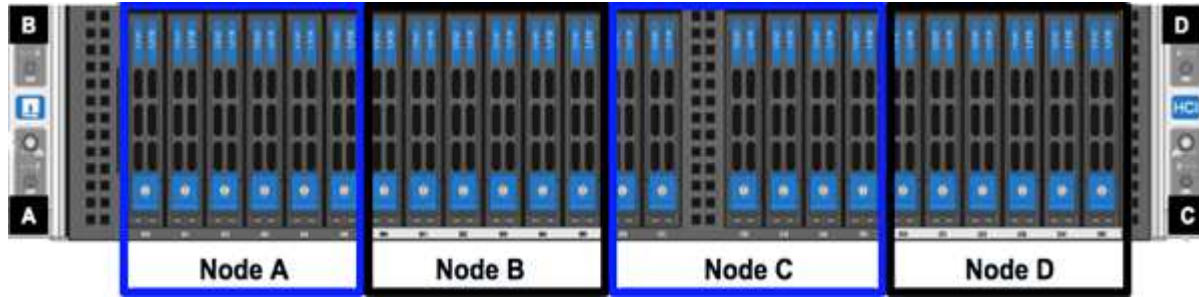
Pasos

1. Instale los nodos H410C y H410S en el chasis. A continuación, se muestra un ejemplo de vista posterior de un chasis con cuatro nodos instalados:

CHASSIS BACK VIEW



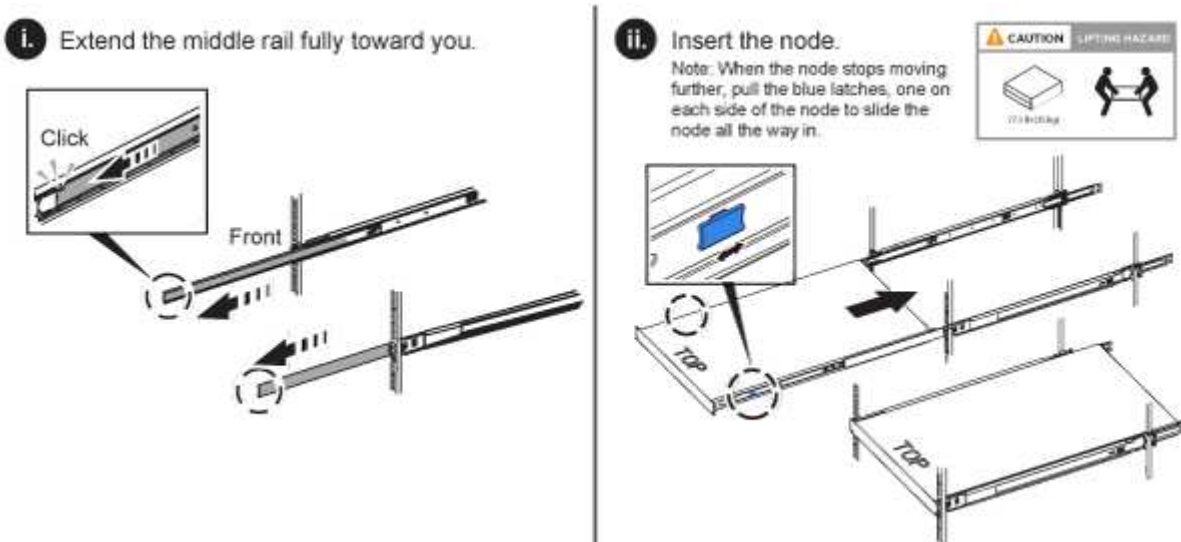
2. Instale las unidades para los nodos de almacenamiento H410S.



Nodo/chasis H610C

En el caso de H610C, los términos "nodo" y "chasis" se utilizan indistintamente porque el nodo y el chasis no son componentes separados, a diferencia del caso del chasis de 2U de cuatro nodos.

A continuación se muestra una ilustración de la instalación del nodo/chasis en el rack:

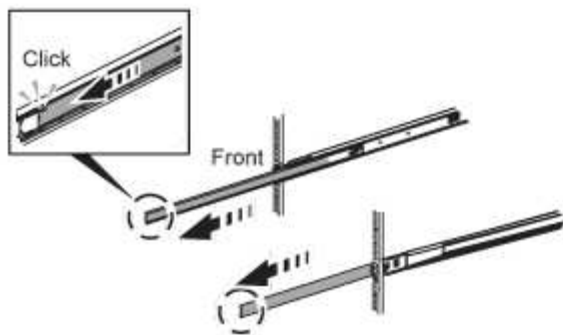


H610S y H615C, nodo/chasis

En el caso H615C y H610S, los términos "nodo" y "chasis" se utilizan indistintamente porque los componentes de nodo y chasis no son separados, a diferencia del caso del chasis de 2U de cuatro nodos.

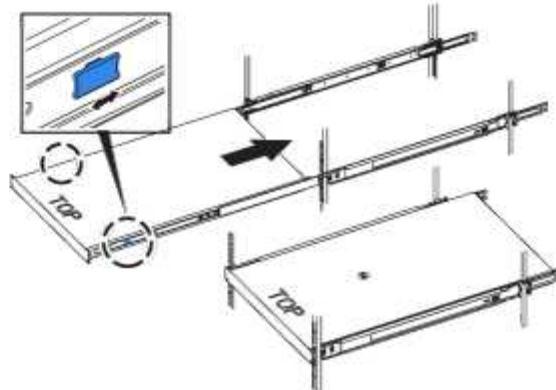
A continuación se muestra una ilustración de la instalación del nodo/chasis en el rack:

i. Extend the middle rail fully toward you.



ii. Insert the node.

Note: When the node stops moving further, pull the blue latches, one on each side of the node to slide the node all the way in.



Instale los interruptores

Si desea utilizar los conmutadores Mellanox SN2010, SN2100 y SN2700 en la instalación de NetApp HCI, siga las instrucciones que se proporcionan aquí para instalar y cablear los conmutadores:

- ["Manual del usuario de hardware de Mellanox"](#)
- ["TR-4836: Guía de cableado de los conmutadores NetApp HCI con Mellanox SN2100 y SN2700 \(se requiere inicio de sesión\)"](#)

Cablee los nodos

Si va a añadir nodos a una instalación existente de NetApp HCI, compruebe que la configuración de cableado y red de los nodos que añade sea idéntica a la de la instalación existente.



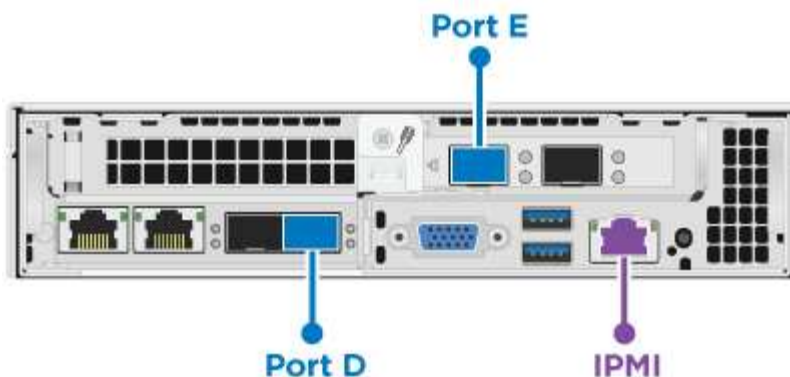
Asegúrese de que la apertura de flujo de aire de la parte trasera del chasis no esté bloqueada con cables o etiquetas. Esto puede provocar fallos prematuros en los componentes debido al sobrecalentamiento.

- [Nodo de computación H410C y nodo de almacenamiento H410S](#)
- [Nodo de computación H610C](#)
- [Nodo de computación H615C](#)
- [Nodo de almacenamiento H610S](#)

Nodo de computación H410C y nodo de almacenamiento H410S

Tiene dos opciones para cablear el nodo H410C: Mediante dos cables o mediante seis cables.

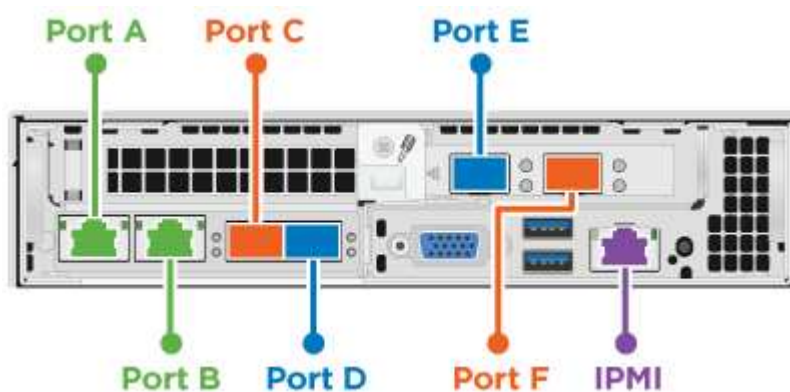
Esta es la configuración de dos cables:



● En el caso de los puertos D y E, conecte dos cables o transceptores SFP28/SFP+ para conectividad de gestión compartida, máquina virtual y almacenamiento.

● (Opcional, recomendado) Conecte un cableCAT5e en el puerto IPMI para conectividad de gestión fuera de banda.

Esta es la configuración de seis cables:



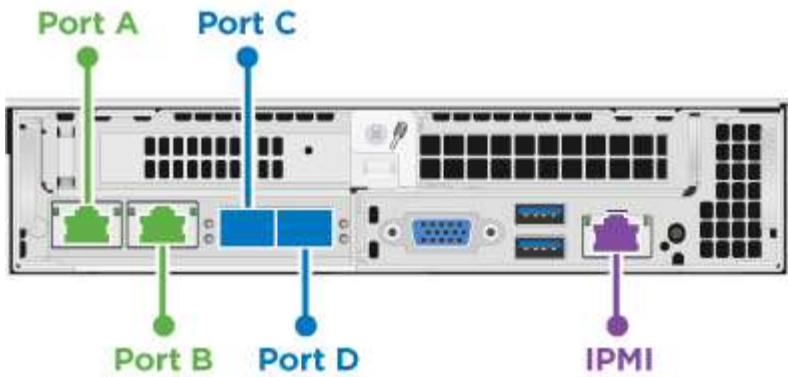
● Para los puertos A y B, conecte dos cables CAT5e o superiores en los puertos A y B para conectividad de gestión.

● En el caso de los puertos C y F, conecte dos cables o transceptores SFP28/SFP+ para conectividad de máquina virtual.

● En el caso de los puertos D y E, conecte dos cables o transceptores SFP28/SFP+ para conectividad de almacenamiento.

● (Opcional, recomendado) Conecte un cableCAT5e en el puerto IPMI para conectividad de gestión fuera de banda.

A continuación se muestra el cableado para el nodo H410S:



● Para los puertos A y B, conecte dos cables CAT5e o superiores en los puertos A y B para conectividad de gestión.

● En el caso de los puertos C y D, conecte dos cables o transceptores SFP28/SFP+ para conectividad de almacenamiento.

● (Opcional, recomendado) Conecte un cable CAT5e en el puerto IPMI para conectividad de gestión fuera de banda.

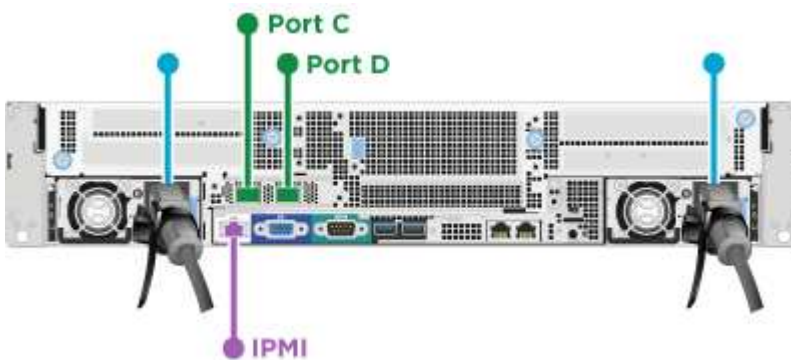
Después de conectar los nodos, conecte los cables de alimentación a las dos unidades de suministro de alimentación por chasis y enchúfelos en un PDU o tomacorriente de 240 V.

Nodo de computación H610C

A continuación se muestra el cableado para el nodo H610C:



Los nodos H610C se implementan solo en la configuración de dos cables. Asegúrese de que todas las VLAN están presentes en los puertos C y D.



● Para los puertos C y D, conecte el nodo a una red de 10 GbE mediante dos cables SFP28/SFP+.

● (Opcional, recomendado) Conecte el nodo a una red de 1 GbE mediante un conector RJ45 en el puerto IPMI.

Conecte ambos cables de alimentación al nodo y enchufe los cables de alimentación a una toma de alimentación de 200-240 V.

Nodo de computación H615C

A continuación se muestra el cableado del nodo H615C:



Los nodos H615C solo se implementan en la configuración de dos cables. Asegúrese de que todas las VLAN están presentes en los puertos A y B.



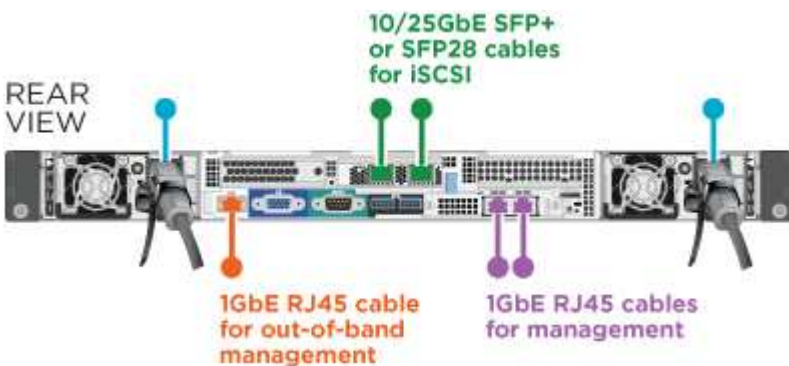
Para los puertos A y B, conecte el nodo a una red de 10 GbE mediante dos cables SFP28/SFP+.

(Opcional, recomendado) Conecte el nodo a una red de 1 GbE mediante un conector RJ45 en el puerto IPMI.

Conecte ambos cables de alimentación al nodo y enchufe los cables de alimentación a una toma de alimentación de 110 V.

Nodo de almacenamiento H610S

Este es el cableado para el nodo H610S:



Conecte el nodo a una red de 1 GbE mediante dos conectores RJ45 en el puerto IPMI.

Conecte el nodo a una red de 10 GbE mediante dos cables SFP28 o SFP+.

Conecte el nodo a una red de 1 GbE mediante un conector RJ45 en el puerto IPMI.

 Conecte ambos cables de alimentación al nodo.

Encienda los nodos

Los nodos tardan aproximadamente seis minutos en arrancar.

A continuación encontrará una ilustración en la que se muestra el botón de encendido en el chasis NetApp HCI 2U:



A continuación, se muestra una ilustración que muestra el botón de encendido en el nodo H610C:



A continuación, se muestra una ilustración en la que se muestra el botón de alimentación de los nodos H615C y H610S:



Configure NetApp HCI

Elija una de las siguientes opciones:

- [Nueva instalación de NetApp HCI](#)
- [Amplíe una instalación existente de NetApp HCI](#)

Nueva instalación de NetApp HCI

Pasos

1. Configure una dirección IPv4 en la red de gestión (Bond1G) en un nodo de almacenamiento de NetApp HCI.



Si va a utilizar DHCP en la red de gestión, puede conectarse a la dirección IPv4 adquirida por DHCP del sistema de almacenamiento.

- a. Conecte un teclado, un vídeo y un ratón (KVM) a la parte posterior del nodo de almacenamiento.
 - b. Configure la dirección IP, la máscara de subred y la dirección de puerta de enlace para Bond1G en la interfaz de usuario. También puede configurar un ID de VLAN para la red Bond1G.
2. Utilice un explorador web compatible (Mozilla Firefox, Google Chrome o Microsoft Edge) para ir al motor de implementación de NetApp. Para ello, conéctese a la dirección IPv4 que configuró en el paso 1.
 3. Use la interfaz de usuario del motor de implementación de NetApp para configurar NetApp HCI.



Todos los demás nodos NetApp HCI se detectan de forma automática.

Amplíe una instalación existente de NetApp HCI

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web.
2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. Siga los pasos del asistente para añadir nodos de almacenamiento y computación a la instalación de NetApp HCI.



Para añadir nodos de computación H410C, la instalación existente debe ejecutar NetApp HCI 1.4 o posterior. Para añadir nodos de computación H615C, la instalación existente debe ejecutar NetApp HCI 1.7 o una versión posterior.



Los nodos NetApp HCI instalados recientemente en la misma red se detectan de forma automática.

Realice tareas posteriores a la configuración

Según el tipo de nodo que tenga, es posible que necesite realizar pasos adicionales después de instalar el hardware y configurar NetApp HCI.

- [Nodo H610C](#)
- [Los nodos H615C y H610S](#)

Nodo H610C

Instale los controladores de GPU en ESXi para cada nodo H610C que ha instalado, y valide su funcionalidad.

Los nodos H615C y H610S

Pasos

1. Utilice un explorador web y desplácese a la dirección IP predeterminada del BMC: 192.168.0.120
2. Inicie sesión con el nombre de usuario `root` y contraseña `calvin`.
3. Desde la pantalla de administración de nodos, vaya a **Configuración > Configuración de red** y configure los parámetros de red para el puerto de administración fuera de banda.

Si el nodo H615C tiene GPU en él, instale los controladores de GPU en ESXi para cada nodo H615C que haya instalado, y valide su funcionalidad.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["TR-4820: Guía de planificación rápida de redes de NetApp HCI"](#)
- ["Asesor de configuración de NetApp" 5.8.1](#) o posterior herramienta de validación de red

Configure LACP para alcanzar un rendimiento de almacenamiento óptimo

Para alcanzar un rendimiento óptimo en el clúster de almacenamiento de NetApp HCI, se debe configurar el protocolo de control de agregación de enlaces (LACP) en los puertos del switch que se utilizan para cada nodo de almacenamiento.

Antes de empezar

- Configuró los puertos del switch conectados a las interfaces 10/25GbE de los nodos de almacenamiento de NetApp HCI como canales de puertos LACP.
- Estableció los temporizadores LACP de los switches que controlan el tráfico de almacenamiento en "fast mode (1s)" para lograr un tiempo de detección de conmutación al nodo de respaldo óptimo. Durante la implementación, las interfaces Bond1G en todos los nodos de almacenamiento se configuran automáticamente para el modo activo-pasivo.
- Configuró un canal de puerto virtual (VPC) de Cisco o una tecnología de apilamiento de switches equivalente para los switches que controlan la red de almacenamiento. La tecnología de apilamiento de switches facilita la configuración de LACP y los canales de puertos, y proporciona una topología sin bucles entre los switches y los puertos 10 GbE en los nodos de almacenamiento.

Pasos

1. Siga las recomendaciones del proveedor de switches a fin de habilitar LACP en los puertos del switch utilizados para los nodos de almacenamiento de NetApp H-Series.
2. Cambie el modo de unión con LACP de todos los nodos de almacenamiento en la interfaz de usuario en el nodo (también conocida como interfaz de usuario de terminal o TUI) antes de implementar NetApp HCI.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Validar su entorno con Active IQ Config Advisor

Antes de montar en rack el hardware de NetApp HCI y realizar la instalación de NetApp HCI, debe verificar que su entorno cumple con los requisitos de red de NetApp HCI. Active IQ Config Advisor ejecuta comprobaciones de su entorno validando las configuraciones de red, switch y VMware vSphere. La herramienta genera un informe que puede utilizar para ayudarle a resolver problemas y puede reenviar el informe a su ingeniero de los servicios profesionales para que prepare y programe una instalación.

Instale Active IQ Config Advisor

Descargue e instale Active IQ Config Advisor en un PC que tenga acceso a las redes NetApp HCI.

Pasos

1. En un navegador web, seleccione **Herramientas** en el menú Soporte de NetApp, busque Active IQ Config Advisor y descargue la herramienta.

["Herramientas del del sitio de soporte de NetApp"](#).

Después de aceptar el Contrato de licencia para el usuario final (EULA), aparece la página Descargar. Los binarios de Microsoft Windows, Linux y Mac están disponibles en el panel **herramienta cliente**.

2. Ejecute el archivo ejecutable.
3. Seleccione un idioma y haga clic en **Aceptar**.
4. Haga clic en **Siguiente**.
5. Lea el EULA y haga clic en **Acepto**.
6. Haga clic en **instalar**.
7. Asegúrese de que **Ejecutar Active IQ Config Advisor** está seleccionado y haga clic en **Finalizar**.

Tras un breve retraso, la interfaz de usuario de Active IQ Config Advisor se abre en una nueva pestaña o ventana del navegador.

Utilice Active IQ Config Advisor

Active IQ Config Advisor se ejecuta en una ventana del explorador, recopila información sobre la red y el entorno y genera un informe que puede utilizar para resolver cualquier problema de configuración o red que pudiera interferir en la implementación de NetApp HCI.

Antes de empezar

Instaló Active IQ Config Advisor en un dispositivo que puede acceder a la red de gestión, las redes de VMware vCenter Server (si se va a unir a una instalación existente de VMware) y los switches que se usarán para NetApp HCI.



Si utiliza switches Mellanox y los servicios profesionales de NetApp los configuran como parte de la puesta en marcha, no necesita proporcionar información del switch.

Acerca de esta tarea

Active IQ Config Advisor solo realiza comprobaciones de solo lectura para recopilar información. No se modifica ninguna configuración como parte de la colección.

Pasos

1. Abra Active IQ Config Advisor.

Config Advisor aparece con la ventana **Configuración básica** en un navegador web. Aquí puede definir la configuración global de la colección y cifrar los resultados de la misma.

2. Introduzca una frase de contraseña en la sección **Configuración de cifrado** para cifrar el proyecto de recopilación.

Esto garantiza que sólo podrá cargar este proyecto de recopilación una vez creado.

3. Identifique este informe de recopilación como el suyo introduciendo su nombre y dirección de correo electrónico en la sección **verificación de usuarios**.
4. Haga clic en **Guardar**.
5. Haga clic en **Crear una nueva recopilación de datos**.
6. Seleccione **solución basada** en el menú desplegable **Tipo de colección**.
7. Seleccione **implementación previa de NetApp HCI** en el menú desplegable **Perfil**.
8. Para cada tipo de dispositivo de la columna **Tipo**, seleccione el número de ese tipo de dispositivo de la red NetApp HCI en el menú desplegable **acciones**.

Por ejemplo, si tiene tres conmutadores Cisco, seleccione 3 en el menú desplegable de la columna **acciones** de esa fila. Aparecen tres filas, una para cada switch Cisco identificado.



Si utiliza switches Mellanox y los servicios profesionales de NetApp los configuran como parte de la puesta en marcha, no necesita proporcionar información del switch.

9. Para los switches identificados, introduzca la dirección IP de administración y las credenciales de administrador.
10. Para cualquier instancia de VMware vCenter Server que haya identificado, realice una de las siguientes acciones:
 - Si va a implementar una nueva instancia de vCenter Server, proporcione la dirección IP o el nombre de dominio completo (FQDN) correspondiente al servidor.
 - Si ya se está uniendo a una instancia existente de vCenter Server, proporcione la dirección IP o el FQDN y las credenciales de administrador para el servidor.
11. Opcional: Si agregó información para los conmutadores, introduzca el número de nodos de computación y almacenamiento en la sección **validación de conmutador**.
12. Elija la configuración de cableado de nodos de computación que va a utilizar en la sección **Red de nodos de computación**.
13. Introduzca puertos de switch individuales y las etiquetas VLAN que desee utilizar para las redes de gestión, vMotion y almacenamiento de los switches de la sección **Red de nodos de computación**.
14. Introduzca los puertos de switch individuales y las etiquetas VLAN que vaya a utilizar para las redes de gestión y almacenamiento de los conmutadores de la sección **Red de nodos de almacenamiento**.
15. En la sección **Network Settings Check**, introduzca las direcciones IP y la dirección IP de la puerta de enlace para la red de gestión, seguido de las listas de servidores para DNS, NTP y vCenter Server (si va a implementar una instancia nueva de vCenter Server con NetApp HCI).

En esta sección, Active IQ Config Advisor puede asegurarse de que la red de gestión esté disponible para su uso y también garantiza que servicios como DNS y NTP funcionen correctamente.

- Haga clic en **Validar** para asegurarse de que toda la información de la dirección IP y las credenciales introducidas son válidas.
- Haga clic en **Guardar o recopilar**.

Esto inicia el proceso de recopilación y puede ver el progreso a medida que la recopilación se ejecuta junto con un registro en tiempo real de los comandos de recopilación. La columna **Progress** muestra barras de progreso codificadas por colores para cada tarea de recopilación.



Las barras de progreso utilizan los colores siguientes para mostrar el estado:

- **Verde:** La colección ha terminado sin errores de comando. Puede ver los riesgos y recomendaciones de implementación haciendo clic en el icono **Ver y analizar** del menú **acciones**.
 - **Amarillo:** La colección ha terminado con algunos errores de comando. Puede ver los riesgos y recomendaciones de implementación haciendo clic en el icono **Ver y analizar** del menú **acciones**.
 - **Rojo:** La colección ha fallado. Debe resolver los errores y ejecutar la colección de nuevo.
- Opcional: Una vez completada la colección, puede hacer clic en el icono binocular de cualquier fila de recopilación para ver los comandos que se ejecutaron y los datos recopilados.
 - Seleccione la ficha **Ver y analizar**.

Esta página muestra un informe de estado general de su entorno. Es posible seleccionar una sección del gráfico circular para ver más detalles sobre esas comprobaciones o descripciones específicas de los problemas, junto con recomendaciones para resolver los problemas que puedan interferir en la implementación correcta. Puede resolver estos problemas usted mismo o solicitar ayuda de los Servicios profesionales de NetApp.

- Haga clic en **Exportar** para exportar el informe de recopilación como documento PDF o de Microsoft Word.



Entre los documentos de PDF y Microsoft Word se incluye la información de configuración del switch para la implementación que utilizan los Servicios profesionales de NetApp para comprobar los ajustes de red.

- Envíe el archivo del informe exportado al representante de los servicios profesionales de NetApp.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Configure IPMI para cada nodo

Después de haber montado en rack, cableado y encendido el hardware de NetApp HCI, es posible configurar el acceso de la interfaz de gestión de plataforma inteligente (IPMI) para cada nodo. Asigne una dirección IP a cada puerto IPMI y cambie la contraseña de administrador IPMI predeterminada en cuanto tenga acceso IPMI remoto al nodo.

Requisitos previos

Una vez que haya comprobado que su entorno está listo para admitir NetApp HCI y que se resuelve cualquier problema potencial, tendrá que completar algunas tareas finales antes de la implementación.

- Asegúrese de tener un informe de Active IQ Config Advisor correcto.
- Reúna toda la información relevante acerca de la red, de la infraestructura actual o planificada de VMware y de las credenciales de usuario planificadas.
- Monte en rack, cablee y encienda la instalación del NetApp HCI.

Asignar manualmente la dirección IP del puerto IPMI

El protocolo de configuración dinámica de hosts (DHCP) está habilitado de forma predeterminada para el puerto IPMI de cada nodo NetApp HCI. Si la red IPMI no utiliza DHCP, es posible asignar manualmente una dirección IPv4 estática al puerto IPMI.

Antes de empezar

Asegúrese de que tiene un conmutador o monitor de teclado, vídeo y ratón (KVM) que puede utilizar para acceder al BIOS de cada nodo.

Acerca de esta tarea

Utilice las teclas de flecha para navegar en el BIOS. Pulse para seleccionar una pestaña o una opción `Enter`. Vuelva a la pantalla anterior pulsando `ESC`.

Pasos

1. Encienda el nodo.
2. En el arranque, presione la para ingresar al BIOS `Del` clave.
3. Seleccione la pestaña IPMI.
4. Seleccione **Configuración de red BMC** y pulse `Enter`.
5. Elija **Sí** y pulse `Enter`.
6. Seleccione **origen de dirección de configuración** y pulse `Enter`.
7. Elija **estático** y pulse `Enter`.
8. Seleccione **Dirección IP de la estación** e introduzca una nueva dirección IP para el puerto IPMI. Pulse `Enter` al finalizar.
9. Seleccione **Subnet mask** e introduzca una nueva máscara de subred para el puerto IPMI. Pulse `Enter` al finalizar.
10. Seleccione **Dirección IP de puerta de enlace** e introduzca una nueva dirección IP de puerta de enlace para el puerto IPMI. Pulse `Enter` al finalizar.
11. Conecte un extremo de un cable Ethernet al puerto IPMI y el otro extremo a un switch.

El puerto IPMI para este nodo está listo para usarse.

12. Repita este procedimiento para todos los demás nodos NetApp HCI con puertos IPMI no configurados.

Cambie la contraseña de IPMI predeterminada para los nodos H410C y H410S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de computación y de almacenamiento.

Antes de empezar

Configuró la dirección IP de IPMI para cada nodo de almacenamiento y de computación.

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `ADMIN` y contraseña `ADMIN` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en la ficha **Configuración**.
4. Haga clic en **usuarios**.
5. Seleccione la `ADMIN` Haga clic en **Modificar usuario**.
6. Seleccione la casilla de verificación **Cambiar contraseña**.
7. Introduzca una nueva contraseña en los campos **Contraseña** y **Confirmar contraseña**.
8. Haga clic en **Modificar** y, a continuación, haga clic en **Aceptar**.
9. Repita este procedimiento para todos los demás nodos NetApp HCI H410C y H410S con contraseñas IPMI predeterminadas.

Cambie la contraseña de IPMI predeterminada para los nodos H610C, H615C y H610S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de computación y de almacenamiento.

Antes de empezar

Configuró la dirección IP de IPMI para cada nodo de almacenamiento y de computación.

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `root` y contraseña `calvin` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en el icono de navegación del menú que aparece en la parte superior izquierda de la página para abrir el cajón de la barra lateral.
4. Haga clic en **Configuración**.
5. Haga clic en **Administración de usuarios**.
6. Seleccione el usuario **Administrador** de la lista.
7. Active la casilla de verificación **Cambiar contraseña**.
8. Introduzca una nueva contraseña segura en los campos **Contraseña** y **Confirmar contraseña**.
9. Haga clic en **Guardar** en la parte inferior de la página.
10. Repita este procedimiento para todos los demás nodos NetApp HCI H610C, H615C o H610S con contraseñas de IPMI predeterminadas.

Obtenga más información

- ["Documentación de SolidFire Active IQ de NetApp"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Ponga en marcha NetApp HCI

Acceda al motor de implementación de NetApp

Información general de las opciones de acceso del motor de implementación de NetApp

Para implementar NetApp HCI, necesita acceso al motor de implementación de NetApp en uno de los nodos de almacenamiento de NetApp H-Series a través de la dirección IPv4 asignada a la interfaz Bond1G; esta es la interfaz lógica que combina los puertos A y B para los nodos de almacenamiento. Este nodo de almacenamiento se convierte en el nodo de almacenamiento de control para el proceso de implementación. Según el entorno, se debe configurar la dirección IPv4 o recuperarla de uno de los nodos de almacenamiento.



Solo se puede acceder al motor de implementación de NetApp con la interfaz Bond1G de un nodo de almacenamiento. No se admite el uso de la interfaz Bond10G, la interfaz lógica que combina los puertos C y D para los nodos de almacenamiento.

De los siguientes métodos, utilice el que mejor describa su entorno de red para acceder al motor de implementación de NetApp:

Situación	Método
No tiene DHCP en el entorno	"Acceda al motor de implementación de NetApp en entornos sin DHCP"
Tiene DHCP en el entorno	"Acceda al motor de implementación de NetApp en entornos con DHCP"
Desea asignar manualmente todas las direcciones IP	"Asignar manualmente todas las direcciones IP para acceder al motor de implementación de NetApp"

Obtenga más información

- ["Configure el acceso completo a la interfaz de usuario web de Nombre de dominio"](#)

Acceda al motor de implementación de NetApp en entornos sin DHCP

Cuando DHCP no está en uso en la red, se debe establecer la dirección IPv4 estática en la interfaz Bond1G de uno de los nodos de almacenamiento (también conocido como nodo de almacenamiento de control) que se utilizará para acceder al motor de implementación de NetApp. El motor de implementación de NetApp en el nodo de almacenamiento de control detecta y se comunica con otros nodos de almacenamiento mediante direcciones IPv4 configuradas automáticamente en las interfaces Bond10G de todos los nodos. Debe usar este método a menos que la red tenga requisitos especiales.

Lo que necesitará

- Usted o el administrador de red completaron las tareas del documento instrucciones de instalación y

configuración.

- Tiene acceso físico a los nodos del NetApp HCI.
- Todos los nodos del NetApp HCI están encendidos.
- DHCP no está habilitado para las redes NetApp HCI, y los nodos NetApp HCI no obtuvieron direcciones IP de los servidores DHCP.
- La red de gestión de NetApp HCI está configurada como la VLAN nativa en las interfaces Bond1G y Bond10G de todos los nodos.

Pasos

1. Conecte un KVM a la parte posterior de uno de los nodos de almacenamiento NetApp HCI (este nodo se convertirá en el nodo de almacenamiento de control).
2. Configure la dirección IP, la máscara de subred y la dirección de puerta de enlace para Bond1G en la interfaz de usuario. También puede configurar un ID de VLAN para la red Bond1G si es necesario.



No se puede reutilizar esta dirección IPv4 más adelante durante la implementación con el motor de implementación de NetApp.

3. Abra un explorador web en un equipo que pueda acceder a la red de gestión de NetApp HCI.
4. Vaya a la dirección IP que asignó al nodo de almacenamiento de control. Por ejemplo:

```
http://<Bond1G IP address>
```



Asegúrese de utilizar HTTP aquí.

Esto lo llevará hasta la interfaz de usuario del motor de implementación de NetApp.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Acceda al motor de implementación de NetApp en entornos con DHCP

En los entornos donde los servidores adquieren automáticamente la configuración de IPv4 desde DHCP, es posible acceder al motor de implementación de NetApp con la dirección IPv4 asignada a la interfaz Bond1G en uno de los nodos de almacenamiento. Puede usar un stick USB para recuperar la dirección IPv4 de uno de los nodos de almacenamiento. El motor de implementación de NetApp detecta automáticamente otros nodos de almacenamiento y computación que utilizan direcciones IPv4 asignadas por DHCP. No debe utilizar este método a menos que la red tenga requisitos especiales.

Lo que necesitará

- Usted o el administrador de red completaron las tareas del documento instrucciones de instalación y configuración.
- Tiene acceso físico a los nodos del NetApp HCI.

- Todos los nodos del NetApp HCI están encendidos.
- DHCP está habilitado en las redes de almacenamiento y gestión de NetApp HCI.
- El pool de direcciones de DHCP es lo suficientemente grande para admitir dos direcciones IPv4 por nodo NetApp HCI.



Para una correcta implementación de NetApp HCI, todos los nodos de la implementación deben tener direcciones IPv4 autoconfiguradas o adquiridas por DHCP (no se pueden mezclar los métodos de asignación de direcciones IPv4).

Acerca de esta tarea

Si DHCP está en uso solo para la red de almacenamiento (interfaces Bond10G), debe usar los pasos descritos en el enlace: ["Acceda al motor de implementación de NetApp en entornos sin DHCP"](#) Para acceder al motor de implementación de NetApp.

Pasos

1. Los nodos tardan varios minutos en solicitar las direcciones IP.
2. Elija un nodo de almacenamiento e inserte un stick USB en el nodo. Déjelo insertado durante al menos cinco segundos.
3. Retire el stick USB e insértelo en el equipo.
4. Abra el `readme.html` archivo. Esto lo llevará hasta la interfaz de usuario del motor de implementación de NetApp.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Asignar manualmente todas las direcciones IP para acceder al motor de implementación de NetApp

Es posible asignar manualmente direcciones IPv4 estáticas a las interfaces Bond1G y Bond10G de todos los nodos NetApp HCI para acceder al motor de implementación de NetApp e implementar NetApp HCI. No debe utilizar este método a menos que la red tenga requisitos especiales.

Lo que necesitará

- Usted o el administrador de red completaron las tareas del documento instrucciones de instalación y configuración.
- Tiene acceso físico a los nodos del NetApp HCI.
- Todos los nodos del NetApp HCI están encendidos.
- DHCP no está habilitado para las redes NetApp HCI, y los nodos NetApp HCI no obtuvieron direcciones IP de los servidores DHCP. NOTA: Todas las direcciones IP que se asignan manualmente antes de utilizar el motor de implementación de NetApp para implementar el sistema son temporales y no se pueden reutilizar. Si decide asignar manualmente direcciones IP, debe separar un conjunto secundario permanente de direcciones IP sin usar que se puedan asignar durante la implementación final.

Acerca de esta tarea

En esta configuración, los nodos de computación y de almacenamiento utilizan direcciones IPv4 estáticas para

detectar otros nodos y comunicarse con ellos durante la implementación. No se recomienda utilizar esta configuración.

Pasos

1. Conecte un KVM a la parte posterior de uno de los nodos de almacenamiento NetApp HCI (este nodo se convertirá en el nodo de almacenamiento de control).
2. Configure la dirección IP, la máscara de subred y la dirección de puerta de enlace para Bond1G y Bond10G en la interfaz de usuario. También puede configurar un identificador de VLAN para cada red si es necesario.
3. Repita el paso 2 para los nodos restantes de almacenamiento y computación.
4. Abra un explorador web en un equipo que pueda acceder a la red de gestión de NetApp HCI.
5. Vaya a la dirección IP de Bond1G que asignó al nodo de almacenamiento de control. Por ejemplo:

```
http://<Bond1G IP address>
```

Esto lo llevará hasta la interfaz de usuario del motor de implementación de NetApp.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Inicie la implementación

Antes de continuar con la implementación de NetApp HCI, debe leer y comprender los contratos de licencia para usuario final.

Pasos

1. En la página **Bienvenido a NetApp HCI**, haga clic en **comenzar**.
2. En la página **requisitos previos**, haga lo siguiente:
 - a. Compruebe que se cumpla cada requisito previo y haga clic en cada casilla asociada para confirmar.
 - b. Haga clic en **continuar**.
3. En la página **licencias de usuario final**, haga lo siguiente:
 - a. Lea el contrato de licencia para usuario final de NetApp.
 - b. Si acepta los términos, haga clic en **Acepto** en la parte inferior del texto del acuerdo.
 - c. Lea el contrato de licencia para usuario final de VMware.
 - d. Si acepta los términos, haga clic en **Acepto** en la parte inferior del texto del acuerdo.
 - e. Haga clic en **continuar**.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Importe un perfil de instalación

Si obtiene la ayuda de NetApp "[ConfigBuilder](#)" Resultado de perfil para la instalación, puede importarlo durante el proceso de instalación de NetApp HCI para que rellene automáticamente los campos en el motor de puesta en marcha de NetApp. Este es un paso opcional.

Acerca de esta tarea

Si importa un perfil de instalación, tiene que introducir credenciales para que NetApp HCI las utilice en la página **credenciales** del motor de implementación de NetApp.



Si los campos del perfil de instalación se dejan en blanco o se introducen incorrectamente, es posible que deba introducir o corregir manualmente la información en las páginas del motor de implementación de NetApp. Si necesita agregar o corregir información, asegúrese de actualizar la información de los registros y del perfil de instalación.

Importar un perfil

1. En la página **Perfil de instalación**, haga clic en **examinar** para buscar y cargar su perfil de instalación.
2. En el cuadro de diálogo File, seleccione y abra el archivo JSON de perfiles.
3. Una vez que el perfil se haya importado correctamente, haga clic en **continuar**.

Es posible recorrer cada página del motor de implementación de NetApp y comprobar la configuración que se ha importado del perfil de instalación.

Continúe sin importar un perfil

1. Para omitir el paso de importación, en la página **Perfil de instalación**, haga clic en **continuar**.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Configure VMware vSphere

Configuración de VMware vSphere

NetApp HCI utiliza los componentes de vCenter Server y ESXi de VMware vSphere. VCenter Server se utiliza para gestionar y supervisar el hipervisor ESXi de VMware instalado en cada nodo de computación. Puede instalar y configurar una nueva puesta en marcha de vSphere, que también instala el plugin de NetApp Element para vCenter Server, o bien puede unir y ampliar una puesta en marcha de vSphere existente.

Tenga en cuenta las siguientes salvedades cuando utilice el motor de implementación de NetApp para instalar una implementación de vSphere nueva:

- El motor de implementación de NetApp instala la nueva instancia de vCenter Server Appliance con la opción de implementación de tamaño pequeño.

- La licencia de vCenter Server es una licencia de evaluación temporal. Para extender el funcionamiento después del período de evaluación, se debe obtener una clave de licencia nueva de VMware y añadirla al inventario de licencias de vCenter Server.



Si la configuración de inventario de vSphere utiliza una carpeta para almacenar el clúster de NetApp HCI en el centro de datos de vCenter, se producirá un error en algunas operaciones, como la ampliación de los recursos de computación de NetApp HCI. Compruebe que el clúster de NetApp HCI se encuentre directamente en el centro de datos en el árbol de inventario del cliente web de vSphere y que no se almacene en una carpeta. Consulte el artículo de la base de conocimientos de NetApp para obtener más información.

Si se instala una nueva instancia de vCenter Server, es posible instalar un switch estándar de vSphere o un switch distribuido de vSphere (VDS) durante la configuración de red. Un VDS permite una gestión de red de máquinas virtuales simplificada y centralizada después de la implementación de NetApp HCI. La funcionalidad de servicios de datos cloud en NetApp HCI requiere VDS; los switches estándar de vSphere no son compatibles con los servicios de datos en el cloud.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Configurar un nuevo entorno de VMware vSphere

Es posible implementar un nuevo entorno de vSphere como parte del proceso de instalación de NetApp HCI. Para ello, se deben proporcionar algunos datos de la red que debe utilizar vSphere. Tenga en cuenta que si configura vSphere con una dirección IP, la dirección no se puede cambiar después de la instalación.

Lo que necesitará

Obtuvo la información de red para el entorno de vSphere planificado.

Pasos

1. Haga clic en **Configurar una nueva implementación de vSphere**.
2. Seleccione la versión de vSphere que el sistema debe instalar durante la implementación.
3. Configure el nuevo entorno de vSphere mediante una de las siguientes opciones:

Opción	Pasos
Usar un nombre de dominio (recomendado).	<ol style="list-style-type: none"> a. Haga clic en Configurar utilizando un nombre de dominio completo. b. Introduzca el nombre de dominio de vCenter Server en el campo vCenter Server Fully Qualified Domain Name. c. Introduzca la dirección IP del servidor DNS en el campo Dirección IP del servidor DNS. d. Haga clic en continuar.

Opción	Pasos
Usar una dirección IP.	a. Haga clic en Configurar mediante una dirección IP . b. Haga clic en continuar .

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Únase a una puesta en marcha de VMware vSphere existente

Puede configurar NetApp HCI para aprovechar la puesta en marcha de vSphere existente proporcionando la información de red de vCenter Server y las credenciales.

Lo que necesitará

- Si se une a una puesta en marcha existente de vSphere 6.7, asegúrese de que vCenter Server ejecute la versión 6.7 Update 1.
- Si se une a una puesta en marcha existente de vSphere 6.5, asegúrese de que vCenter Server ejecute la versión 6.5 Update 2 o una versión posterior.
- Obtenga los detalles de la red y las credenciales de administrador para la implementación existente de vSphere.
- Si el plugin de NetApp Element para vCenter Server está registrado en la instancia existente de vCenter, tendrá que hacerlo **"cancele el registro"** antes de continuar. El plugin se vuelve a registrar una vez completada la implementación de NetApp HCI.

Acerca de esta tarea

Si se unen varios sistemas de vCenter Server conectados mediante vCenter Linked Mode, NetApp HCI solo reconoce uno de los sistemas de vCenter Server.



- A partir del plugin de Element para vCenter Server 5.0, se debe usar **"vCenter Linked Mode"**. Se registra el plugin de Element desde un nodo de gestión independiente para cada instancia de vCenter Server que administra los clústeres de almacenamiento de SolidFire de NetApp (recomendado).
- Usar el plugin de Element para vCenter Server 4.10 y versiones anteriores para gestionar recursos de clúster desde otras instancias de vCenter Server mediante **"vCenter Linked Mode"** solo se limita a clústeres de almacenamiento local.

Pasos

1. Haga clic en **Join and extend an existing vSphere deployment**.
2. Introduzca el nombre de dominio o la dirección IP en el campo **vCenter Server Domain Name or IP address**. Si introduce un nombre de dominio, también debe introducir la dirección IP de un servidor DNS activo en el campo **Dirección IP del servidor DNS** que aparece.
3. Introduzca las credenciales de un administrador de vSphere en los campos **User Name y Password**.
4. Haga clic en **continuar**.



Si el plugin de NetApp Element para vCenter Server se registró durante este paso, se muestra un mensaje de error que indica que el usuario "[cancele el registro](#)" el plugin. Antes de continuar con la implementación de NetApp HCI. El plugin se vuelve a registrar una vez completada la implementación.

Obtenga más información

- "[Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI](#)"

Configurar las credenciales de NetApp HCI

Durante la implementación, se define un conjunto de credenciales para utilizar en el entorno de VMware vSphere recién implementado, los recursos de computación y almacenamiento de NetApp HCI y el nodo de gestión. Si va a implementar NetApp HCI en un entorno de vSphere existente, estas credenciales no se aplican a la instancia existente de vCenter Server.

Acerca de esta tarea

Recuerde los puntos siguientes acerca de las credenciales establecidas en el motor de implementación de NetApp HCI:

- **NetApp Hybrid Cloud Control (HCC) o Element UI:** Para iniciar sesión en NetApp HCC o en la interfaz de usuario de Element una vez realizada correctamente la implementación, utilice el nombre de usuario y la contraseña especificados en este paso de implementación.
- **VMware vCenter:** Para iniciar sesión en vCenter (si está instalado como parte de la implementación), utilice el nombre de usuario con el sufijo `@vsphere.local` o el incorporado `Administrator@vsphere.local` cuenta de usuario y la contraseña especificada en este paso de implementación.
- **VMware ESXi:** Para iniciar sesión en ESXi en los nodos de computación, utilice el nombre de usuario `root` y la misma contraseña especificada en este paso de implementación.

Para interactuar con las instancias de VMware vCenter, el control del cloud híbrido de NetApp utilizará una de las siguientes opciones:

- El incorporado `Administrator@vsphere.local` Cuenta de usuario en la instancia de vCenter que se instaló como parte de la implementación.
- Las credenciales de vCenter que se utilizaron para conectar la puesta en marcha de NetApp HCI a una instancia existente de VMware vCenter Server.

Pasos

1. En la página **credenciales**, introduzca un nombre de usuario en el campo **Nombre de usuario**.
2. Introduzca una contraseña en el campo **Contraseña**. La contraseña debe cumplir los criterios de contraseña que aparecen en el cuadro **la contraseña debe contener**.
3. Confirme la contraseña en el campo **Volver a introducir contraseña**.
4. Haga clic en **continuar**.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)
- Para actualizar las credenciales de vCenter y ESXi más adelante, consulte ["Actualice las credenciales de vCenter o ESXi"](#).

Seleccione una topología de red

Durante el cableado de los nodos de NetApp HCI, existe la opción de usar configuraciones de cables de red diferentes según las necesidades. Para cada nodo de computación, es posible usar los seis puertos de red con diferentes tipos de tráfico asignados a cada par de puertos, o es posible usar dos puertos con todos los tipos de tráfico asignados a los puertos. Para los nodos de almacenamiento, se usa la configuración de cuatro cables estándar. Su elección afectará los nodos de computación que se puedan seleccionar en el inventario.

Lo que necesitará

Si selecciona la topología de red de dos cables para los nodos de computación, debe tener en cuenta los siguientes requisitos:

- Tiene una licencia VMware vSphere Enterprise Plus lista para aplicar después de completar la implementación.
- Verificó que la configuración de la red y los switches de red es correcta.
- Se requiere el etiquetado de VLAN en las redes de vMotion y de almacenamiento para todos los nodos de computación y de almacenamiento.

Pasos

1. En la página **topología de red**, seleccione una topología de nodo de computación que se ajuste a la manera en que instaló los nodos de computación para NetApp HCI:
 - **6 cable Option:** La opción de seis cables proporciona puertos dedicados para cada tipo de tráfico (administración, máquina virtual y almacenamiento). De manera opcional, es posible habilitar vSphere Distributed Switch (VDS). Al habilitar VDS, se configura un switch distribuido con el que es posible gestionar de forma simple y centralizada la configuración de red de las máquinas virtuales una vez completada la implementación de NetApp HCI. Si se habilita esta función, debe tener una licencia vSphere Enterprise Plus lista para aplicar después de la implementación.
 - **2 cable Option:** La opción de dos cables combina el tráfico de gestión, máquinas virtuales y almacenamiento en dos puertos Unidos. Esta opción de cableado requiere VDS y lo habilita automáticamente. Debe tener una licencia vSphere Enterprise Plus lista para aplicar después de la implementación.
2. Algunas opciones de cableado muestran varias vistas del panel posterior de diferentes tipos de hardware de nodos. Desplácese por las vistas del panel posterior para ver cómo conectar los cables de red para ese modelo de nodo específico y la opción de cableado.
3. Cuando termine, haga clic en **continuar**.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Selección de inventario

Selección de inventario y compatibilidad de nodos

Al elegir nodos para su implementación, algunas restricciones se aplican a las configuraciones de nodos que puede combinar en la misma implementación.

Compatibilidad del nodo de almacenamiento

NetApp HCI admite nodos de almacenamiento y unidades con la funcionalidad de cifrado de unidades SED (unidad de cifrado automático) y FIPS 140-2-2. Al poner en marcha o ampliar NetApp HCI, se pueden combinar nodos con diferentes niveles de cifrado reportados, pero NetApp HCI solo admite una forma más básica de cifrado en esta situación. Por ejemplo, si combina un nodo de almacenamiento que es compatible con el cifrado FIPS con nodos que solo admiten el cifrado SED, el cifrado SED es compatible con esta configuración, pero el cifrado de unidad FIPS no lo es.



Añadir nodos de almacenamiento capaces de cifrar unidades FIPS en el clúster de almacenamiento no habilita automáticamente la función de cifrado de unidades FIPS. Después de implementar o expandir una instalación con nodos compatibles con FIPS, debe habilitar manualmente el cifrado de unidades FIPS. Consulte "[Documentación del software Element](#)" si desea obtener instrucciones.

Todos los nodos de almacenamiento deben ejecutar la misma versión secundaria del software Element para que sean compatibles con la misma puesta en marcha. Por ejemplo, no es posible mezclar un nodo de almacenamiento que ejecuta Element 11.3.1 con otros nodos de almacenamiento que ejecutan Element 11.5.



Según la configuración de hardware de un nodo, los nodos de almacenamiento H410S pueden aparecer en la lista de inventario etiquetada como H300S, H500S o H700S.

NetApp HCI solo admite algunos modelos de nodo de almacenamiento en clústeres de almacenamiento de dos nodos. Para obtener más información, consulte "[clústeres de almacenamiento de dos nodos](#)" O las notas de la versión de NetApp HCI.



Para puestas en marcha de clústeres de almacenamiento de dos nodos, los tipos de nodos de almacenamiento se limitan a los nodos con unidades de 480 GB y 960 GB.

Compatibilidad del nodo de computación

Los nodos de computación deben cumplir con los siguientes requisitos para poder seleccionarse como inventario:

- Las generaciones de CPU de todos los nodos de computación deben coincidir para que VMware vMotion funcione correctamente. Después de seleccionar un nodo de computación del inventario, no se pueden seleccionar nodos de computación con generaciones de CPU diferentes.
- No se pueden combinar nodos de computación con nodos de computación habilitados para GPU en el mismo clúster de computación. Si selecciona un nodo de computación habilitado para GPU, los nodos de computación solo para CPU pasan a ser inSeleccionables y viceversa.
- La versión de software que se ejecuta en el nodo de computación debe coincidir con la versión principal y secundaria del motor de puesta en marcha de NetApp que aloja la puesta en marcha. Si este no es el caso, debe volver a crear la imagen del nodo de computación mediante el proceso RTFI. Consulte los artículos de la base de conocimientos de NetApp sobre RTFI para obtener instrucciones.

- El nodo de computación debe tener la configuración de cableado seleccionada en la página Topología de red para poder seleccionarse en la lista **nodos de computación**.
- Las configuraciones de cableado de red para nodos de computación del mismo modelo deben coincidir en un único clúster de computación.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación sobre SolidFire y el software Element"](#)

Seleccione un inventario

En la página **Inventory**, el motor de implementación de NetApp detecta automáticamente los nodos de almacenamiento y de computación disponibles, lo que permite seleccionar y agregar todos los recursos de NetApp HCI a la implementación. Si un nodo no cumple con los requisitos de la implementación, no se puede seleccionar y los problemas se indican como errores. Puede colocar el cursor sobre el error en la fila del nodo para ver una explicación. Al elegir el inventario de nodos en la página Inventory, el nodo de almacenamiento que aloja el motor de implementación de NetApp se selecciona automáticamente y no puede anular la selección.

Lo que necesitará

Las tramas gigantes deben estar habilitadas para una detección de inventario correcta. Si no aparecen nodos ni solo un subconjunto de nodos en el inventario, compruebe que los puertos del switch utilizados para los nodos de NetApp HCI (todas las interfaces SFP+/SFP28) estén configurados con tramas gigantes.

Pasos

1. En la página **Inventario**, consulte la lista de nodos disponibles.

Si el sistema no puede detectar ningún inventario, se muestra un error. Corrija el error antes de continuar. Si el sistema utiliza DHCP para la asignación de direcciones IP, es posible que los recursos de computación y de almacenamiento no se muestren en el inventario de forma inmediata.

2. Opcional: Si un recurso no aparece inmediatamente en el inventario o si debe solucionar un error y actualizar el inventario, haga clic en **Actualizar inventario**. Es posible que deba actualizar el inventario varias veces.
3. Opcional: Para filtrar el inventario por atributos de nodo, como el tipo de nodo:
 - a. Haga clic en **filtro** en el encabezado de las listas **nodos de computación** o **nodos de almacenamiento**.
 - b. Elija criterios de las listas desplegadas.
 - c. Debajo de las listas desplegadas, introduzca información para cumplir los criterios.
 - d. Haga clic en **Agregar filtro**.
 - e. Borre los filtros individuales haciendo clic en **X** junto a un filtro activo o borrando todos los filtros haciendo clic en **X** encima de la lista de filtros.
4. Seleccione todos los nodos de computación que se enviaron con el sistema en la lista **nodos de computación**.

Debe seleccionar al menos dos nodos de computación para continuar con la implementación.

5. En la lista **nodos de almacenamiento**, seleccione todos los nodos de almacenamiento que se enviaron con el sistema.

Debe seleccionar al menos dos nodos de almacenamiento para continuar con la implementación.

6. Opcional: Si la casilla de selección de un nodo de almacenamiento tiene una Marca, ese nodo supera el 33 % de la capacidad total del clúster de almacenamiento. Haga lo siguiente:
 - Desactive la casilla de selección para el nodo de almacenamiento con una Marca.
 - Seleccione nodos de almacenamiento adicionales para distribuir más uniformemente la capacidad del clúster de almacenamiento entre los nodos.
7. Haga clic en **continuar**.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Configure los ajustes de red

NetApp HCI proporciona una página de ajustes de red con varias secciones para simplificar la configuración de red. Puede continuar por cada sección e introducir información o asignar direcciones IP a los hosts y nodos de cada red.

Lo que necesitará

- Obtuvo la siguiente información:
 - El prefijo de nombre planificado para los hosts y el clúster de almacenamiento
 - La máscara de subred, la dirección IP inicial, la puerta de enlace predeterminada y los identificadores de VLAN planificados para las redes de gestión, iSCSI y vMotion
 - La máscara de subred, la dirección IP, la puerta de enlace predeterminada y los identificadores de VLAN para las implementaciones de VMware vCenter planificadas
 - La dirección del servidor del protocolo de tiempo de redes (NTP) para NetApp HCI
 - La información de dirección IP del servidor DNS para NetApp HCI
- Si desea implementar una instancia de vSphere Distributed Switch, debe tener una licencia vSphere Enterprise Plus lista para aplicar después de completar la implementación.
- Si asignó identificadores de VLAN a puertos de nodo durante la configuración de la interfaz de usuario de terminal (TUI), ha configurado esos puertos con el mismo ID de VLAN durante la configuración de red. No es necesario configurar puertos de host etiquetados como puertos de acceso o VLAN nativas en los puertos del switch conectados.
- Comprobó que la configuración del switch de red es correcta. Una configuración incorrecta del switch (como redes VLAN o tamaños de MTU incorrectos) produce errores en la implementación.

Acerca de esta tarea

Si seleccionó la topología de red de dos cables para los nodos de computación, debe usar identificadores de VLAN para las redes de almacenamiento y de vMotion de todos los nodos de computación y de almacenamiento en la implementación (los identificadores de VLAN son opcionales para las redes de gestión). Tenga en cuenta que NetApp HCI valida las direcciones IP que introduzca durante estos pasos, pero puede

desactivar esta validación con el botón **validación de red en directo es**. NetApp HCI también realiza comprobaciones con otra información que introduce durante estos pasos, como garantizar que no se solapen las subredes, garantizando que no se asigne ningún identificador de VLAN a varias redes y otras validaciones básicas.



En entornos que requieren el etiquetado de VLAN en el lado del host antes de la puesta en marcha, si ha configurado identificadores de VLAN en los nodos de computación y de almacenamiento, de manera que sean detectables por el motor de puesta en marcha de NetApp, asegúrese de utilizar las VLAN correctas al configurar la configuración de red en el motor de puesta en marcha de NetApp.

Si va a implementar un clúster de almacenamiento de dos o tres nodos, puede completar la información de la dirección IP de los nodos testigo en la página **Configuración de red**.



En las páginas de asignación de direcciones IP, la información que introduzca en el modo **asignar automáticamente direcciones IP** no afecta a la información introducida en el modo **asignar manualmente direcciones IP** y viceversa. Si introduce direcciones IP en ambos modos, NetApp HCI utiliza la información de la dirección IP en cualquier modo que esté activo al hacer clic en **continuar** en la parte inferior de la página.

Resolución de problemas comunes

NetApp HCI realiza comprobaciones sobre la información que introduce en estas páginas. A continuación se presentan algunos problemas y soluciones comunes:

Problema	Solución alternativa
En el modo de asignación automática de direcciones IP, después de introducir una dirección IP inicial, verá el mensaje <code>IPs in the range are in use</code> : Con una lista desplegable desplazable de las direcciones IP en uso.	NetApp HCI ha asignado un rango contiguo de direcciones IP, pero una o varias de esas direcciones IP ya están en uso. Libere las direcciones IP en uso y vuelva a intentarlo, o utilice el modo de asignación manual de direcciones IP para asignar direcciones IP específicas.
Tras introducir una puerta de enlace predeterminada, aparecerá el mensaje <code>The gateway is not valid</code> .	La dirección IP de la puerta de enlace predeterminada no coincide con la subred que ha proporcionado o hay un problema con la red o el servidor que debe resolver. Consulte los siguientes artículos de la base de conocimientos de NetApp si desea obtener más información: <ul style="list-style-type: none"> • "Solucione problemas de una puerta de enlace no válida en el motor de implementación de NetApp" • "La puerta de enlace no es válida en el motor de implementación de NetApp"
Ha completado varias páginas de configuración Configuración de red y se ha dado cuenta de que hay información incorrecta sobre una de las páginas anteriores en la secuencia.	Mediante la secuencia de páginas numeradas en la parte superior de la página, puede seleccionar una página que haya completado previamente y cambiar la información allí. Cuando haya terminado, puede hacer clic en continuar en las páginas completadas para volver a la página actual.

Configure los ajustes de DNS y NTP

Pasos

1. En la página **DNS/NTP**, introduzca la información del servidor DNS y NTP para NetApp HCI en los siguientes campos:

Campo	Descripción
Dirección IP del servidor DNS 1	La dirección IP del servidor DNS primario para NetApp HCI. Si especificó un servidor DNS en la página vCenter Configuration, este campo se rellena y es de solo lectura.
Dirección IP del servidor DNS 2 (opcional)	La dirección IP opcional de un servidor DNS secundario para NetApp HCI.
Dirección del servidor NTP 1	La dirección IP o el nombre de dominio completo del servidor NTP primario para esta infraestructura.
Dirección del servidor NTP 2 (opcional)	Una dirección IP opcional o un nombre de dominio completo del servidor NTP secundario para esta infraestructura.

Asigne identificadores de VLAN

En la página **VLAN IDs**, puede asignar identificadores de VLAN a redes NetApp HCI. También puede optar por no utilizar los identificadores de VLAN. Si seleccionó la topología de red de dos cables para los nodos de computación, debe usar identificadores de VLAN para las redes de almacenamiento y de vMotion de todos los nodos de computación y de almacenamiento en la implementación (los identificadores de VLAN son opcionales para las redes de gestión).



Cuando asigna identificadores de VLAN, está configurando etiquetas de VLAN que NetApp HCI aplicará al tráfico de red. No es necesario introducir la VLAN nativa como un identificador de VLAN; para utilizar la VLAN nativa para una red, deje el campo correspondiente vacío.

Pasos

Seleccione una de las siguientes opciones:

Opción	Pasos
Asigne identificadores de VLAN	<ol style="list-style-type: none">1. Seleccione Sí para la opción * Will you assign VLAN IDs*.2. En la columna VLAN ID, introduzca una etiqueta VLAN que se utilizará para cada tipo de tráfico de red que desee asignar a una VLAN. Tanto el tráfico de vMotion como el tráfico de iSCSI de computación deben utilizar un identificador de VLAN no compartido.3. Haga clic en continuar.

Opción	Pasos
No asigne identificadores de VLAN	<ol style="list-style-type: none"> 1. Seleccione no para la opción Will you assign VLAN IDs. 2. Haga clic en continuar.

Configure la red de gestión

En la página **Administración**, puede elegir que NetApp HCI rellene automáticamente los rangos de direcciones IP para las redes de administración en función de una dirección IP inicial o puede elegir introducir manualmente toda la información de direcciones IP.

Pasos

Seleccione una de las siguientes opciones:

Opción	Pasos
Asignar automáticamente direcciones IP	<ol style="list-style-type: none"> 1. Seleccione la opción asignar direcciones IP automáticamente. 2. En la columna Subnet, introduzca una definición de subred en formato CIDR para cada VLAN. 3. En la columna Default Gateway, introduzca una puerta de enlace predeterminada para cada VLAN. 4. En la columna Subnet, introduzca una dirección IP inicial que se utilizará para cada VLAN y tipo de nodo. NetApp HCI rellena automáticamente las direcciones IP finales para cada host o grupo de hosts. 5. Haga clic en continuar.
Asignar manualmente direcciones IP	<ol style="list-style-type: none"> 1. Seleccione la opción asignar manualmente direcciones IP. 2. En la columna Subnet, introduzca una definición de subred en formato CIDR para cada VLAN. 3. En la columna Default Gateway, introduzca una puerta de enlace predeterminada para cada VLAN. 4. En la fila de cada host o nodo, introduzca la dirección IP para ese host o nodo. 5. Introduzca la dirección IP virtual de gestión (MVIP) para la red de gestión. 6. Haga clic en continuar.

Configure la red de vMotion

En la página **vMotion**, puede optar por que NetApp HCI rellene automáticamente los rangos de direcciones IP para la red de vMotion en función de una dirección IP inicial o puede optar por introducir manualmente toda la información de direcciones IP.

Pasos

Seleccione una de las siguientes opciones:

Opción	Pasos
Asignar automáticamente direcciones IP	<ol style="list-style-type: none">1. Seleccione la opción asignar direcciones IP automáticamente.2. En la columna Subnet, introduzca una definición de subred en formato CIDR para cada VLAN.3. (Opcional) en la columna Default Gateway, introduzca una puerta de enlace predeterminada para cada VLAN.4. En la columna Subnet, introduzca una dirección IP inicial que se utilizará para cada VLAN y tipo de nodo. NetApp HCI rellena automáticamente las direcciones IP finales para cada host o grupo de hosts.5. Haga clic en continuar.
Asignar manualmente direcciones IP	<ol style="list-style-type: none">1. Seleccione la opción asignar manualmente direcciones IP.2. En la columna Subnet, introduzca una definición de subred en formato CIDR para cada VLAN.3. (Opcional) en la columna Default Gateway, introduzca una puerta de enlace predeterminada para cada VLAN.4. En la fila de cada host o nodo, introduzca la dirección IP para ese host o nodo.5. Haga clic en continuar.

Configure la red iSCSI

En la página **iSCSI**, puede elegir que NetApp HCI rellene automáticamente los rangos de direcciones IP para la red iSCSI basándose en una dirección IP inicial o puede elegir introducir manualmente toda la información de direcciones IP.

Pasos

Seleccione una de las siguientes opciones:

Opción	Pasos
Asignar automáticamente direcciones IP	<ol style="list-style-type: none"> 1. Seleccione la opción asignar direcciones IP automáticamente. 2. En la columna Subnet, introduzca una definición de subred en formato CIDR para la red iSCSI. 3. (Opcional) en la columna Default Gateway, introduzca una puerta de enlace predeterminada para la red iSCSI. 4. En la columna Subnet, introduzca una dirección IP inicial que se utilizará para cada tipo de nodo. NetApp HCI rellena automáticamente las direcciones IP finales para cada host o grupo de hosts. 5. Haga clic en continuar.
Asignar manualmente direcciones IP	<ol style="list-style-type: none"> 1. Seleccione la opción asignar manualmente direcciones IP. 2. En la columna Subnet, introduzca una definición de subred en formato CIDR para la red iSCSI. 3. (Opcional) en la columna Default Gateway, introduzca una puerta de enlace predeterminada para la red iSCSI. 4. En la sección nodo de gestión, introduzca una dirección IP para el nodo de administración. 5. Para cada nodo de la sección nodos de computación, introduzca las direcciones IP iSCSI A e iSCSI B. 6. En la fila Storage Virtual IP (SVIP), introduzca la dirección IP SVIP para la red iSCSI. 7. En las filas restantes, para cada host o nodo, introduzca la dirección IP de ese host o nodo. 8. Haga clic en continuar.

Asigne los nombres de clúster y host

En la página **Nomenclatura**, puede optar por que NetApp HCI rellene automáticamente el nombre del clúster y los nombres de los nodos del clúster en función de un prefijo de nomenclatura. También puede elegir introducir manualmente todos los nombres del clúster y los nodos.

Pasos

Seleccione una de las siguientes opciones:

Opción	Pasos
Asignar automáticamente nombres de clúster y host	<ol style="list-style-type: none"> 1. Seleccione la opción asignar automáticamente nombres de clúster/host. 2. En la sección prefijo de instalación, introduzca un prefijo de nombre que se utilizará para todos los nombres de host de nodo del clúster (incluidos los nodos testigo y nodo de administración). NetApp HCI rellena automáticamente los nombres de host según el tipo de nodo, así como sufijos para los nombres de nodos comunes (como los nodos de computación y de almacenamiento). 3. (Opcional) en la columna Esquema de nomenclatura, modifique cualquiera de los nombres resultantes para los hosts. 4. Haga clic en continuar.
Asignar manualmente los nombres de clúster y host	<ol style="list-style-type: none"> 1. Seleccione la opción asignar manualmente nombres de clúster/host. 2. En la columna Host / Cluster Name, introduzca el nombre de host de cada host y un nombre de clúster para el clúster de almacenamiento. 3. Haga clic en continuar.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Revisar e implementar la configuración

Antes de iniciar la implementación, es posible revisar la información proporcionada. También es posible corregir los datos incorrectos o incompletos antes de continuar.



Durante la implementación, el proceso de instalación del nodo de gestión crea volúmenes con nombres que comienzan con `NetApp-HCI-` En el clúster de almacenamiento de Element y una cuenta de SolidFire que comienza con el nombre `tenant_`. No elimine estos volúmenes o cuentas; si lo hace, se producirá una pérdida en la funcionalidad de gestión.

Pasos

1. Opcional: Seleccione el icono **Descargar** para descargar la información de instalación en formato CSV. Puede guardar este archivo y consultarlo posteriormente para obtener información de configuración.



Puede importar el archivo CSV como perfil de instalación en la página **Perfil de instalación** del motor de puesta en marcha de NetApp (NDE) si es necesario durante una instalación futura.

2. Expanda cada sección y revise la información. Para expandir todas las secciones a la vez, seleccione **expandir todo**.
3. Opcional: Para hacer cambios en la información de una sección que se muestra:
 - a. Seleccione **Editar** en la sección correspondiente.
 - b. Realice los cambios necesarios.
 - c. Seleccione **continuar** hasta que llegue a la página **Revisión**. La configuración anterior se guarda en cada página.
 - d. Repita los pasos 2 y 3 para hacer otros cambios que sean necesarios.
4. Si no desea enviar estadísticas del clúster ni información de soporte a los servidores SolidFire Active IQ alojados en NetApp, desactive la casilla de comprobación final.

Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.

5. Si toda la información es correcta, seleccione **Iniciar despliegue**.

Aparecerá un cuadro de diálogo. En caso de que se produzcan problemas eléctricos o de conectividad de red durante el proceso de configuración final, o si se pierde la sesión del explorador, es posible copiar la URL que se muestra en el cuadro de diálogo y utilizarla para ir a la página de progreso de configuración final.

6. Revise la información en el cuadro de diálogo y seleccione **Copiar en Portapapeles** para copiar la URL en el portapapeles.
7. Guarde la URL en un archivo de texto en el equipo.
8. Cuando esté listo para continuar con la implementación, seleccione **OK**.

Se inicia la implementación y se muestra una página de progreso. No cierre la ventana del explorador ni salga de la página de progreso hasta que finalice la implementación. Si pierde la sesión del explorador por algún motivo, puede ir a la URL que copió anteriormente (y aceptar cualquier advertencia de seguridad que se muestre) para volver a obtener acceso a la página de progreso de configuración final.



Si se produce un error en la implementación, guarde el texto del mensaje de error y póngase en contacto con el soporte de NetApp.

Una vez completada la implementación, los nodos de computación pueden reiniciarse más de una vez antes de prepararse para el servicio.

Después de terminar

Empiece a usar NetApp HCI seleccionando **Iniciar vSphere**.



- Para las instalaciones de NetApp HCI mediante vSphere 6.7, este enlace inicia la interfaz web HTML5 de vSphere. Para las instalaciones que utilizan vSphere 6.5, este enlace inicia la interfaz web de Adobe Flash vSphere.
- En dos configuraciones de nodos de almacenamiento o tres, NDE configura los nodos del testigo para usar el almacén de datos local en los nodos de computación. Como resultado, el cliente vSphere muestra dos advertencias sobre el uso del almacén de datos en el disco*. Para continuar, seleccione el enlace **Restablecer a verde** en cada advertencia.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Tareas posteriores a la implementación

Tareas posteriores a la implementación

Según las opciones que elija durante el proceso de implementación, debe completar algunas tareas finales antes de que el sistema NetApp HCI esté listo para su uso en producción, como la actualización del firmware y los controladores, y la realización de los cambios finales de configuración necesarios.

- ["Cambios de red admitidos"](#)
- ["Deshabilite el servicio smartd en los nodos de computación de NetApp HCI"](#)
- ["Deshabilite el comando "laccp-individual" en los switches configurados"](#)
- ["Cree una función HCC de NetApp en vCenter"](#)
- ["Mantenga actualizado VMware vSphere"](#)
- ["Instale los controladores de GPU para los nodos de computación habilitados para GPU"](#)
- ["Acceda a Control del cloud híbrido de NetApp"](#)
- ["Reduzca el desgaste de los medios de arranque en un nodo de computación NetApp HCI"](#)

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Cambios de red admitidos

Después de implementar NetApp HCI, puede realizar cambios limitados en la configuración de red predeterminada. Sin embargo, se requieren ciertos ajustes para un funcionamiento fluido y una detección de red adecuada. Cambiar esta configuración provocará un comportamiento inesperado y podría evitar que amplíe los recursos de computación y almacenamiento.

Después de implementar el sistema, puede realizar los siguientes cambios en la configuración de red predeterminada en VMware vSphere, según lo dicten los requisitos de red:

- Cambie los nombres de vSwitch
- Cambie los nombres de grupo de puertos
- Agregar y quitar grupos de puertos adicionales
- Cambie el orden de conmutación por error de la interfaz vmnic para los grupos de puertos adicionales que haya agregado

Los nodos de computación H300E, H500E, H700E y H410C

NetApp HCI espera la siguiente configuración de red para los nodos H300E, H500E, H700E y H410C.

A continuación, se muestra una configuración de seis interfaces con VMware vSphere Distributed Switching (VDS). Esta configuración solo es compatible cuando se utiliza con switches distribuidos de VMware vSphere y requiere la licencia de VMware vSphere Enterprise Plus.

Función de red	vmkernel	vmnic (interfaz física)
Gestión	vmk0	Vmnic2 (puerto A), vmnic3 (puerto B)
ISCSI-a	vmk1	Vmnic5 (puerto E)
ISCSI-B	vmk2	Vmnic1 (puerto D)
VMotion	vmk3	Vmnic4 (puerto C), vmnic0 (puerto F)

A continuación se muestra una configuración de seis interfaces con VMware vSphere Standard Switching (VSS). Esta configuración utiliza VMware vSphere Standard Switch (VSS).

Función de red	vmkernel	vmnic (interfaz física)
Gestión	vmk0	Vmnic2 (puerto A), vmnic3 (puerto B)
ISCSI-a	vmk2	Vmnic1 (puerto E)
ISCSI-B	vmk3	Vmnic5 (puerto D)
VMotion	vmk1	Vmnic4 (puerto C), vmnic0 (puerto F)

A continuación se muestra una configuración con dos interfaces. Esta configuración solo se admite cuando se utiliza con switches distribuidos (VDS) de VMware vSphere y requiere una licencia de VMware vSphere Enterprise Plus.

Función de red	vmkernel	vmnic (interfaz física)
Gestión	vmk0	Vmnic1 (puerto D), vmnic5 (puerto E)
ISCSI-a	vmk1	Vmnic1 (puerto E)
ISCSI-B	vmk2	Vmnic5 (puerto D)

Función de red	vmkernel	vmnic (interfaz física)
VMotion	vmk3	Vmnic1 (puerto C), vmnic5 (puerto F)

Nodos de computación H610C

NetApp HCI espera la siguiente configuración de red para los nodos H610C.

Esta configuración solo se admite cuando se utiliza con switches distribuidos (VDS) de VMware vSphere y requiere una licencia de VMware vSphere Enterprise Plus.



Los puertos A y B no se utilizan en H610C.

Función de red	vmkernel	vmnic (interfaz física)
Gestión	vmk0	Vmnic2 (puerto C), vmnic3 (puerto D)
ISCSI-a	vmk1	Vmnic3 (puerto D)
ISCSI-B	vmk2	Vmnic2 (puerto C)
VMotion	vmk3	Vmnic2 (puerto C), vmnic3 (puerto D)

Nodos de computación H615C

NetApp HCI espera la siguiente configuración de red para los nodos H615C.

Esta configuración solo se admite cuando se utiliza con switches distribuidos (VDS) de VMware vSphere y requiere una licencia de VMware vSphere Enterprise Plus.

Función de red	vmkernel	vmnic (interfaz física)
Gestión	vmk0	Vmnic0 (puerto A), vmnic1 (puerto B)
ISCSI-a	vmk1	Vmnic0 (puerto B)
ISCSI-B	vmk2	Vmnic1 (puerto A)
VMotion	vmk3	Vmnic0 (puerto A), vmnic1 (puerto B)

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Deshabilite el servicio smartd en los nodos de computación de NetApp HCI

De forma predeterminada, el servicio `smartd` sondea periódicamente las unidades en

los nodos de computación. Debe deshabilitar este servicio en todos los nodos de computación después de implementar NetApp HCI.

Pasos

1. Con SSH o una sesión de consola local, inicie sesión en VMware ESXi en el nodo de computación usando credenciales raíz.
2. Detenga la ejecución smartd servicio:

```
/etc/init.d/smartd stop
```

3. Evite el smartd servicio desde el inicio en el arranque:

```
chkconfig smartd off
```

4. Repita estos pasos en el resto de los nodos de computación que se encuentran en la instalación.

Obtenga más información

- ["Apague el servicio inteligente en VMware ESXi"](#)
- ["Artículo de la base de conocimientos de VMware 2133286"](#)

Deshabilite el comando "lacp-individual" en los switches configurados

De forma predeterminada, el switch Mellanox lacp-individual Y el switch de Cisco lacp suspend-individual el comando se mantiene configurado tras la implementación. Este comando no es necesario después de la instalación; si sigue configurado, puede provocar problemas de acceso a volúmenes al solucionar problemas o reiniciar un switch. Tras la puesta en marcha, debe comprobar la configuración de cada switch de Mellanox y switch de Cisco y quitar el lacp-individual o lacp suspend-individual comando.

Pasos

1. Con SSH, abra una sesión al switch.
2. Muestre la configuración que se está ejecutando:

```
show running-config
```
3. Compruebe la salida de configuración del interruptor para lacp-individual o lacp suspend-individual comando.



La xxx-xxx son los números de interfaz proporcionados por el usuario. Si es necesario, puede acceder al número de interfaz mediante la visualización de las interfaces del grupo de agregación de enlaces de varios chasis: `show mlag interfaces`

- a. Para un conmutador Mellanox, compruebe si la salida contiene la siguiente línea:

```
interface mlag-port-channel xxx-xxx lacp-individual enable force
```

- b. Para un conmutador Cisco, compruebe si la salida contiene la siguiente línea:

```
interface mlag-port-channel xxx-xxx lacp suspend-individual enable force
```

4. Si el comando está presente, quitarlo de la configuración.

- a. Para un switch Mellanox:

```
no interface mlag-port-channel xxx-xxx lacp-individual enable force
```

- b. Para un switch de Cisco:

```
no interface mlag-port-channel xxx-xxx lacp suspend-individual enable force
```

5. Repita estos pasos para cada switch de la configuración.

Obtenga más información

- ["El nodo de almacenamiento se desactiva durante la solución de problemas"](#)

Cree una función HCC de NetApp en vCenter

Es posible crear un rol HCC de NetApp en vCenter para añadir manualmente activos de vCenter (controladoras) o nodos de computación (nodos) al nodo de gestión tras la instalación, o para modificar las controladoras o los nodos existentes.

Este rol HCC de NetApp limita su vista de servicios de nodos de gestión a activos de solo NetApp.

Acerca de esta tarea

- En este procedimiento, se describen los pasos disponibles en la versión 6.7 de vSphere. La interfaz de usuario de vSphere puede diferir levemente de lo que se describe según la versión de vSphere instalada. Para obtener más ayuda, consulte la documentación de VMware vCenter.
- Para ["Cree una nueva función HCC de NetApp"](#), Primero debe configurar una cuenta de usuario nueva en vCenter, crear una función HCC de NetApp y, a continuación, asignar los permisos de usuario.
- En el caso de configuraciones de hosts ESXi de NetApp, debe actualizar la cuenta de usuario creada por NDE al nuevo rol HCC de NetApp:
 - Uso ["esta opción"](#) Si el host ESXi de NetApp no existe dentro de un clúster de hosts de vCenter
 - Uso ["esta opción"](#) Si el host ESXi de NetApp existe dentro de un clúster de hosts de vCenter
- Puede hacerlo ["configure un activo de controladora"](#) que ya existe en el nodo de gestión.
- Use el nuevo rol HCC de NetApp a ["añadir un activo o un nodo de computación"](#) al nodo de gestión.

Cree una nueva función HCC de NetApp

Configure una nueva cuenta de usuario en vCenter, cree un rol NetApp HCC y, a continuación, asigne los permisos de usuario.

Configure una cuenta de usuario nueva en vCenter

Realice los pasos siguientes para configurar una cuenta de usuario nueva en vCenter.

Pasos

1. Inicie sesión en vSphere Web Client como `administrator@vsphere.local` o equivalente.
2. En el menú, seleccione **Administración**.
3. En la sección **Inicio de sesión único**, seleccione **usuarios y grupos**.
4. En la lista **dominio**, seleccione `vsphere.local` O el dominio LDAP.
5. Seleccione **Agregar usuario**.
6. Complete el formulario **Agregar usuario**.

Cree un nuevo rol HCC de NetApp en vCenter

Realice los siguientes pasos para crear una nueva función HCC de NetApp en vCenter.

Pasos

1. Seleccione **Editar rol** y asigne los permisos necesarios.
2. En el panel de navegación izquierdo, seleccione **Global**.
3. Seleccione **Diagnóstico y licencias**.
4. En el panel de navegación izquierdo, seleccione **hosts**.
5. Seleccione **Mantenimiento, Alimentación, Configuración de particiones de almacenamiento y firmware**.
6. Guardar como NetApp Role.

Asigne permisos de usuario a vCenter

Ejecute los siguientes pasos para asignar los permisos de usuario al nuevo rol HCC de NetApp en vCenter.

Pasos

1. En el menú, seleccione **hosts y Clusters**.
2. En el panel de navegación de la izquierda, seleccione una de las siguientes opciones:
 - El nivel superior de vCenter.
 - Su instancia de vCenter deseada si se encuentra en modo vinculado.



- A partir del plugin de NetApp Element para vCenter Server 5.0, se debe utilizar "**VCenter Linked Mode**", Se registra el plugin de Element desde un nodo de gestión independiente para cada instancia de vCenter Server que administra los clústeres de almacenamiento de SolidFire de NetApp (recomendado).
- Usar el plugin de NetApp Element para vCenter Server 4.10 y versiones anteriores para gestionar recursos de clúster desde otras instancias de vCenter Server mediante "**VCenter Linked Mode**" solo se limita a clústeres de almacenamiento local.

3. En el panel de navegación de la derecha, seleccione **permisos**.
4. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP

- b. Utilice la búsqueda para buscar el nuevo usuario en el que ha creado [Configure una cuenta de usuario nueva en vCenter](#).
- c. Seleccione `NetApp Role`.



Seleccione **NO** seleccione **propagar a niños**.

Add Permission | satyabra-vcen... X

User: vsphere.local

Q netapp

Role: NetApp Role

Propagate to children

CANCEL OK

Asigne permisos de usuario al centro de datos

Realice los siguientes pasos para asignar los permisos de usuario al centro de datos en vCenter.

Pasos

1. En el panel izquierdo, seleccione **Datacenter**.
2. En el panel de navegación de la derecha, seleccione **permisos**.
3. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP.
- b. Utilice la búsqueda para encontrar el nuevo usuario HCC que ha creado en [Configure una cuenta de usuario nueva en vCenter](#).
- c. Seleccione `ReadOnly role`.



Seleccione **NO** seleccione **propagar a niños**.

Asigne permisos de usuario a almacenes de datos NetApp HCI

Realice los siguientes pasos para asignar los permisos de usuario a los almacenes de datos de NetApp HCI en vCenter.

Pasos

1. En el panel izquierdo, seleccione **Datacenter**.
2. Cree una nueva carpeta de almacenamiento. Haga clic con el botón derecho del ratón en **Datacenter** y seleccione **Crear carpeta de almacenamiento**.
3. Transfiera todos los almacenes de datos de NetApp HCI del clúster de almacenamiento y local al nodo de computación a la nueva carpeta de almacenamiento.
4. Seleccione la nueva carpeta de almacenamiento.
5. En el panel de navegación de la derecha, seleccione **permisos**.
6. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP.
- b. Utilice la búsqueda para encontrar el nuevo usuario HCC que ha creado en [Configure una cuenta de usuario nueva en vCenter](#).
- c. Seleccione `Administrator role`.
- d. Seleccione **propagar a niños**.

Asignar permisos de usuario a un clúster de hosts de NetApp

Realice los siguientes pasos para asignar los permisos de usuario a un clúster de hosts de NetApp en vCenter.

Pasos

1. En el panel de navegación de la izquierda, seleccione el clúster de hosts de NetApp.
2. En el panel de navegación de la derecha, seleccione **permisos**.
3. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP.
- b. Utilice la búsqueda para encontrar el nuevo usuario HCC que ha creado en [Configure una cuenta de usuario nueva en vCenter](#).
- c. Seleccione `NetApp Role` o `Administrator`.
- d. Seleccione **propagar a niños**.

Configuraciones de host ESXi de NetApp

En el caso de configuraciones de hosts ESXi de NetApp, debe actualizar la cuenta de usuario creada por NDE al nuevo rol HCC de NetApp.

El host NetApp ESXi no existe en un clúster de hosts de vCenter

Si el host ESXi de NetApp no existe dentro de un clúster de hosts de vCenter, es posible usar el siguiente procedimiento para asignar el rol HCC de NetApp y los permisos de usuario en vCenter.

Pasos

1. En el menú, seleccione **hosts y Clusters**.
2. En el panel de navegación de la izquierda, seleccione el host ESXi de NetApp.
3. En el panel de navegación de la derecha, seleccione **permisos**.
4. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP.
 - b. Utilice la búsqueda para buscar el nuevo usuario en el que ha creado [Configure una cuenta de usuario nueva en vCenter](#).
 - c. Seleccione `NetApp Role` O `Administrator`.
5. Seleccione **propagar a niños**.

El host ESXi de NetApp existe en un clúster de hosts de vCenter

Si existe un host ESXi de NetApp dentro de un clúster de hosts de vCenter con hosts ESXi de otros proveedores, puede usar el siguiente procedimiento para asignar la función HCC de NetApp y los permisos de usuario en vCenter.

1. En el menú, seleccione **hosts y Clusters**.
2. En el panel de navegación de la izquierda, expanda el clúster de hosts que desee.
3. En el panel de navegación de la derecha, seleccione **permisos**.
4. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP.
- b. Utilice la búsqueda para buscar el nuevo usuario en el que ha creado [Configure una cuenta de usuario nueva en vCenter](#).
- c. Seleccione `NetApp Role`.



Seleccione **NO** seleccione **propagar a niños**.

5. En el panel de navegación de la izquierda, seleccione un host ESXi de NetApp.
6. En el panel de navegación de la derecha, seleccione **permisos**.
7. Seleccione el icono **+** para añadir el nuevo usuario.

Agregue los siguientes detalles en la ventana **Agregar permiso**:

- a. Seleccione `vsphere.local` O el dominio LDAP.
- b. Utilice la búsqueda para buscar el nuevo usuario en el que ha creado [Configure una cuenta de usuario nueva en vCenter](#).

[nueva en vCenter.](#)

c. Seleccione `NetApp Role o. Administrator.`

d. Seleccione **propagar a niños.**

8. Repita esto para los hosts ESXi de NetApp restantes en el clúster de hosts.

El activo de la controladora ya existe en el nodo de gestión

Si ya existe un activo de la controladora en el nodo de gestión, realice los siguientes pasos para configurar la controladora mediante `PUT /assets /{asset_id} /controllers /{controller_id}.`

Pasos

1. Acceda a la interfaz de usuario de API de servicio mnode en el nodo de gestión:

<https://<ManagementNodeIP>/mnode>

2. Seleccione **autorizar** e introduzca las credenciales para acceder a las llamadas API.

3. Seleccione `GET /assets` Para obtener el ID de padre.

4. Seleccione `PUT /assets /{asset_id} /controllers /{controller_id}.`

a. Introduzca las credenciales creadas en la configuración de la cuenta en el cuerpo de la solicitud.

Añada un activo o un nodo de computación al nodo de gestión

Si necesita agregar manualmente un nuevo activo o un nodo de computación (y activos de BMC) después de la instalación, utilice la nueva cuenta de usuario de HCC creada en [Configure una cuenta de usuario nueva en vCenter.](#) Para obtener más información, consulte ["Añada activos de computación y de controladora al nodo de gestión"](#).

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Mantenga actualizado VMware vSphere

Después de implementar NetApp HCI, debe utilizar VMware vSphere Lifecycle Manager a fin de aplicar las versiones de seguridad más recientes para la versión de VMware vSphere utilizada con NetApp HCI.

Utilice la ["Herramienta de matriz de interoperabilidad"](#) para garantizar que todas las versiones de software sean compatibles. Consulte ["Documentación de VMware vSphere Lifecycle Manager"](#) si quiere más información.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Instale los controladores de GPU para los nodos de computación habilitados para GPU

Los nodos de computación con unidades de procesamiento de gráficos (GPU) de NVIDIA, al igual que H610C, necesitan controladores de software de NVIDIA instalados en VMware ESXi para poder aprovechar la potencia de procesamiento aumentada. Después de poner en marcha los nodos de computación con GPU, debe realizar estos pasos en cada nodo de computación habilitado para GPU a fin de instalar los controladores de GPU en ESXi.

Pasos

1. Abra un explorador y vaya al portal de licencias de NVIDIA en la siguiente URL:

```
https://nvid.nvidia.com/dashboard/
```

2. Descargue uno de los siguientes paquetes de controladores en su equipo, dependiendo de su entorno:

La versión de vSphere	Paquete de controladores
VSphere 6.5	NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip
VSphere 6.7	NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip

3. Extraiga el paquete de controladores del ordenador.

El archivo .VIB resultante es el archivo de controlador sin comprimir.

4. Copie el .VIB Archivo de controlador del equipo a ESXi que se ejecuta en el nodo de computación. Los siguientes comandos de ejemplo para cada versión asumen que el controlador se encuentra en el `$HOME/NVIDIA/ESX6.x/` directorio en el host de gestión. La utilidad SCP está disponible en la mayoría de distribuciones de Linux, o está disponible como una utilidad descargable para todas las versiones de Windows:

Versión de ESXi	Descripción
ESXi 6.5	<pre>scp \$HOME/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.</pre>
ESXi 6.7	<pre>scp \$HOME/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.</pre>

5. Siga los pasos siguientes para iniciar sesión como root en el host ESXi e instalar NVIDIA vGPU Manager en ESXi.
 - a. Ejecute el siguiente comando para iniciar sesión en el host ESXi como usuario raíz:

```
ssh root@<ESXi_IP_ADDRESS>
```

- b. Ejecute el siguiente comando para verificar que no hay controladores de GPU NVIDIA instalados actualmente:

```
nvidia-smi
```

Este comando debería devolver el mensaje `nvidia-smi: not found`.

- c. Ejecute los siguientes comandos para activar el modo de mantenimiento en el host e instale NVIDIA vGPU Manager desde el archivo VIB:

```
esxcli system maintenanceMode set --enable true  
esxcli software vib install -v /NVIDIA*.vib
```

Debería ver el mensaje `Operation finished successfully`.

- d. Ejecute el siguiente comando y compruebe que los ocho controladores de GPU aparecen en la lista del resultado del comando:

```
nvidia-smi
```

- e. Ejecute el siguiente comando para comprobar que el paquete NVIDIA vGPU se ha instalado y cargado correctamente:

```
vmkload_mod -l | grep nvidia
```

El comando debería mostrar un resultado similar al siguiente: `nvidia 816 13808`

- f. Ejecute el siguiente comando para reiniciar el host:

```
reboot -f
```

- g. Ejecute el siguiente comando para salir del modo de mantenimiento:

```
esxcli system maintenanceMode set --enable false
```

6. Repita los pasos 4-6 para cualquier otro nodo de computación recién implementado con GPU de NVIDIA.

7. Realice las siguientes tareas siguiendo las instrucciones del sitio de documentación de NVIDIA:

- Instale el servidor de licencias de NVIDIA.
- Configurar los invitados de máquinas virtuales para el software NVIDIA vGPU.
- Si utiliza puestos de trabajo habilitados para vGPU en un contexto de infraestructura de puestos de trabajo virtuales (VDI), configure VMware Horizon View para el software vGPU de NVIDIA.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Acceda a Control del cloud híbrido de NetApp

El control del cloud híbrido de NetApp le permite gestionar NetApp HCI. Puede actualizar los servicios de gestión y otros componentes de NetApp HCI, así como ampliar y supervisar la instalación. Para iniciar sesión en NetApp Hybrid Cloud Control, vaya a la dirección IP del nodo de gestión.

Lo que necesitará

- **Permisos de administrador de clúster:** Tiene permisos como administrador en el clúster de almacenamiento.
- **Servicios de administración:** Ha actualizado sus servicios de administración a al menos la versión 2.1.326. El control del cloud híbrido de NetApp no está disponible en versiones anteriores del paquete de servicio. Para obtener información acerca de la versión actual del paquete de servicio, consulte ["Notas de la versión de los servicios de gestión"](#).

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.

Aparece la interfaz de control del cloud híbrido de NetApp.



Si ha iniciado sesión con permisos insuficientes, verá un mensaje "no se puede cargar" en todas las páginas de recursos de HCC y los recursos no estarán disponibles.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Reduzca el desgaste de los medios de arranque en un nodo de computación NetApp HCI

Cuando utiliza medios de arranque flash o NVDIMM con un nodo de computación NetApp HCI, mantener los registros del sistema en ese medio provoca escrituras frecuentes en ese medio. Esto puede degradar al final la memoria flash. Utilice las instrucciones del siguiente artículo de la base de conocimientos para mover el registro de host y el archivo de volcado principal a una ubicación de almacenamiento compartido, lo que puede ayudar a evitar la degradación del medio de arranque a lo largo del tiempo y

ayudar a evitar errores de disco de arranque completo.

["Cómo reducir el deterioro de la unidad de arranque de un nodo de computación NetApp HCI"](#)

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Gestione NetApp HCI

Información general de la gestión de NetApp HCI

Es posible configurar el nombre de dominio completo y gestionar credenciales para NetApp HCI, cuentas de usuario, clústeres de almacenamiento, volúmenes, grupos de acceso de volúmenes, Los iniciadores, las políticas de calidad de servicio de los volúmenes y el nodo de gestión.

Estos son los elementos con los que puede trabajar:

- ["Configure el acceso completo a la interfaz de usuario web de Nombre de dominio"](#)
- ["Cambiar las credenciales en NetApp HCI"](#)
- ["Actualice las credenciales de vCenter y ESXi"](#)
- ["Gestione activos de almacenamiento de NetApp HCI"](#)
- ["Trabaje con el nodo de gestión"](#)
- ["Apaga o enciende el sistema NetApp HCI"](#)

Obtenga más información

- ["Recursos de NetApp HCI"](#)

Configure el acceso completo a la interfaz de usuario web de Nombre de dominio

NetApp HCI con el software Element 12.2 o una versión posterior le permite acceder a las interfaces web del clúster de almacenamiento mediante el nombre de dominio completo (FQDN). Si desea usar el FQDN para acceder a interfaces de usuario web como la interfaz de usuario web de Element, la interfaz de usuario por nodo o la interfaz de usuario de nodo de gestión, primero debe añadir un ajuste de clúster de almacenamiento para identificar el FQDN que utiliza el clúster.

Ahora se puede acceder a las interfaces web del clúster de almacenamiento mediante el nombre de dominio completo (FQDN). Si desea usar el FQDN para acceder a interfaces de usuario web como la interfaz de usuario web de Element, la interfaz de usuario por nodo o la interfaz de usuario de nodo de gestión, primero debe añadir un ajuste de clúster de almacenamiento para identificar el FQDN que utiliza el clúster. Esto permite al clúster redirigir correctamente una sesión de inicio de sesión y mejora la integración con servicios externos como gestores de claves y proveedores de identidades para la autenticación de múltiples factores.

Lo que necesitará

- Esta función requiere Element 12.2 o posterior.
- Para configurar esta función con las API REST de NetApp Hybrid Cloud Control, se requieren servicios de gestión 2.15 o posteriores.
- Para configurar esta función con la interfaz de usuario de control del cloud híbrido de NetApp se requieren servicios de gestión 2.19 o posteriores.

- Para utilizar las API DE REST, debe haber puesto en marcha un nodo de gestión que ejecuta la versión 11.5 o una versión posterior.
- Necesita nombres de dominio completos para el nodo de gestión y cada clúster de almacenamiento que se resuelven correctamente con la dirección IP del nodo de gestión y cada dirección IP de clúster de almacenamiento de.

Puede configurar o quitar el acceso de interfaz de usuario web FQDN de NetApp Hybrid Cloud Control y la API DE REST. También puede solucionar problemas de RFQ configuradas incorrectamente.

- [Configure el acceso de interfaz de usuario web de FQDN mediante NetApp Hybrid Cloud Control](#)
- [Configure el acceso de interfaz de usuario web del FQDN mediante la API DE REST](#)
- [Elimine el acceso de interfaz de usuario web de FQDN mediante el control de cloud híbrido de NetApp](#)
- [Quite el acceso de interfaz de usuario web del FQDN mediante la API DE REST](#)
- [Resolución de problemas](#)

Configure el acceso de interfaz de usuario web de FQDN mediante NetApp Hybrid Cloud Control

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione el icono de menú en la parte superior derecha de la página.
4. Seleccione **Configurar**.
5. En el panel **nombres de dominio completos**, seleccione **Configurar**.
6. En la ventana que aparece, introduzca las FQDN para el nodo de administración y cada clúster de almacenamiento.
7. Seleccione **Guardar**.

El panel **nombres de dominio completos** enumera cada clúster de almacenamiento con su MVIP y FQDN asociados.



En el panel **nombres de dominio completos** sólo aparecen los clústeres de almacenamiento conectados con el conjunto FQDN.

Configure el acceso de interfaz de usuario web del FQDN mediante la API DE REST

Pasos

1. Asegúrese de que los nodos de almacenamiento de Element y el nodo de gestión tengan DNS configurado correctamente para el entorno de red para que se puedan resolver las FQDN del entorno. Para establecer DNS, vaya a la interfaz de usuario por nodo para nodos de almacenamiento y al nodo de gestión y seleccione **Configuración de red > Red de administración**.

a. IU por nodo para nodos de almacenamiento: https://<storage_node_management_IP>:442

b. IU por nodo para el nodo de gestión: https://<management_node_IP>:442

2. Cambie la configuración del clúster de almacenamiento mediante la API de Element.

a. Acceda a la API de Element y cree la siguiente preferencia de interfaz del clúster mediante el `CreateClusterInterfacePreference` Método API e inserte el FQDN de MVIP del clúster para el valor de preferencia:

- Nombre: `mvip_fqdn`
- Valor: `<Fully Qualified Domain Name for the Cluster MVIP>`

Por ejemplo, aquí el nombre de dominio completo es `storagecluster.my.org`:

```
https://<Cluster_MVIP>/json-rpc/12.2?method=CreateClusterInterfacePreference&name=mvip_fqdn&value=storagecluster.my.org
```

3. Cambie la configuración del nodo de gestión con la API DE REST en el nodo de gestión:

a. Acceda a la interfaz de usuario de API DE REST para el nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/2/`. Por ejemplo:

```
https://<management_node_IP>/mnode/2/
```

b. Seleccione **autorizar** o cualquier icono de bloqueo e introduzca el nombre de usuario y la contraseña del clúster de elementos.

c. Introduzca el ID de cliente as `mnode-client`.

d. Seleccione **autorizar** para iniciar una sesión.

e. Cierre la ventana.

f. Seleccione **GET /settings**.

g. Seleccione **probar**.

h. Seleccione **Ejecutar**.

i. Tenga en cuenta si el proxy se utiliza o no como se indica en la `"use_proxy"` por `true` o `false`.

j. Seleccione **COLOCAR /settings**.

k. Seleccione **probar**.

l. En el área cuerpo de la solicitud, introduzca el nombre de dominio completo del nodo de gestión como valor para `mnode_fqdn` parámetro. Especifique también si se debe utilizar el proxy (`true` o `false` desde el paso anterior) para la `use_proxy` parámetro.


```
{
  "mnode_fqdn": "mnode.my.org",
  "use_proxy": false
}
```

m. Seleccione **Ejecutar**.

Elimine el acceso de interfaz de usuario web de FQDN mediante el control de cloud híbrido de NetApp

Puede usar este procedimiento para quitar el acceso web FQDN para el nodo de gestión y los clústeres de almacenamiento.

Pasos

1. En el panel **nombres de dominio completos**, seleccione **Editar**.
2. En la ventana resultante, elimine el contenido en el campo de texto **FQDN**.
3. Seleccione **Guardar**.

La ventana se cierra y el FQDN ya no aparece en el panel **nombres de dominio completos**.

Quite el acceso de interfaz de usuario web del FQDN mediante la API DE REST

Pasos

1. Cambie la configuración del clúster de almacenamiento mediante la API de Element.
 - a. Acceda a la API de Element y elimine la siguiente preferencia de interfaz de clúster mediante el `DeleteClusterInterfacePreference` Método API:
 - Nombre: `mvip_fqdn`

Por ejemplo:

```
https://<Cluster_MVIP>/json-rpc/12.2?method=DeleteClusterInterfacePreference&name=mvip_fqdn
```

2. Cambie la configuración del nodo de gestión con la API DE REST en el nodo de gestión:
 - a. Acceda a la interfaz de usuario de API DE REST para el nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/2/`. Por ejemplo:

```
https://<management_node_IP>/mnode/2/
```

- b. Seleccione **autorizar** o cualquier icono de bloqueo e introduzca el nombre de usuario y la contraseña del clúster de elementos.
- c. Introduzca el ID de cliente as `mnode-client`.

- d. Seleccione **autorizar** para iniciar una sesión.
- e. Cierre la ventana.
- f. Seleccione **COLOCAR /settings**.
- g. Seleccione **probar**.
- h. En el área cuerpo de la solicitud, no introduzca un valor para `mnode_fqdn` parámetro. Especifique también si se debe utilizar el proxy (`true` o `false`) para `use_proxy` parámetro.

```
{
  "mnode_fqdn": "",
  "use_proxy": false
}
```

- i. Seleccione **Ejecutar**.

Resolución de problemas

Si las FQDN están configuradas incorrectamente, es posible que tenga problemas para acceder al nodo de administración, a un clúster de almacenamiento o a ambos. Utilice la siguiente información como ayuda para solucionar el problema.

Problema	Causa	Resolución
<ul style="list-style-type: none"> • Se obtiene un error del explorador al intentar acceder al nodo de gestión o al clúster de almacenamiento mediante el FQDN. • No puede iniciar sesión en el nodo de gestión ni en el clúster de almacenamiento mediante una dirección IP. 	El nombre de dominio completo del nodo de gestión y el nombre de dominio completo del clúster de almacenamiento están configurados incorrectamente.	Use las instrucciones de API DE REST que aparecen en esta página para quitar las opciones de FQDN del nodo de gestión y del clúster de almacenamiento y volver a configurarlos.
<ul style="list-style-type: none"> • Se obtiene un error del explorador al intentar acceder al FQDN del clúster de almacenamiento. • No puede iniciar sesión en el nodo de gestión ni en el clúster de almacenamiento mediante una dirección IP. 	El nombre de dominio completo del nodo de gestión está configurado correctamente, pero el nombre de dominio completo del clúster de almacenamiento está configurado incorrectamente.	Use las instrucciones de API DE REST que aparecen en esta página para quitar la configuración de FQDN del clúster de almacenamiento y volver a configurarlos.

Problema	Causa	Resolución
<ul style="list-style-type: none"> • Obtiene un error del explorador al intentar acceder al FQDN del nodo de gestión. • Puede iniciar sesión en el nodo de gestión y el clúster de almacenamiento con una dirección IP. 	El nombre de dominio completo del nodo de gestión está configurado incorrectamente, pero el nombre de dominio completo del clúster de almacenamiento está configurado correctamente.	Inicie sesión en NetApp Hybrid Cloud Control para corregir los ajustes FQDN del nodo de gestión en la interfaz de usuario o utilice las instrucciones API DE REST en esta página para corregir los ajustes.

Obtenga más información

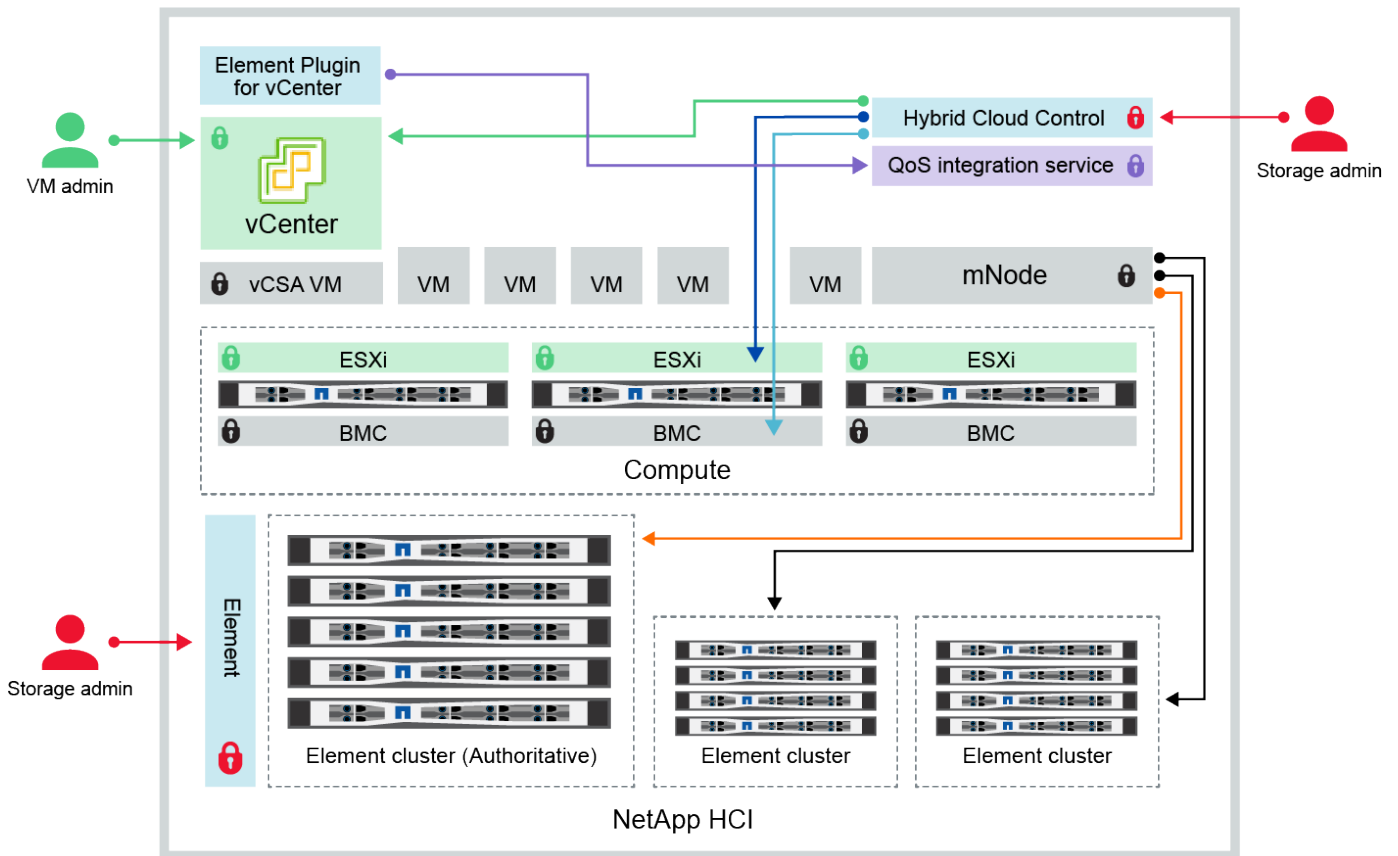
- ["CreateClusterInterfacePreference información de la API en la documentación de SolidFire y Element"](#)
- ["Recursos de NetApp HCI"](#)
- ["Documentación de SolidFire y el software Element"](#)

Cambie las credenciales en NetApp HCI y SolidFire de NetApp



Según las políticas de seguridad de la organización que implementó NetApp HCI o SolidFire de NetApp, los cambios de credenciales o contraseñas suelen formar parte de las prácticas de seguridad. Antes de cambiar las contraseñas, debe tener en cuenta el impacto sobre otros componentes de software en la implementación.



Si cambia las credenciales de un componente de una implementación de NetApp HCI o SolidFire de NetApp, la siguiente tabla proporciona directrices sobre el impacto en otros componentes.




Interacciones de componentes de NetApp
HCI:



- Hybrid Cloud Control and administrator use VMware vSphere Single Sign-on credentials to log into vCenter
- Hybrid Cloud Control uses per-node 'root' account to communicate with VMware ESXi
- Hybrid Cloud Control uses per-node BMC credentials to communicate with BMC on compute nodes
- Element Plugin for VMware vCenter uses password to communicate with QoS service on mNode
- Administrator uses administrative Element storage credentials to log into Element UI and Hybrid Cloud Control
- mNode and services use Element certificates to communicate with authoritative storage cluster
- mNode and services use Element administrative credentials for additional storage clusters

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
<p>Credenciales de Element</p> 	<p>Se aplica a: NetApp HCI y SolidFire</p> <p>Los administradores utilizan estas credenciales para iniciar sesión en:</p> <ul style="list-style-type: none"> • La interfaz de usuario de Element en el clúster de almacenamiento de Element • Control del cloud híbrido en el nodo de gestión (mnode) <p>Cuando Hybrid Cloud Control gestiona varios clústeres de almacenamiento, solo acepta las credenciales de administrador de los clústeres de almacenamiento, conocidas como el <i>autoritativo cluster</i> para el que se configuró mnode inicialmente. Para los clústeres de almacenamiento que se añadieron más adelante al control del cloud híbrido, el nodo mnode almacena de forma segura las credenciales de administración. Si se modifican las credenciales para clústeres de almacenamiento añadidos posteriormente, también se deben actualizar las credenciales en mnode con la API mnode.</p>	<ul style="list-style-type: none"> • "Actualice las contraseñas de administrador del clúster de almacenamiento". • Actualice las credenciales de administrador del clúster de almacenamiento en el nodo m mediante el "API modifyclusteradmin".
<p>Credenciales de inicio de sesión único de vSphere</p> 	<p>Se aplica a: Sólo NetApp HCI</p> <p>Los administradores utilizan estas credenciales para iniciar sesión en VMware vSphere Client. Cuando vCenter forma parte de la instalación de NetApp HCI, las credenciales se configuran en el motor de implementación de NetApp como lo siguiente:</p> <ul style="list-style-type: none"> • <code>nombreusuario@vsphere.locloc </code> con la contraseña especificada, y. • <code>administrator@vsphere.locloc </code> con la contraseña especificada. Cuando se usa una instancia existente de vCenter para poner en marcha NetApp HCI, los administradores DE TI de VMware gestionan las credenciales de inicio de sesión único de vSphere. 	<p>"Actualice las credenciales de vCenter y ESXi".</p>

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
<p data-bbox="126 262 251 567">Credenciales del controlador de administración de la placa base (BMC)</p> 	<p data-bbox="261 262 641 294">Se aplica a: Sólo NetApp HCI</p> <p data-bbox="261 325 1047 493">Los administradores utilizan estas credenciales para iniciar sesión en el BMC de los nodos de computación de NetApp en una implementación de NetApp HCI. El BMC proporciona funcionalidades básicas de supervisión de hardware y consola virtual.</p> <p data-bbox="261 525 1063 766">Las credenciales de BMC (denominadas en ocasiones <i>IPMI</i>) para cada nodo de computación de NetApp se almacenan de forma segura en el nodo men las puestas en marcha de NetApp HCI. Control de cloud híbrido de NetApp usa las credenciales de BMC en una capacidad de cuenta de servicio para comunicarse con el BMC en los nodos de computación durante las actualizaciones del firmware de los nodos de computación.</p> <p data-bbox="261 798 1055 934">Cuando se cambian las credenciales del BMC, también se deben actualizar las credenciales de los nodos de computación respectivos en el mnode para conservar todas las funciones de Hybrid Cloud Control.</p>	<ul data-bbox="1112 262 1485 745" style="list-style-type: none"> • "Configure IPMI para cada nodo en NetApp HCI". • Para los nodos H410C, H610C y H615C, "Cambie la contraseña de IPMI predeterminada". • Para nodos H410S y H610S, "Cambiar la contraseña predeterminada de IPM". • "Cambie las credenciales de BMC en el nodo de gestión".
<p data-bbox="126 987 251 1081">Credenciales de ESXi</p> 	<p data-bbox="261 987 641 1018">Se aplica a: Sólo NetApp HCI</p> <p data-bbox="261 1050 1055 1249">Los administradores pueden iniciar sesión en hosts ESXi mediante SSH o la DCUI local con una cuenta raíz local. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp.</p> <p data-bbox="261 1281 1071 1522">Las credenciales raíz de ESXi para cada nodo de computación de NetApp se almacenan de forma segura en mnode en puestas en marcha de NetApp HCI. Hybrid Cloud Control de NetApp utiliza las credenciales en una capacidad de cuenta de servicio para comunicarse con hosts ESXi directamente durante las actualizaciones del firmware de los nodos de computación y las comprobaciones del estado.</p> <p data-bbox="261 1554 1039 1690">Cuando un administrador de VMware cambia las credenciales raíz de ESXi, las credenciales de los nodos de computación respectivos deben actualizarse en el mnode para mantener la funcionalidad de control de cloud híbrido.</p>	<p data-bbox="1084 987 1469 1050">"Actualice las credenciales de para hosts ESXi y vCenter".</p>

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
<p data-bbox="126 262 261 499">Contraseña de integración de la calidad de servicio</p> 	<p data-bbox="261 262 1084 304">Se aplica a: NetApp HCI y opcional en SolidFire</p> <p data-bbox="261 325 1084 388">No se utiliza para inicios de sesión interactivos por parte de administradores.</p> <p data-bbox="261 430 1084 493">La integración de calidad de servicio entre VMware vSphere y el software Element se habilita mediante:</p> <ul data-bbox="292 525 1084 609" style="list-style-type: none"> • Plugin de Element para vCenter Server y. • Servicio QoS en el mnode. <p data-bbox="261 640 1084 808">Para la autenticación, el servicio QoS utiliza una contraseña que se utiliza exclusivamente en este contexto. La contraseña de calidad de servicio se especifica durante la instalación inicial del plugin de Element para vCenter Server, o bien se genera automáticamente durante la implementación de NetApp HCI.</p> <p data-bbox="261 840 1084 882">Ningún impacto sobre otros componentes.</p>	<p data-bbox="1084 262 1492 388">"Actualice las credenciales de QoSSIOC en el plugin de NetApp Element para vCenter Server".</p> <p data-bbox="1084 430 1492 598">La contraseña de SIOC del plugin de NetApp Element para vCenter Server también se conoce como <i>QoSSIOC Password</i>.</p> <p data-bbox="1084 630 1492 724">Revise el {URL-pico}[plugin de Element para vCenter Server KB].</p>
<p data-bbox="126 934 261 1123">Credenciales de vCenter Service Appliance</p> 	<p data-bbox="261 934 1084 997">Se aplica a: NetApp HCI solo si configura el motor de puesta en marcha de NetApp</p> <p data-bbox="261 1029 1084 1302">Los administradores pueden iniciar sesión en las máquinas virtuales del dispositivo de vCenter Server. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Según la versión de VMware vSphere implementada, algunos administradores del dominio de inicio de sesión único de vSphere también pueden iniciar sesión en el dispositivo.</p> <p data-bbox="261 1333 1084 1375">Ningún impacto sobre otros componentes.</p>	<p data-bbox="1084 934 1492 997">No es necesario realizar cambios.</p>
<p data-bbox="126 1417 261 1690">Credenciales de administrador del nodo de gestión de NetApp</p> 	<p data-bbox="261 1417 1084 1459">Se aplica a: NetApp HCI y opcional en SolidFire</p> <p data-bbox="261 1480 1084 1648">Los administradores pueden iniciar sesión en las máquinas virtuales del nodo de gestión de NetApp para obtener una configuración avanzada y solucionar problemas. Según la versión del nodo de gestión puesta en marcha, el inicio de sesión a través de SSH no se habilita de forma predeterminada.</p> <p data-bbox="261 1680 1084 1785">En implementaciones de NetApp HCI, el usuario y la contraseña fueron especificados durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp.</p> <p data-bbox="261 1816 1084 1858">Ningún impacto sobre otros componentes.</p>	<p data-bbox="1084 1417 1492 1480">No es necesario realizar cambios.</p>

Obtenga más información

- ["Cambie el certificado SSL predeterminado del software Element"](#)
- ["Cambie la contraseña de IPMI para los nodos"](#)
- ["Habilite la autenticación multifactor"](#)
- ["Comience con la gestión de claves externas"](#)
- ["Cree un clúster que admita unidades FIPS"](#)

Actualice las credenciales de vCenter y ESXi

Para mantener toda la funcionalidad del control del cloud híbrido de NetApp en su instalación de NetApp HCI, cuando cambia las credenciales en hosts vCenter y ESXi, también debe actualizar esas credenciales en el servicio de activos en el nodo de gestión.

Acerca de esta tarea

El control de cloud híbrido de NetApp se comunica con vCenter y con los nodos de computación individuales que ejecutan VMware vSphere ESXi para recuperar información para la consola y facilitar actualizaciones graduales del firmware, el software y los controladores. Control de cloud híbrido de NetApp y sus servicios relacionados en el nodo de gestión utilizan credenciales (nombre de usuario/contraseña) para realizar la autenticación en VMware vCenter y ESXi.

Si la comunicación entre estos componentes falla, NetApp Hybrid Cloud Control y vCenter muestran mensajes de error cuando se producen problemas de autenticación. El control de cloud híbrido de NetApp muestra un banner de error rojo si no puede comunicarse con la instancia de VMware vCenter asociada en la instalación de NetApp HCI. VMware vCenter mostrará mensajes de bloqueo de cuenta ESXi para hosts ESXi individuales como resultado del control de cloud híbrido de NetApp con credenciales obsoletas.

El nodo de gestión en NetApp HCI hace referencia a estos componentes con los nombres siguientes:

- "Activos de controladora" son instancias de vCenter asociadas con la instalación de NetApp HCI.
- "Activos de nodos de computación" son los hosts ESXi en la instalación de NetApp HCI.

Durante la instalación inicial de NetApp HCI con el motor de puesta en marcha de NetApp, el nodo de gestión almacenaba las credenciales del usuario administrativo que especificó para vCenter y la contraseña de la cuenta "raíz" en los servidores ESXi.

Actualice la contraseña de vCenter mediante la API DE REST de nodo de gestión

Siga los pasos para actualizar los activos de la controladora. Consulte ["Ver o editar activos de controladora existentes"](#).

Actualice la contraseña de ESXi mediante la API DE REST del nodo de gestión

Pasos

1. Para obtener información general de la interfaz de usuario de la API DE REST del nodo de gestión, consulte ["Información general de la interfaz de usuario de la API DE REST del nodo de gestión"](#).
2. Acceda a la interfaz de usuario de API DE REST para realizar servicios de gestión en el nodo de gestión:


```
https://<ManagementNodeIP>/mnode
```

Sustituya <management node IP> por la dirección IPv4 del nodo de gestión en la red de gestión que utiliza NetApp HCI.

3. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña de administración del clúster de SolidFire de NetApp.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
4. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /assets/Compute_Nodes**.

De esta forma, se recuperan los registros de activos de nodos de computación almacenados en el nodo de gestión.

Este es el enlace directo a esta API en la interfaz de usuario:

```
https://<ManagementNodeIP>/mnode/#/assets/routes.v1.assets_api.get_compute_nodes
```

5. Haga clic en **probar**.
6. Haga clic en **Ejecutar**.
7. En el cuerpo de respuesta, identifique los registros de activos del nodo de computación que necesitan credenciales actualizadas. Puede utilizar las propiedades "ip" y "host_name" para encontrar los registros de host ESXi correctos.

```
"config": { },
"credentialid": <credential_id>,
"hardware_tag": <tag>,
"host_name": <host_name>,
"id": <id>,
"ip": <ip>,
"parent": <parent>,
"type": ESXi Host
```



El paso siguiente utiliza los campos "padre" e "id" del registro de activos de cálculo para hacer referencia al registro que se va a actualizar.

8. Configure el activo específico del nodo de computación:
 - a. Haga clic en **PUT /assets/{Asset_id}/compute-Nodes/{Compute_id}**.

Este es el enlace directo a la API en la interfaz de usuario:

```
https://<ManagementNodeIP>/mnode/#/assets/routes.v1.assets_api.put_assets_compute_id
```

- a. Haga clic en **probar**.
- b. Introduzca "asset_id" con la información "parent".
- c. Introduzca "Compute_id" con la información "id".
- d. Modifique el cuerpo de la solicitud en la interfaz de usuario para actualizar sólo los parámetros de contraseña y nombre de usuario en el registro de activos de computación:

```
{  
  "password": "<password>",  
  "username": "<username>"  
}
```

- e. Haga clic en **Ejecutar**.
 - f. Validar que la respuesta es HTTP 200, que indica que las nuevas credenciales se han almacenado en el registro de activos de cálculo de referencia
9. Repita los dos pasos anteriores para obtener activos de nodos de computación adicionales que se deben actualizar con una contraseña nueva.
10. Vaya a https://<mNode_ip>/inventory/1/.
- a. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña de administración del clúster de SolidFire de NetApp.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Haga clic en **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana.
 - b. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /Installations**.
 - c. Haga clic en **probar**.
 - d. Seleccione **Verdadero** en la lista desplegable Descripción de actualización.
 - e. Haga clic en **Ejecutar**.
 - f. Validar que la respuesta es HTTP 200.
11. Espere aproximadamente 15 minutos para que desaparezca el mensaje de bloqueo de cuenta en vCenter.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Gestione el almacenamiento NetApp HCI

Información general del almacenamiento de Manage NetApp HCI

Con NetApp HCI, puede gestionar estos activos de almacenamiento utilizando el control del cloud híbrido de NetApp.

- ["Crear y administrar cuentas de usuario"](#)
- ["Añadir y gestionar clústeres de almacenamiento"](#)
- ["Cree y gestione volúmenes"](#)
- ["Permite crear y gestionar grupos de acceso de volúmenes"](#)
- ["Cree y gestione iniciadores"](#)
- ["Cree y gestione políticas de calidad de servicio de volúmenes"](#)

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Cree y gestione cuentas de usuario con NetApp Hybrid Cloud Control

En los sistemas de almacenamiento basados en Element, se pueden crear usuarios de clúster autorizados para permitir el acceso de inicio de sesión a Hybrid Cloud Control de NetApp en función de los permisos que desee para los usuarios "Administrator" o "Read-only". Además de los usuarios del clúster, también hay cuentas de volúmenes que permiten que los clientes se conecten a volúmenes en un nodo de almacenamiento.

Gestione los siguientes tipos de cuentas:

- [Administrar cuentas de clúster autorizadas](#)
- [Permite gestionar cuentas de volumen](#)

Habilite LDAP

Para utilizar LDAP en cualquier cuenta de usuario, primero debe habilitar LDAP.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, haga clic en el icono de opciones de la parte superior derecha y seleccione **Gestión de usuarios**.
3. En la página Users (usuarios), haga clic en **Configure LDAP** (Configurar LDAP*).
4. Defina su configuración de LDAP.
5. Seleccione el tipo de autenticación Search and Bind o Direct Bind.
6. Antes de guardar los cambios, haga clic en **probar conexión LDAP** en la parte superior de la página, introduzca el nombre de usuario y la contraseña de un usuario que sepa que existe y haga clic en **Prueba**.

7. Haga clic en **Guardar**.

Administrar cuentas de clúster autorizadas

"[Cuentas de usuario autoritativas](#)" Se gestionan desde la opción de gestión de usuarios del menú superior derecho del control del cloud híbrido de NetApp. Estos tipos de cuentas permiten la autenticación en cualquier activo de almacenamiento asociado con una instancia de NetApp Hybrid Cloud Control de nodos y clústeres. Con esta cuenta, puede gestionar volúmenes, cuentas, grupos de acceso y mucho más en todos los clústeres.

Cree una cuenta de clúster autorizada

Puede crear una cuenta con Hybrid Cloud Control de NetApp.

Esta cuenta puede usarse para iniciar sesión en el control de cloud híbrido, la interfaz de usuario por nodo del clúster y el clúster de almacenamiento en el software NetApp Element.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, haga clic en el icono de opciones de la parte superior derecha y seleccione **Gestión de usuarios**.
3. Seleccione **Crear usuario**.
4. Seleccione el tipo de autenticación del clúster o LDAP.
5. Realice una de las siguientes acciones:
 - Si seleccionó LDAP, introduzca el DN.



Para usar LDAP, primero se debe habilitar LDAP o LDAPS. Consulte [Habilite LDAP](#).

- Si seleccionó Cluster como Auth Type, introduzca un nombre y una contraseña para la nueva cuenta.

6. Seleccione permisos de administrador o de solo lectura.



Para ver los permisos del software NetApp Element, haga clic en **Mostrar permisos heredados**. Si selecciona un subconjunto de estos permisos, a la cuenta se le asignan permisos de sólo lectura. Si selecciona todos los permisos heredados, la cuenta tiene permisos de administrador asignados.



Para asegurarse de que todos los hijos de un grupo heredan permisos, cree un grupo de administración de organización DN en el servidor LDAP. Todas las cuentas secundarias de ese grupo heredarán dichos permisos.

7. Marque la casilla que indica que "he leído y acepto el contrato de licencia para usuario final de NetApp".
8. Haga clic en **Crear usuario**.

Edite una cuenta de clúster autorizada

Puede cambiar los permisos o la contraseña de una cuenta de usuario mediante NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, haga clic en el icono de la parte superior derecha y seleccione **Gestión de usuarios**.
3. Si lo desea, puede filtrar la lista de cuentas de usuario seleccionando **Cluster, LDAP** o **IDP**.

Si configuró usuarios en el clúster de almacenamiento con LDAP, esas cuentas muestran un tipo de usuario "LDAP". Si configuró usuarios en el clúster de almacenamiento con IDP, esas cuentas muestran un tipo de usuario "IDP".

4. En la columna **acciones** de la tabla, expanda el menú de la cuenta y seleccione **Editar**.
5. Realice los cambios necesarios.
6. Seleccione **Guardar**.
7. Cierre la sesión en Hybrid Cloud Control de NetApp.
8. "**Actualice las credenciales**" Obtenga el activo autorizado de clústeres mediante la API de control de cloud híbrido de NetApp.



Es posible que la interfaz de usuario de control de cloud híbrido de NetApp demore hasta 2 minutos en actualizar el inventario. Para actualizar manualmente el inventario, acceda al servicio de inventario de la interfaz de usuario de LA API DE REST <https://<ManagementNodeIP>/inventory/1/> y correr GET /installations /{id} para el clúster.

9. Inicie sesión en NetApp Hybrid Cloud Control.

Elimine una cuenta de usuario autorizada

Puede eliminar una o varias cuentas cuando ya no sea necesaria. Es posible eliminar una cuenta de usuario de LDAP.

No puede eliminar la cuenta de usuario de administrador principal para el clúster autorizado.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, haga clic en el icono de la parte superior derecha y seleccione **Gestión de usuarios**.
3. En la columna **acciones** de la tabla Users (usuarios), expanda el menú de la cuenta y seleccione **Delete** (Eliminar).
4. Confirme la eliminación seleccionando **Sí**.

Permite gestionar cuentas de volumen

"**Cuentas de volumen**" Se gestionan en la tabla volúmenes de control del cloud híbrido de NetApp. Estas cuentas solo son específicas del clúster de almacenamiento en el que se crearon. Estos tipos de cuentas permiten establecer permisos en los volúmenes de la red, pero no afectan fuera de dichos volúmenes.

Una cuenta de volumen contiene la autenticación CHAP que se necesita para acceder a los volúmenes que tiene asignados.

Cree una cuenta de volumen

Cree una cuenta específica para este volumen.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, seleccione **almacenamiento > volúmenes**.
3. Seleccione la ficha **Cuentas**.
4. Seleccione el botón **Crear cuenta**.
5. Escriba un nombre para la cuenta nueva.
6. En la sección CHAP Settings, introduzca la siguiente información:
 - Initiator Secret para la autenticación CHAP de la sesión de nodo
 - Target Secret para la autenticación CHAP de la sesión de nodo



Para generar automáticamente cualquiera de las contraseñas, deje los campos de credenciales vacíos.

7. Seleccione **Crear cuenta**.

Editar una cuenta de volumen

Puede cambiar la información de CHAP y cambiar si una cuenta está activa o bloqueada.



Si se elimina o se bloquea una cuenta asociada con el nodo de gestión, se produce un nodo de gestión inaccesible.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, seleccione **almacenamiento > volúmenes**.
3. Seleccione la ficha **Cuentas**.
4. En la columna **acciones** de la tabla, expanda el menú de la cuenta y seleccione **Editar**.
5. Realice los cambios necesarios.
6. Confirme los cambios seleccionando **Sí**.

Eliminar una cuenta de volumen

Elimine una cuenta que ya no necesite.

Antes de eliminar una cuenta de volumen, elimine y purgue todos los volúmenes asociados con la cuenta en primer lugar.



Si se elimina o se bloquea una cuenta asociada con el nodo de gestión, se produce un nodo de gestión inaccesible.



Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada. Si elimina estas cuentas, podría dejar el nodo de gestión en estado inutilizable.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, seleccione **almacenamiento > volúmenes**.
3. Seleccione la ficha **Cuentas**.
4. En la columna **acciones** de la tabla, expanda el menú de la cuenta y seleccione **Eliminar**.
5. Confirme la eliminación seleccionando **Sí**.

Obtenga más información

- ["Más información acerca de las cuentas"](#)
- ["Trabajar con cuentas de usuario"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Añada y gestione clústeres de almacenamiento utilizando Hybrid Cloud Control de NetApp

Puede añadir clústeres de almacenamiento al inventario de activos del nodo de gestión para poder gestionarlos mediante el control del cloud híbrido (HCC) de NetApp. El primer clúster de almacenamiento añadido durante la configuración del sistema es el valor predeterminado "[clúster de almacenamiento fiable](#)", Pero se pueden añadir agrupaciones adicionales con la interfaz de usuario de HCC.

Después de añadir un clúster de almacenamiento, es posible supervisar el rendimiento del clúster, cambiar las credenciales del clúster de almacenamiento del activo gestionado o quitar un clúster de almacenamiento del inventario de activos del nodo de gestión si ya no se necesita gestionar mediante HCC.

A partir de Element 12.2, puede utilizar la "[modo de mantenimiento](#)" opciones de funciones para habilitar y deshabilitar el modo de mantenimiento para los nodos del clúster de almacenamiento.

Lo que necesitará

- **Permisos de administrador de clúster:** Tiene permisos como administrador en "[clúster de almacenamiento fiable](#)". El clúster de autoridad es el primer clúster que se ha agregado al inventario de nodos de gestión durante la configuración del sistema.
- **Software Element:** La versión del clúster de almacenamiento ejecuta el software NetApp Element 11.3 o posterior.
- **Nodo de gestión:** Ha implementado un nodo de gestión que ejecuta la versión 11.3 o posterior.
- **Servicios de administración:** Ha actualizado su paquete de servicios de administración a la versión 2.17 o posterior.

Opciones

- [Añada un clúster de almacenamiento](#)
- [Confirmar el estado del clúster de almacenamiento](#)
- [Editar credenciales del clúster de almacenamiento](#)
- [Quite un clúster de almacenamiento de](#)
- [Habilite y deshabilite el modo de mantenimiento](#)

Añada un clúster de almacenamiento

Puede añadir un clúster de almacenamiento al inventario de activos del nodo de gestión con Hybrid Cloud Control de NetApp. Esto permite gestionar y supervisar el clúster con la interfaz de usuario de HCC.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento**.
4. Seleccione **Agregar clúster de almacenamiento**.
5. Introduzca la siguiente información:
 - Dirección IP virtual de gestión del clúster de almacenamiento



Solo se pueden añadir clústeres de almacenamiento remotos que actualmente no están gestionados por un nodo de gestión.

- Nombre de usuario y contraseña del clúster de almacenamiento

6. Seleccione **Agregar**.



Después de añadir el clúster de almacenamiento, el inventario de clústeres puede tardar hasta 2 minutos en actualizarse y mostrar los nuevos adición. Es posible que deba actualizar la página en el explorador para ver los cambios.

7. Si va a añadir clústeres eSDS de Element, introduzca o cargue la clave privada SSH y la cuenta de usuario SSH.

Confirmar el estado del clúster de almacenamiento

Puede supervisar el estado de conexión de activos de clústeres de almacenamiento mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. Revise el estado de los clústeres de almacenamiento de en el inventario.
4. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento** para obtener más información.

Editar credenciales del clúster de almacenamiento

Puede editar el nombre de usuario y la contraseña del administrador del clúster de almacenamiento mediante la interfaz de usuario de NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento**.
4. Seleccione el menú **acciones** para el clúster y seleccione **Editar credenciales de clúster**.
5. Actualice el nombre de usuario y la contraseña del clúster de almacenamiento.
6. Seleccione **Guardar**.

Quite un clúster de almacenamiento de

Al quitar un clúster de almacenamiento de NetApp Hybrid Cloud Control, se quita el clúster del inventario del nodo de gestión. Una vez que se quita un clúster de almacenamiento, el clúster ya no puede gestionarse mediante HCC y solo es posible acceder a él; para ello, solo debe navegar directamente a su dirección IP de gestión.



No se puede quitar el clúster autorizado del inventario. Para determinar el clúster autorizado, vaya a **Administración de usuarios > usuarios**. El clúster autorizado se muestra junto al encabezado **usuarios**.

Pasos

1. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador autorizadas del clúster de almacenamiento.
2. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
3. En el panel **clústeres de almacenamiento**, seleccione **Detalles del clúster de almacenamiento**.
4. Seleccione el menú **acciones** del clúster y seleccione **Quitar clúster de almacenamiento**.



Al hacer clic en **Sí** a continuación, se elimina el clúster de la instalación.

5. Seleccione **Sí**.

Habilite y deshabilite el modo de mantenimiento

Este "**modo de mantenimiento**" las opciones de funciones le proporcionan la capacidad a. [habilite](#) y. [desactivar](#) modo de mantenimiento para un nodo de clúster de almacenamiento.

Lo que necesitará

- **Software Element:** La versión del clúster de almacenamiento ejecuta el software NetApp Element 12.2 o posterior.
- **Nodo de gestión:** Ha implementado un nodo de gestión que ejecuta la versión 12.2 o posterior.
- **Servicios de administración:** Ha actualizado su paquete de servicios de administración a la versión 2.19

o posterior.

- Tiene acceso para iniciar sesión en el nivel de administrador.

Habilitar el modo de mantenimiento

Puede utilizar el siguiente procedimiento para habilitar el modo de mantenimiento para un nodo de clúster de almacenamiento.



Solo un nodo puede estar en modo de mantenimiento a la vez.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.



Las opciones de las funciones del modo de mantenimiento se deshabilitan en el nivel de solo lectura.

3. En el cuadro azul de navegación izquierdo, seleccione la instalación de NetApp HCI.
4. En el panel de navegación izquierdo, seleccione **Nodes**.
5. Para ver la información del inventario de almacenamiento, seleccione **almacenamiento**.
6. Habilite el modo de mantenimiento en un nodo de almacenamiento:

La tabla nodos de almacenamiento se actualiza automáticamente cada dos minutos para las acciones iniciadas por el usuario no. Antes de una acción, para asegurarse de tener el estado más actualizado, puede actualizar la tabla nodos con el icono de actualización ubicado en el lado superior derecho de la tabla nodos.



- a. En **acciones**, seleccione **Activar modo de mantenimiento**.

Mientras **modo de mantenimiento** está activado, las acciones del modo de mantenimiento no están disponibles para el nodo seleccionado y para todos los demás nodos del mismo clúster.

Una vez completada **activación del modo de mantenimiento**, la columna **Estado del nodo** muestra un

icono de llave y el texto "**modo de mantenimiento**" para el nodo que está en modo de mantenimiento.

desactive el modo de mantenimiento

Una vez que un nodo se ha colocado correctamente en modo de mantenimiento, la acción **Desactivar modo de mantenimiento** está disponible para este nodo. Las acciones en los otros nodos no están disponibles hasta que el modo de mantenimiento se deshabilita correctamente en el nodo que experimenta mantenimiento.

Pasos

1. Para el nodo en modo de mantenimiento, en **acciones**, seleccione **Desactivar modo de mantenimiento**.

Mientras **el modo de mantenimiento** está desactivado, las acciones del modo de mantenimiento no están disponibles para el nodo seleccionado y para todos los demás nodos del mismo clúster.

Después de que se completa **desactivación del modo de mantenimiento**, la columna **Estado del nodo** muestra **activo**.



Cuando un nodo se encuentra en modo de mantenimiento, no acepta datos nuevos. Como resultado, puede tardar más tiempo en deshabilitar el modo de mantenimiento, porque el nodo debe sincronizar sus datos de nuevo para poder salir del modo de mantenimiento. Cuanto más tiempo gaste en el modo de mantenimiento, más tiempo será necesario para deshabilitar el modo de mantenimiento.

Solucionar problemas

Si se producen errores cuando se habilita o se deshabilita el modo de mantenimiento, se muestra un error de banner en la parte superior de la tabla Nodes. Para obtener más información sobre el error, puede seleccionar el enlace **Mostrar detalles** que se proporciona en el banner para mostrar cuáles son las devoluciones de la API.

Obtenga más información

- ["Crear y gestionar activos de clúster de almacenamiento"](#)
- ["Página de recursos de NetApp HCI"](#)

Cree y gestione volúmenes mediante Hybrid Cloud Control de NetApp

Es posible crear un volumen y asociarlo con una cuenta determinada. Al asociar un volumen con una cuenta, la cuenta podrá acceder al volumen a través de iniciadores iSCSI y las credenciales de CHAP.

Puede especificar la configuración de calidad de servicio de un volumen mientras lo crea.

Puede gestionar volúmenes en NetApp Hybrid Cloud Control de las siguientes formas:

- [Cree un volumen](#)
- [Aplique una política de calidad de servicio en un volumen](#)
- [Editar un volumen](#)
- [Clonar volúmenes](#)

- Añadir volúmenes a un grupo de acceso de volúmenes
- Eliminar un volumen
- Restaurar un volumen eliminado
- Purgar un volumen eliminado

Cree un volumen

Puede crear un volumen de almacenamiento con NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione la ficha **volúmenes** > **Descripción general**.

ID ↑	Name	Account	Access Groups	Access	Used	Size	Snapshots	QoS Policy	Min IOPS	Max IOPS	Burst IOPS	iSCSI Sessions	Actions
1	NetApp-HCI-Datastore-01	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	4%	2.15 TB	0		50	15000	15000	2	⋮
2	NetApp-HCI-Datastore-02	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	0%	2.15 TB	0		50	15000	15000	2	⋮
3	NetApp-HCI-credential...			Read/Write	0%	5.37 GB	0		1000	2000	4000	1	⋮
4	NetApp-HCI-mnode-api			Read/Write	0%	53.69 GB	0		1000	2000	4000	1	⋮
5	NetApp-HCI-hci-monitor			Read/Write	0%	1.07 GB	0		1000	2000	4000	1	⋮

4. Seleccione **Crear volumen**.
5. Escriba un nombre para el volumen nuevo.
6. Introduzca el tamaño total del volumen.



El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GiB: 1 GB = 1 000 000 000 bytes 1 GiB = 1 073 741 824 bytes

7. Seleccione un tamaño de bloque para el volumen.
8. En la lista **cuenta**, seleccione la cuenta que debe tener acceso al volumen.

Si no existe ninguna cuenta, haga clic en **Crear nueva cuenta**, escriba un nuevo nombre de cuenta y haga clic en **Crear cuenta**. La cuenta se crea y se asocia con el nuevo volumen en la lista **cuenta**.



Si hay más de 50 cuentas, no aparecerá la lista. Comience a escribir y la función de autocompletar mostrará los valores que puede elegir.

9. Para configurar Quality of Service del volumen, realice una de las siguientes acciones:
 - En **Configuración de calidad de servicio**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores de QoS predeterminados.
 - Seleccione una política de QoS existente activando la opción **asignar directiva de calidad de servicio** y eligiendo una política de QoS existente en la lista resultante.

- Cree y asigne una nueva directiva QoS activando el botón **asignar directiva de calidad de servicio** y haciendo clic en **Crear nueva directiva QoS**. En la ventana que se abre, escriba un nombre para la política de calidad de servicio y, a continuación, escriba los valores de calidad de servicio. Cuando termine, haga clic en **Crear política de calidad de servicio**.

Los volúmenes que tengan un valor de IOPS máximo o de ráfaga superior a 20 20,000 IOPS podrían requerir una profundidad de cola alta o varias sesiones para alcanzar este nivel de IOPS en un único volumen.

10. Haga clic en **Crear volumen**.

Aplique una política de calidad de servicio en un volumen

Puede aplicar una política de calidad de servicio a los volúmenes de almacenamiento existentes mediante Cloud Control de NetApp. Si en cambio, debe establecer valores de calidad de servicio personalizados para un volumen, puede hacerlo [Editar un volumen](#). Para crear una nueva política de calidad de servicio, consulte ["Cree y gestione políticas de calidad de servicio de volúmenes"](#).

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes > Descripción general**.
4. Seleccione uno o varios volúmenes para asociarlos con una política de calidad de servicio.
5. Haga clic en la lista desplegable **acciones** situada en la parte superior de la tabla Volumes y seleccione **aplicar directiva QoS**.
6. En la ventana resultante, seleccione una directiva QoS de la lista y haga clic en **aplicar directiva QoS**.



Si utiliza políticas de calidad de servicio en un volumen, puede establecer la calidad de servicio personalizada para quitar la asociación de la política de calidad de servicio con el volumen. Los valores de calidad de servicio personalizados anulan los valores de política de calidad de servicio de los volúmenes.

Editar un volumen

Con Hybrid Cloud Control de NetApp, es posible editar atributos de volúmenes como los valores de calidad de servicio, el tamaño de los volúmenes y la unidad de medida mediante la cual se calculan los valores de bytes. También se puede modificar el acceso de la cuenta para el uso de la replicación o para restringir el acceso al volumen.

Acerca de esta tarea

Puede cambiar el tamaño de un volumen cuando haya espacio suficiente en el clúster en las siguientes condiciones:

- Condiciones de funcionamiento normales.
- Se informa de los errores de los volúmenes.
- El volumen se clona.
- El volumen se vuelve a sincronizar.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes > Descripción general**.
4. En la columna **acciones** de la tabla Volumes, expanda el menú para el volumen y seleccione **Editar**.
5. Realice los cambios necesarios:

- a. Cambie el tamaño total del volumen.



Puede aumentar el tamaño del volumen, pero no reducirlo. En cada operación de ajuste de tamaño, solo se puede ajustar el tamaño de un volumen. Las operaciones de recopilación de datos basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.



Si desea ajustar el tamaño del volumen para la replicación, primero aumente el tamaño del volumen asignado como el destino de replicación. Posteriormente, puede cambiar el tamaño del volumen de origen. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.



El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GiB: 1 GB = 1 000 000 000 bytes 1 GiB = 1 073 741 824 bytes

- b. Seleccione un nivel de acceso de cuenta diferente:

- Solo lectura
- Lectura/Escritura
- Bloqueado
- Destino de replicación

- c. Seleccione la cuenta que debería tener acceso al volumen.

Comience a escribir y la función de autocompletar mostrará los posibles valores que puede elegir.

Si no existe ninguna cuenta, haga clic en **Crear nueva cuenta**, escriba un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se creará y se asociará con el volumen existente.

- d. Cambie la calidad de servicio llevando a cabo una de las siguientes acciones:

- i. Seleccione una política existente.
- ii. En Custom Settings, establezca los valores mínimos, máximos y de ráfaga para IOPS, o bien utilice los valores predeterminados.



Si utiliza políticas de calidad de servicio en un volumen, puede establecer la calidad de servicio personalizada para quitar la asociación de la política de calidad de servicio con el volumen. La calidad de servicio personalizada anulará los valores de las políticas de calidad de servicio de los volúmenes.



Cuando cambie los valores de IOPS, debe incrementar sus diez o cien. Los valores de entrada deben ser números enteros válidos. Configure los volúmenes con un valor de ráfaga muy alto. De este modo, el sistema podrá procesar grandes cargas de trabajo secuenciales en bloque ocasionales con mayor rapidez, a la vez que se limitan las IOPS sostenidas de un volumen.

6. Seleccione **Guardar**.

Clonar volúmenes

Es posible crear un clon de un solo volumen de almacenamiento o clonar un grupo de volúmenes para hacer una copia de los datos en un momento específico. Cuando se clona un volumen, el sistema crea una copia de Snapshot del volumen y, a continuación, crea una copia de los datos que se indican en la copia de Snapshot.

Antes de empezar

- Debe haber al menos un clúster añadido y en ejecución.
- Se creó al menos un volumen.
- Se creó una cuenta de usuario.
- El espacio sin aprovisionar disponible debe ser igual o mayor que el tamaño del volumen.

Acerca de esta tarea

El clúster admite hasta dos solicitudes de clones en ejecución por volumen a la vez y hasta 8 operaciones de clones de volúmenes activos a la vez. Las solicitudes que superen este límite se pondrán en cola para procesarlas más adelante.

El clonado de volúmenes es un proceso asíncrono, y la cantidad de tiempo que requiere el proceso depende del tamaño del volumen que se clona y de la carga del clúster actual.



Los volúmenes clonados no heredan pertenencia al grupo de acceso de volúmenes en el volumen de origen.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione la ficha **volúmenes > Descripción general**.
4. Seleccione cada volumen que desea clonar.
5. Haga clic en la lista desplegable **acciones** situada en la parte superior de la tabla Volumes y seleccione **Clonar**.
6. En la ventana que se abre, realice lo siguiente:
 - a. Introduzca un prefijo de nombre de volumen (lo cual es opcional).
 - b. Seleccione el tipo de acceso en la lista **Access**.
 - c. Elija una cuenta para asociar con el nuevo clon de volumen (de forma predeterminada, se selecciona **Copiar desde volumen**, que utilizará la misma cuenta que el volumen original).
 - d. Si no existe ninguna cuenta, haga clic en **Crear nueva cuenta**, escriba un nuevo nombre de cuenta y haga clic en **Crear cuenta**. La cuenta se creará y se asociará con el volumen.



Utilice prácticas recomendadas de nomenclatura descriptiva. Esto es especialmente importante si se utilizan varios clústeres o instancias de vCenter Server en el entorno.



Al aumentar el tamaño del volumen de un clon, se genera un volumen nuevo con espacio libre adicional al final del volumen. Según cómo use el volumen, podría necesitar ampliar las particiones o crear otras nuevas en el espacio libre para utilizarlo.

a. Haga clic en **Clonar volúmenes**.



El tiempo para completar una operación de clonación se ve afectado por el tamaño del volumen y la carga actual del clúster. Actualice la página si el volumen clonado no aparece en la lista de volúmenes.

Añada volúmenes a un grupo de acceso de volúmenes

Es posible añadir un volumen único o un grupo de volúmenes a un grupo de acceso de volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes** > **Descripción general**.
4. Seleccione uno o varios volúmenes para asociarlos con un grupo de acceso de volúmenes.
5. Haga clic en la lista desplegable **acciones** de la parte superior de la tabla Volumes y seleccione **Agregar a grupo de acceso**.
6. En la ventana que aparece, seleccione un grupo de acceso de volúmenes de la lista **Grupo de acceso de volúmenes**.
7. Haga clic en **Añadir volumen**.

Eliminar un volumen

Es posible eliminar uno o varios volúmenes de un clúster de almacenamiento de Element.

Acerca de esta tarea

El sistema no purga de manera inmediata volúmenes eliminados; estos siguen disponibles durante aproximadamente ocho horas. Después de ocho horas, se purgan y ya no están disponibles. Si un volumen se restaura antes de que el sistema lo purgue, el volumen volverá a conectarse y las conexiones iSCSI se restaurarán.

Si se elimina el volumen que se utilizó para crear una snapshot, sus snapshots asociadas pasan a estar inactivas. Cuando se purgan los volúmenes de origen eliminados, también se eliminan del sistema las snapshots inactivas asociadas.



Los volúmenes persistentes asociados con servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine los volúmenes o su cuenta asociada. Si elimina estos volúmenes, podría dejar el nodo de gestión inutilizable.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes > Descripción general**.
4. Seleccione uno o varios volúmenes para eliminarlos.
5. Haga clic en la lista desplegable **acciones** situada en la parte superior de la tabla Volumes y seleccione **Eliminar**.
6. En la ventana resultante, confirme la acción haciendo clic en **Sí**.

Restaurar un volumen eliminado

Después de eliminar un volumen de almacenamiento, es posible restaurarlo si lo hace antes de ocho horas después de la eliminación.

El sistema no purga de manera inmediata volúmenes eliminados; estos siguen disponibles durante aproximadamente ocho horas. Después de ocho horas, se purgan y ya no están disponibles. Si un volumen se restaura antes de que el sistema lo purgue, el volumen volverá a conectarse y las conexiones iSCSI se restaurarán.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes > Descripción general**.
4. Seleccione **eliminado**.
5. En la columna **acciones** de la tabla Volumes, expanda el menú para el volumen y seleccione **Restaurar**.
6. Confirme el proceso seleccionando **Sí**.

Purgar un volumen eliminado

Una vez que se eliminan los volúmenes de almacenamiento, siguen disponibles durante ocho horas aproximadamente. Después de ocho horas, se purgan automáticamente y ya no están disponibles. Si no desea esperar las ocho horas, puede eliminarse

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes > Descripción general**.
4. Seleccione **eliminado**.
5. Seleccione uno o varios volúmenes para purgar.
6. Debe realizar una de las siguientes acciones:
 - Si ha seleccionado varios volúmenes, haga clic en el filtro rápido **Purge** situado en la parte superior de la tabla.
 - Si seleccionó un único volumen, en la columna **acciones** de la tabla Volumes, expanda el menú para el volumen y seleccione **Purgar**.

7. En la columna **acciones** de la tabla de volúmenes, expanda el menú para el volumen y seleccione **Purgar**.
8. Confirme el proceso seleccionando **Sí**.

Obtenga más información

- ["Más información acerca de los volúmenes"](#)
- ["Documentación de SolidFire y el software Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Permite crear y gestionar grupos de acceso de volúmenes

Se pueden crear nuevos grupos de acceso de volúmenes, realizar cambios en el nombre, los iniciadores asociados o los volúmenes asociados de los grupos de acceso, o eliminar los grupos de acceso de volúmenes existentes mediante NetApp Hybrid Cloud Control.

Lo que necesitará

- Tiene credenciales de administrador para este sistema NetApp HCI.
- Ha actualizado sus servicios de administración a al menos la versión 2.15.28. La gestión del almacenamiento de control de cloud híbrido de NetApp no está disponible en versiones anteriores del paquete de servicio.
- Asegúrese de tener un esquema de nomenclatura lógico para los grupos de acceso de volúmenes.

Añadir un grupo de acceso de volúmenes

Es posible añadir un grupo de acceso de volúmenes a un clúster de almacenamiento mediante NetApp Hybrid Cloud Control.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la ficha **grupos de acceso**.
5. Seleccione el botón **Crear grupo de acceso**.
6. En el cuadro de diálogo que se abre, escriba un nombre para el nuevo grupo de acceso de volúmenes.
7. (Opcional) en la sección **Initiators**, seleccione uno o más iniciadores para asociarlos con el nuevo grupo de acceso de volúmenes.

Si asocia un iniciador con el grupo de acceso de volúmenes, ese iniciador puede acceder a cada volumen del grupo sin necesidad de autenticación.

8. (Opcional) en la sección **Volumes**, seleccione uno o varios volúmenes para incluirlos en este grupo de acceso de volúmenes.
9. Seleccione **Crear grupo de acceso**.

Edite un grupo de acceso de volúmenes

Puede editar las propiedades de un grupo de acceso de volúmenes existente mediante NetApp Hybrid Cloud Control. Es posible realizar cambios en el nombre, los iniciadores asociados o los volúmenes asociados de un grupo de acceso.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la ficha **grupos de acceso**.
5. En la columna **acciones** de la tabla de grupos de acceso, expanda el menú de opciones para el grupo de acceso que necesita editar.
6. En el menú de opciones, seleccione **Editar**.
7. Realice los cambios necesarios en el nombre, los iniciadores asociados o los volúmenes asociados.
8. Confirme los cambios seleccionando **Guardar**.
9. En la tabla **grupos de acceso**, compruebe que el grupo de acceso refleja los cambios.

Elimine un grupo de acceso de volúmenes

Es posible quitar un grupo de acceso de volúmenes mediante NetApp Hybrid Cloud Control y, al mismo tiempo, quitar los iniciadores asociados con este grupo de acceso del sistema.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la ficha **grupos de acceso**.
5. En la columna **acciones** de la tabla de grupos de acceso, expanda el menú de opciones para el grupo de acceso que necesita eliminar.
6. En el menú de opciones, seleccione **Eliminar**.
7. Si no desea eliminar los iniciadores asociados con el grupo de acceso, anule la selección de la casilla de verificación **Eliminar iniciadores de este grupo de acceso**.
8. Confirme la operación de eliminación seleccionando **Sí**.

Obtenga más información

- ["Obtenga información acerca de los grupos de acceso de volúmenes"](#)
- ["Añada un iniciador de a un grupo de acceso de volúmenes"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Cree y gestione iniciadores

Puede utilizar "iniciadores" Para el acceso basado en CHAP en lugar de basado en la cuenta a los volúmenes. Los iniciadores se pueden crear y eliminar, y es posible asignarles alias descriptivos para simplificar la administración y el acceso de los volúmenes. Cuando se añade un iniciador a un grupo de acceso de volúmenes, ese iniciador permite el acceso a todos los volúmenes del grupo.

Lo que necesitará

- Tiene credenciales de administrador del clúster.
- Ha actualizado sus servicios de administración a al menos la versión 2.17. La gestión del iniciador de control de cloud híbrido de NetApp no está disponible en versiones anteriores del paquete de servicio.

Opciones

- [Cree un iniciador](#)
- [Añada iniciadores a un grupo de acceso de volúmenes](#)
- [Cambie un alias de iniciador](#)
- [Elimine los iniciadores](#)

Cree un iniciador

Es posible crear iniciadores iSCSI o Fibre Channel y, opcionalmente, asignarles alias.

Acerca de esta tarea

El formato aceptado de un IQN de iniciador es `iqn.yyyy-mm` donde `y` y `m` son dígitos seguidos de texto que solo puede contener dígitos, caracteres alfabéticos en minúscula, un punto (`.`), dos puntos (`:`) o guión (`-`). A continuación, se ofrece un ejemplo de formato:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

El formato aceptado de WWPN de un iniciador Fibre Channel es `:Aa:bB:CC:dd:11:22:33:44` o `AabBCCdd11223344`. A continuación, se ofrece un ejemplo de formato:

```
5f:47:ac:c0:5c:74:d4:02
```

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. Seleccione el botón **Crear iniciadores**.

Opción	Pasos
Cree uno o varios iniciadores	<ol style="list-style-type: none"> Introduzca el IQN o el WWPN del iniciador en el campo IQN/WWPN. Introduzca un nombre descriptivo para el iniciador en el campo Alias. (Opcional) Seleccione Agregar iniciador para abrir nuevos campos de iniciador o utilice la opción creación masiva en su lugar. Seleccione Crear iniciadores.
Cree iniciadores masivos	<ol style="list-style-type: none"> Seleccione adición masiva de IQN/WWPN. Introduzca una lista de varios IQN o WWPN en el cuadro de texto. Cada IQN o WWPN debe estar separado por comas o espacios en su propia línea. Seleccione Agregar IQN/WWPN. (Opcional) Añada alias únicos a cada iniciador. Quite todos los iniciadores de la lista que puedan existir ya en la instalación. Seleccione Crear iniciadores.

Añada iniciadores a un grupo de acceso de volúmenes

Es posible añadir un iniciador a un grupo de acceso de volúmenes. Cuando se añade un iniciador a un grupo de acceso de volúmenes, el iniciador permite el acceso a todos los volúmenes en ese grupo de acceso de volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. Seleccione uno o varios iniciadores que desee añadir.
6. Seleccione **acciones > Agregar a grupo de acceso**.
7. Seleccione el grupo de acceso.
8. Confirme los cambios seleccionando **Agregar iniciador**.

Cambie un alias de iniciador

Es posible cambiar el alias de un iniciador existente o añadir un alias si aún no hay ninguno.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster

de almacenamiento de Element.

2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. En la columna **acciones**, expanda el menú de opciones del iniciador.
6. Seleccione **Editar**.
7. Realice los cambios necesarios en el alias o agregue un nuevo alias.
8. Seleccione **Guardar**.

Elimine los iniciadores

Puede eliminar uno o varios iniciadores. Cuando se elimina un iniciador, el sistema la quita de los grupos de acceso de volúmenes asociados. Las conexiones que usan el iniciador siguen siendo válidas hasta que se restablece la conexión.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de Element.
2. En Dashboard de, expanda el nombre del clúster de almacenamiento en el menú de navegación izquierdo.
3. Seleccione **volúmenes**.
4. Seleccione la pestaña **Initiators**.
5. Elimine uno o varios iniciadores:
 - a. Seleccione el o los iniciadores que desea eliminar.
 - b. Seleccione **acciones > Eliminar**.
 - c. Confirme la operación de eliminación y seleccione **Sí**.

Obtenga más información

- ["Obtenga más información acerca de los iniciadores"](#)
- ["Obtenga información acerca de los grupos de acceso de volúmenes"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Cree y gestione políticas de calidad de servicio de volúmenes

Una política de calidad de servicio (QoS) permite crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes. El clúster seleccionado debe ser Element 10.0 o posterior para usar políticas de calidad de servicio; de lo contrario, las funciones de las políticas de calidad de servicio no estarán disponibles.



Consulte el contenido de conceptos de NetApp HCI para obtener más información sobre el uso de ["Políticas de calidad de servicio"](#) en lugar de volumen individual ["Calidad de servicio"](#).

Con el control del cloud híbrido de NetApp, puede crear y gestionar políticas de calidad de servicio

completando las siguientes tareas:

- [Cree una política de calidad de servicio](#)
- [Aplique una política de calidad de servicio en un volumen](#)
- [Cambie la asignación de políticas de calidad de servicio de un volumen](#)
- [Edite una política de calidad de servicio](#)
- [Elimine una política de calidad de servicio](#)

Cree una política de calidad de servicio

Puede crear políticas de calidad de servicio y aplicarlas a volúmenes que tengan un rendimiento equivalente.



Si utiliza políticas de calidad de servicio, no use la calidad de servicio personalizada en un volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Haga clic en la ficha **Directivas de QoS**.
5. Haga clic en **Crear directiva**.
6. Introduzca el **Nombre de la directiva**.



Utilice prácticas recomendadas de nomenclatura descriptiva. Esto es especialmente importante si se utilizan varios clústeres o instancias de vCenter Server en el entorno.

7. Introduzca los valores mínimos de IOPS, máximo de IOPS y de IOPS de ráfaga.
8. Haga clic en **Crear directiva QoS**.

Se genera un ID del sistema para la política y esta se muestra en la página QoS Políticas con sus valores de calidad de servicio asignados.

Aplique una política de calidad de servicio en un volumen

Puede asignar una política de calidad de servicio existente a un volumen con Hybrid Cloud Control de NetApp.

Lo que necesitará

Se ha aplicado la política de calidad de servicio que desea asignar [creado](#).

Acerca de esta tarea

En esta tarea, se describe cómo asignar una política de calidad de servicio a un volumen individual mediante el cambio de configuración. La última versión de Hybrid Cloud Control de NetApp no tiene una opción de asignación masiva para más de un volumen. Hasta que la funcionalidad que se debe asignar de forma masiva se proporcione en una versión futura, se puede usar la interfaz de usuario web de Element o la interfaz de usuario del plugin de vCenter para asignar de forma masiva políticas de calidad de servicio.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Haga clic en el menú **acciones** situado junto al volumen que desea modificar.
5. En el menú que se abre, seleccione **Editar**.
6. En el cuadro de diálogo, habilite **asignar directiva QoS** y seleccione la directiva QoS en la lista desplegable para aplicarla al volumen seleccionado.



La asignación de calidad de servicio anulará los valores de QoS de cada volumen que se hayan aplicado anteriormente.

7. Haga clic en **Guardar**.

El volumen actualizado con la política de calidad de servicio asignada se muestra en la página Overview.

Cambie la asignación de políticas de calidad de servicio de un volumen

Puede quitar la asignación de una política de calidad de servicio de un volumen, o bien seleccionar otra política de calidad de servicio o personalizar la calidad de servicio.

Lo que necesitará

El volumen que desea modificar es **asignado** Una política de calidad de servicio.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Haga clic en el menú **acciones** situado junto al volumen que desea modificar.
5. En el menú que se abre, seleccione **Editar**.
6. En el cuadro de diálogo, realice una de las siguientes acciones:

- Desactive **asignar directiva de QoS** y modifique los valores **Min IOPS**, **Max IOPS** y **Burst IOPS** para la QoS de volumen individual.



Cuando se deshabilitan las políticas de calidad de servicio, el volumen utiliza valores de IOPS de calidad de servicio predeterminados, a menos que se modifiquen de otro modo.

- Seleccione una política de calidad de servicio diferente de la lista desplegable que desee aplicar al volumen seleccionado.

7. Haga clic en **Guardar**.

El volumen actualizado se muestra en la página Overview.

Edite una política de calidad de servicio

Una política de calidad de servicio existente se puede cambiar, o bien se pueden editar los valores asociados con esta. Los cambios en los valores de rendimiento de las políticas de calidad de servicio afectan a la calidad de servicio de todos los volúmenes asociados con la política.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Haga clic en la ficha **Directivas de QoS**.
5. Haga clic en el menú **acciones** situado junto a la directiva QoS que desea modificar.
6. Haga clic en **Editar**.
7. En el cuadro de diálogo **Editar directiva de QoS**, cambie una o más de las siguientes opciones:
 - **Nombre:** El nombre definido por el usuario para la directiva QoS.
 - **Min IOPS:** El número mínimo de IOPS garantizado para el volumen. El valor predeterminado es de 15 50.
 - **Max IOPS:** El número máximo de IOPS permitido para el volumen. El valor predeterminado es de 15 15,000.
 - **Burst IOPS:** El número máximo de IOPS permitido durante un breve período de tiempo para el volumen. El valor predeterminado es de 15 15,000.
8. Haga clic en **Guardar**.

La política de calidad de servicio actualizada se muestra en la página QoS Políticas.



Puede hacer clic en el enlace de la columna **volúmenes activos** de una directiva para mostrar una lista filtrada de los volúmenes asignados a esa directiva.

Elimine una política de calidad de servicio

Puede eliminar una política de calidad de servicio si ya no es necesaria. Cuando se elimina una política de calidad de servicio, todos los volúmenes asignados con la política se conservan los valores de calidad de servicio definidos previamente por la política, pero como calidad de servicio de un volumen individual. Se eliminará cualquier asociación con la política de calidad de servicio eliminada.

Pasos

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En Dashboard de, expanda el menú para su clúster de almacenamiento.
3. Seleccione **almacenamiento > volúmenes**.
4. Haga clic en la ficha **Directivas de QoS**.
5. Haga clic en el menú **acciones** situado junto a la directiva QoS que desea modificar.
6. Haga clic en **Eliminar**.
7. Confirme la acción.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Documentación de SolidFire y el software Element"](#)

Trabaje con el nodo de gestión

Información general sobre los nodos de gestión

Es posible usar el nodo de gestión (mNode) para usar los servicios del sistema, gestionar los activos y las configuraciones del clúster, ejecutar pruebas y utilidades del sistema, configurar Active IQ para la supervisión del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas.



Como práctica recomendada, solo asocie un nodo de gestión a una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de gestión.

En los clústeres que ejecutan el software Element versión 11.3 o posterior, se puede trabajar con el nodo de gestión mediante una de las dos interfaces:

- Con la interfaz de usuario del nodo de gestión ([https://\[mNode IP\]:442](https://[mNode IP]:442)), puede realizar cambios en la configuración de la red y del clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.
- Con la interfaz de usuario de API de REST integrada ([https://\[mNode IP\]/mnode](https://[mNode IP]/mnode)), puede ejecutar o comprender las API relacionadas con los servicios del nodo de administración, incluida la configuración del servidor proxy, las actualizaciones de nivel de servicio o la administración de activos.

Instale o recupere un nodo de gestión:

- ["Instale un nodo de gestión"](#)
- ["Configurar una controladora de interfaz de red \(NIC\) de almacenamiento"](#)
- ["Recupere un nodo de gestión"](#)

Acceda al nodo de gestión:

- ["Acceder al nodo de gestión \(interfaz de usuario o API de REST\)"](#)

Cambie el certificado SSL predeterminado:

- ["Cambie el certificado SSL predeterminado del nodo de gestión"](#)

Realice tareas con la interfaz de usuario del nodo de gestión:

- ["Información general de la interfaz de usuario del nodo de gestión"](#)

Realice tareas con las API DE REST del nodo de gestión:

- ["Información general de la interfaz de usuario de la API DE REST del nodo de"](#)

Deshabilite o habilite la funcionalidad SSH remota o inicie una sesión de túnel de soporte remoto con el soporte de NetApp para ayudarle a resolver problemas:

- ["Habilite las conexiones remotas de soporte de NetApp"](#)
- ["Gestione la funcionalidad SSH en el nodo de gestión"](#)

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Instale o recupere un nodo de gestión

Instale un nodo de gestión

Puede instalar manualmente el nodo de gestión para el clúster que ejecuta el software NetApp Element con la imagen adecuada de su configuración.

Este proceso manual está dirigido a los administradores de NetApp HCI que no utilizan el motor de implementación de NetApp para la instalación de nodos de gestión.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- En la instalación utiliza IPv4. El nodo de gestión 11.3 no admite IPv6.



Si necesita compatibilidad con IPv6, se puede usar el nodo de gestión 11.1.

- Tiene permiso para descargar software del sitio de soporte de NetApp.
- Identificó el tipo de imagen del nodo de gestión correcto para su plataforma:

Plataforma	Tipo de imagen de instalación
Microsoft Hyper-V	.iso
KVM	.iso
VSphere de VMware	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Nodo de gestión 12.0 y posterior con servidor proxy) ha actualizado el control de cloud híbrido de NetApp a los servicios de gestión versión 2.16 antes de configurar un servidor proxy.

Acerca de esta tarea

El nodo de gestión Element 12.2 es una actualización opcional. No es necesario para las puestas en marcha existentes.

Antes de seguir este procedimiento, debe tener conocimientos de ["volúmenes persistentes"](#) y si desea usarlos o no. Los volúmenes persistentes son opcionales, pero se recomienda para la recuperación de datos de configuración del nodo de gestión en caso de pérdida de una máquina virtual.

Pasos

1. [Descargue ISO o OVA e implemente la VM](#)

2. [Cree el administrador del nodo de gestión y configure la red](#)
3. [Configurar la sincronización de hora](#)
4. [Configure el nodo de gestión](#)
5. [Configurar activos de controladora](#)
6. [\(Solo NetApp HCI\) Configure los activos de nodos de computación](#)

Descargue ISO o OVA e implemente la VM

1. Descargue el OVA o ISO para su instalación desde "[NetApp HCI](#)" Página del sitio de soporte de NetApp:
 - a. Seleccione **Descargar la versión más reciente** y acepte el EULA.
 - b. Seleccione la imagen del nodo de gestión que desea descargar.
2. Si ha descargado el OVA, siga estos pasos:
 - a. Implemente el OVA.
 - b. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (por ejemplo, eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.
3. Si ha descargado la ISO, siga estos pasos:
 - a. Cree una nueva máquina virtual de 64 bits desde el hipervisor con la siguiente configuración:
 - Seis CPU virtuales
 - 24 GB DE MEMORIA RAM
 - Tipo de adaptador de almacenamiento definido en LSI Logic Parallel



El valor predeterminado para el nodo de gestión puede ser LSI Logic SAS. En la ventana **Nueva máquina virtual**, compruebe la configuración del adaptador de almacenamiento seleccionando **Personalizar hardware > hardware virtual**. Si es necesario, cambie LSI Logic SAS a **LSI Logic Parallel**.

- Disco virtual de 400 GB, thin provisioning
- Una interfaz de red virtual con acceso a Internet y acceso a la MVIP de almacenamiento.
- Una interfaz de red virtual con acceso de red de gestión al clúster de almacenamiento de. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.



No encienda la máquina virtual antes del paso que indique hacerlo más adelante en este procedimiento.

- b. Adjunte ISO a la máquina virtual y arranque en la imagen de instalación .iso.



La instalación de un nodo de gestión con la imagen puede provocar un retraso de 30 segundos antes de que aparezca la pantalla de inicio.

4. Encienda la máquina virtual del nodo de gestión cuando se complete la instalación.

Cree el administrador del nodo de gestión y configure la red

1. Con la interfaz de usuario de terminal (TUI), cree un usuario administrador del nodo de gestión.



Para desplazarse por las opciones del menú, pulse las teclas de flecha hacia arriba o hacia abajo. Para desplazarse por los botones, pulse TAB. Para pasar de los botones a los campos, pulse TAB. Para desplazarse por los campos, pulse las teclas de flecha hacia arriba o hacia abajo.

2. Configure la red del nodo de gestión (eth0).



Si necesita una NIC adicional para aislar el tráfico de almacenamiento, consulte las instrucciones para configurar otra NIC: ["Configurar una controladora de interfaz de red \(NIC\) de almacenamiento"](#).

Configurar la sincronización de hora

1. Asegúrese de que la hora se haya sincronizado entre el nodo de gestión y el clúster de almacenamiento mediante NTP:



A partir del elemento 12.3.1, los subpasos (a) a (e) se realizan automáticamente. Para el nodo de gestión 12.3.1, vaya a [subpaso \(f\)](#) para completar la configuración de sincronización de tiempo.

- a. Inicie sesión en el nodo de gestión mediante SSH o la consola proporcionada por su hipervisor.
- b. Stop NTPD:

```
sudo service ntpd stop
```

- c. Edite el archivo de configuración NTP `/etc/ntp.conf`:
 - i. Comente los servidores predeterminados (`server 0.gentoo.pool.ntp.org`) agregando una `#` delante de cada uno.
 - ii. Agregue una nueva línea para cada servidor de tiempo predeterminado que desee agregar. Los servidores de hora predeterminados deben ser los mismos servidores NTP que se utilicen en el clúster de almacenamiento que se utilizará en un ["paso posterior"](#).

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time
server>
```

- iii. Guarde el archivo de configuración cuando finalice.

- d. Force una sincronización NTP con el servidor que se acaba de añadir.

```
sudo ntpd -gq
```

- e. Reinicie NTPD.

```
sudo service ntpd start
```

- f. Deshabilitar la sincronización de hora con el host a través del hipervisor (el siguiente es un ejemplo de VMware):



Si implementa el mNode en un entorno de hipervisor distinto a VMware, por ejemplo, desde la imagen .iso en un entorno de OpenStack, consulte la documentación del hipervisor para obtener los comandos equivalentes.

- i. Desactivar la sincronización periódica:

```
vmware-toolbox-cmd timesync disable
```

- ii. Mostrar y confirmar el estado actual del servicio:

```
vmware-toolbox-cmd timesync status
```

- iii. En vSphere, compruebe que el `Synchronize guest time with host` La casilla no está activada en las opciones de la máquina virtual.



No habilite esta opción si realiza cambios futuros en la máquina virtual.



No edite el NTP después de completar la configuración de sincronización de hora porque afecta al NTP cuando ejecuta el "comando setup" en el nodo de gestión.

Configure el nodo de gestión

1. Configure y ejecute el comando de configuración del nodo de gestión:



Se le pedirá que introduzca contraseñas en un mensaje seguro. Si su clúster de está situado detrás de un servidor proxy, debe configurar el proxy de manera que pueda llegar a una red pública.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

a. Sustituya el valor entre corchetes [] (incluidos los corchetes) para cada uno de los siguientes parámetros necesarios:



La forma abreviada del nombre del comando está entre paréntesis () y se puede sustituir por el nombre completo.

- **--mnode_admin_user (-mu) [username]:** El nombre de usuario de la cuenta de administrador del nodo de gestión. Probablemente este sea el nombre de usuario de la cuenta de usuario que utilizó para iniciar sesión en el nodo de gestión.
- **--Storage_mvip (-sm) [dirección MVIP]:** La dirección IP virtual de gestión (MVIP) del clúster de almacenamiento que ejecuta el software Element. Configure el nodo de gestión con el mismo clúster de almacenamiento que utilizó durante "[Configuración de servidores NTP](#)".
- **--Storage_username (-su) [nombre de usuario]:** El nombre de usuario administrador del clúster de almacenamiento para el clúster especificado por `--storage_mvip` parámetro.
- **--Telemetry_active (-t) [true]:** Conserve el valor true que permite la recopilación de datos para análisis por Active IQ.

b. (Opcional): Añada los parámetros de extremo de Active IQ al comando:

- **--remote_host (-rh) [AIQ_endpoint]:** El punto final donde se envían los datos de telemetría Active IQ para ser procesados. Si no se incluye el parámetro, se utiliza el extremo predeterminado.

c. (Recomendado): Añada los siguientes parámetros de volumen persistente. No modifique ni elimine la cuenta y los volúmenes creados para la funcionalidad de volúmenes persistentes o se producirá una pérdida en la funcionalidad de gestión.

- **--use_persistent_Volumes (-pv) [true/false, default: False]:** Enable o disable volúmenes persistentes. Introduzca el valor en true para habilitar la funcionalidad de volúmenes persistentes.
- **--persistent_Volumes_account (-pva) [account_name]:** If `--use_persistent_volumes` está configurado en true, use este parámetro e introduzca el nombre de la cuenta de almacenamiento que se usará para los volúmenes persistentes.



Utilice un nombre de cuenta único para volúmenes persistentes que sean diferentes del nombre de cuenta existente en el clúster. Es de vital importancia mantener la cuenta de los volúmenes persistentes separados del resto del entorno.

- **--persistent_Volumes_mvip (-pvm) [mvip]:** Introduzca la dirección IP virtual de gestión (MVIP) del clúster de almacenamiento que ejecuta el software Element que se usará con volúmenes persistentes. Esto solo es necesario si el nodo de gestión gestiona varios clústeres de almacenamiento. Si no se gestionan varios clústeres, se utiliza la dirección MVIP del clúster predeterminada.

d. Configure un servidor proxy:

- **--use_proxy (-up) [true/false, default: False]:** Activa o desactiva el uso del proxy. Este parámetro es necesario para configurar un servidor proxy.
- **--proxy_hostname_or_ip (-pi) [host]:** El nombre de host del proxy o IP. Esto es necesario si desea utilizar un proxy. Si lo especifica, se le solicitará que introduzca `--proxy_port`.
- **--proxy_username (-pu) [nombre de usuario]:** El nombre de usuario del proxy. Este parámetro es opcional.
- **--proxy_password (-pp) [password]:** La contraseña del proxy. Este parámetro es opcional.
- **--proxy_Port (-pq) [puerto, por defecto: 0]:** El puerto proxy. Si especifica esto, se le pedirá que

introduzca el nombre de host del proxy o la dirección IP (`--proxy_hostname_or_ip`).

- **--proxy_ssh_Port (-ps) [puerto, por defecto: 443]**: El puerto proxy SSH. De forma predeterminada, se establece el puerto 443.
- e. (Opcional) Use `Parameter help` si necesita información adicional acerca de cada parámetro:
- **--help (-h)**: Devuelve información acerca de cada parámetro. Los parámetros se definen como obligatorios u opcionales según la puesta en marcha inicial. Los requisitos de los parámetros de actualización y nueva puesta en marcha pueden variar.
- f. Ejecute el `setup-mnode` comando.

Configurar activos de controladora

1. Busque el ID de instalación:

- a. Desde un explorador, inicie sesión en la API DE REST del nodo de gestión:
- b. Vaya a la MVIP de almacenamiento e inicie sesión. Esta acción hace que se acepte el certificado para el siguiente paso.
- c. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

d. Seleccione **autorizar** y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
- ii. Introduzca el ID de cliente as `mnode-client`.
- iii. Seleccione **autorizar** para iniciar una sesión.

e. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.

f. Seleccione **probar**.

g. Seleccione **Ejecutar**.

h. Desde el cuerpo de respuesta del código 200, copie y guarde `id` para la instalación para utilizar en un paso posterior.

Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

2. (Solo NetApp HCI) Busque la etiqueta de hardware del nodo de computación en vSphere:

- a. Seleccione el host en el navegador vSphere Web Client.
- b. Seleccione la ficha **Monitor** y seleccione **Estado del hardware**.
- c. Se muestran el fabricante del BIOS del nodo y el número de modelo. Copie y guarde el valor para `tag` para su uso en un paso posterior.

3. Añada un activo de controladora de vCenter para la supervisión de NetApp HCI (solo instalaciones NetApp HCI) y el control del cloud híbrido (para todas las instalaciones) a los activos conocidos del nodo de gestión:

- a. Acceda a la interfaz de usuario de API de servicio `mnode` en el nodo de gestión introduciendo la dirección IP del nodo de gestión seguida de `/mnode`:


```
https://<ManagementNodeIP>/mnode
```

- b. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana.
- c. Seleccione **POST /assets/{Asset_id}/controllers** para agregar un subactivo de controlador.



Debe crear un nuevo rol HCC de NetApp en vCenter para añadir un subsistema de controladora. Este nuevo rol de HCC de NetApp limitará la visión de los servicios de los nodos de gestión a activos de NetApp. Consulte "[Cree una función HCC de NetApp en vCenter](#)".

- d. Seleccione **probar**.
- e. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
- f. Introduzca los valores de carga útil necesarios con el tipo `vCenter De aplicaciones y vCenter`.
- g. Seleccione **Ejecutar**.

(Solo NetApp HCI) Configure los activos de nodos de computación

1. (Solo para NetApp HCI) Añada un activo de nodo de computación a los activos conocidos del nodo de gestión:
 - a. Seleccione **POST /assets/{Asset_id}/Compute-Nodes** para agregar un subactivo de nodo de computación con credenciales para el activo de nodo de computación.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
 - d. En la carga útil, introduzca los valores de carga útil necesarios tal y como se definen en la ficha Modelo . Introduzca `ESXi Host` como `type` e introduzca la etiqueta de hardware guardada durante un paso anterior para `hardware_tag`.
 - e. Seleccione **Ejecutar**.

Obtenga más información

- "[Volúmenes persistentes](#)"
- "[Añada activos de computación y de controladora al nodo de gestión](#)"
- "[Configurar un NIC de almacenamiento](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"
- "[Página de recursos de NetApp HCI](#)"

Configurar una controladora de interfaz de red (NIC) de almacenamiento

Si utiliza una NIC adicional para almacenamiento, puede conectarse SSH al nodo de

gestión o usar la consola de vCenter y ejecutar un comando curl para configurar una interfaz de red etiquetada o sin etiqueta.

Antes de empezar

- Conoce la dirección IP eth0.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Implementó un nodo de gestión 11.3 o posterior.

Opciones de configuración

Elija la opción relevante para su entorno:

- [Configure un controlador de interfaz de red \(NIC\) de almacenamiento para una interfaz de red sin etiquetas](#)
- [Configure un controlador de interfaz de red \(NIC\) de almacenamiento para una interfaz de red etiquetada](#)

Configure un controlador de interfaz de red (NIC) de almacenamiento para una interfaz de red sin etiquetas

Pasos

1. Abra una consola SSH o vCenter.
2. Sustituya los valores de la siguiente plantilla de comandos y ejecute el comando:



Los valores se representan mediante \$ para cada uno de los parámetros necesarios para la nueva interfaz de red de almacenamiento. La `cluster` es necesario y se puede utilizar para cambiar el nombre del host del nodo de gestión en la siguiente plantilla. `--insecure` o `-k` las opciones no se deben utilizar en entornos de producción.

```

curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
    "params": {
        "network": {
            "$eth1": {
                "#default" : false,
                "address" : "$storage_IP",
                "auto" : true,
                "family" : "inet",
                "method" : "static",
                "mtu" : "9000",
                "netmask" : "$subnet_mask",
                "status" : "Up"
            }
        },
        "cluster": {
            "name": "$mnode_host_name"
        }
    },
    "method": "SetConfig"
}
'

```

Configure un controlador de interfaz de red (NIC) de almacenamiento para una interfaz de red etiquetada

Pasos

1. Abra una consola SSH o vCenter.
2. Sustituya los valores de la siguiente plantilla de comandos y ejecute el comando:



Los valores se representan mediante \$ para cada uno de los parámetros necesarios para la nueva interfaz de red de almacenamiento. La `cluster` es necesario y se puede utilizar para cambiar el nombre del host del nodo de gestión en la siguiente plantilla. `--insecure` o `-k` las opciones no se deben utilizar en entornos de producción.

```

curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
    "params": {
        "network": {
            "$eth1": {
                "#default" : false,
                "address" : "$storage_IP",
                "auto" : true,
                "family" : "inet",
                "method" : "static",
                "mtu" : "9000",
                "netmask" : "$subnet_mask",
                "status" : "Up",
                "virtualNetworkTag" : "$vlan_id"
            }
        },
        "cluster": {
            "name": "$mnode_host_name",
            "cipi": "$eth1.$vlan_id",
            "sipi": "$eth1.$vlan_id"
        }
    },
    "method": "SetConfig"
}
'

```

Obtenga más información

- ["Añada activos de computación y de controladora al nodo de gestión"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Recupere un nodo de gestión

Puede recuperar y volver a poner en marcha manualmente el nodo de gestión para el clúster que ejecuta el software NetApp Element si el nodo de gestión anterior usaba volúmenes persistentes.

Es posible implementar un nuevo OVA y ejecutar un script de nueva puesta en marcha para extraer datos de configuración de un nodo de gestión previamente instalado que ejecuta la versión 11.3 y posteriores.

Lo que necesitará

- El nodo de gestión anterior ejecutaba la versión 11.3 o posterior del software NetApp Element con "volúmenes persistentes" funcionalidad activada.
- Conoce la dirección MVIP y la SVIP del clúster que contiene los volúmenes persistentes.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- En la instalación utiliza IPv4. El nodo de gestión 11.3 no admite IPv6.
- Tiene permiso para descargar software del sitio de soporte de NetApp.
- Identificó el tipo de imagen del nodo de gestión correcto para su plataforma:

Plataforma	Tipo de imagen de instalación
Microsoft Hyper-V	.iso
KVM	.iso
VSphere de VMware	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Pasos

1. [Descargue ISO o OVA e implemente la VM](#)
2. [Configure la red](#)
3. [Configurar la sincronización de hora](#)
4. [Configure el nodo de gestión](#)

Descargue ISO o OVA e implemente la VM

1. Descargue el OVA o ISO para su instalación desde "[NetApp HCI](#)" Página del sitio de soporte de NetApp:
 - a. Haga clic en **Descargar la versión más reciente** y acepte el EULA.
 - b. Seleccione la imagen del nodo de gestión que desea descargar.
2. Si ha descargado el OVA, siga estos pasos:
 - a. Implemente el OVA.
 - b. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a la máquina virtual en la subred de almacenamiento (por ejemplo, eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.
3. Si ha descargado la ISO, siga estos pasos:
 - a. Cree una nueva máquina virtual de 64 bits desde el hipervisor con la siguiente configuración:
 - Seis CPU virtuales
 - 24 GB DE MEMORIA RAM
 - Disco virtual de 400 GB, thin provisioning
 - Una interfaz de red virtual con acceso a Internet y acceso a la MVIP de almacenamiento.
 - Una interfaz de red virtual con acceso de red de gestión al clúster de almacenamiento de. Si el clúster de almacenamiento se encuentra en una subred separada de su nodo de gestión (eth0) y desea utilizar volúmenes persistentes, añada una segunda controladora de interfaz de red (NIC) a

la máquina virtual en la subred de almacenamiento (eth1) o asegúrese de que la red de gestión pueda enrutar a la red de almacenamiento.



No encienda la máquina virtual antes del paso que indique hacerlo más adelante en este procedimiento.

b. Adjunte ISO a la máquina virtual y arranque en la imagen de instalación .iso.



La instalación de un nodo de gestión con la imagen puede provocar un retraso de 30 segundos antes de que aparezca la pantalla de inicio.

4. Encienda la máquina virtual del nodo de gestión cuando se complete la instalación.

Configure la red

1. Con la interfaz de usuario de terminal (TUI), cree un usuario administrador del nodo de gestión.



Para desplazarse por las opciones del menú, pulse las teclas de flecha hacia arriba o hacia abajo. Para desplazarse por los botones, pulse TAB. Para pasar de los botones a los campos, pulse TAB. Para desplazarse por los campos, pulse las teclas de flecha hacia arriba o hacia abajo.

2. Configure la red del nodo de gestión (eth0).



Si necesita una NIC adicional para aislar el tráfico de almacenamiento, consulte las instrucciones para configurar otra NIC: "[Configurar una controladora de interfaz de red \(NIC\) de almacenamiento](#)".

Configurar la sincronización de hora

1. Asegúrese de que la hora se haya sincronizado entre el nodo de gestión y el clúster de almacenamiento mediante NTP:



A partir del elemento 12.3.1, los subpasos (a) a (e) se realizan automáticamente. Para el nodo de gestión 12.3.1, vaya a [subpaso \(f\)](#) para completar la configuración de sincronización de tiempo.

1. Inicie sesión en el nodo de gestión mediante SSH o la consola proporcionada por su hipervisor.

2. Stop NTPD:

```
sudo service ntpd stop
```

3. Edite el archivo de configuración NTP `/etc/ntp.conf`:

- Comente los servidores predeterminados (`server 0.gentoo.pool.ntp.org`) agregando una `#` delante de cada uno.
- Agregue una nueva línea para cada servidor de tiempo predeterminado que desee agregar. Los servidores de hora predeterminados deben ser los mismos servidores NTP que se utilicen en el clúster de almacenamiento que se utilizará en un ["paso posterior"](#).

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Guarde el archivo de configuración cuando finalice.

4. Fuerce una sincronización NTP con el servidor que se acaba de añadir.

```
sudo ntpd -gq
```

5. Reinicie NTPD.

```
sudo service ntpd start
```

6. Deshabilitar la sincronización de hora con el host a través del hipervisor (el siguiente es un ejemplo de VMware):



Si implementa el mNode en un entorno de hipervisor distinto a VMware, por ejemplo, desde la imagen .iso en un entorno de OpenStack, consulte la documentación del hipervisor para obtener los comandos equivalentes.

a. Desactivar la sincronización periódica:

```
vmware-toolbox-cmd timesync disable
```

b. Mostrar y confirmar el estado actual del servicio:

```
vmware-toolbox-cmd timesync status
```

c. En vSphere, compruebe que el `Synchronize guest time with host` La casilla no está activada en las opciones de la máquina virtual.



No habilite esta opción si realiza cambios futuros en la máquina virtual.



No edite el NTP después de completar la configuración de sincronización de hora porque afecta al NTP cuando ejecuta el [comando re-deploy](#) en el nodo de gestión.

Configure el nodo de gestión

1. Cree un directorio de destino temporal para el contenido del paquete de servicios de gestión:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Descargue el paquete de servicios de gestión (versión 2.15.28 o posterior) que se instaló anteriormente en el nodo de gestión existente y guárdelo en el `/sf/etc/mnode/` directorio.
3. Extraiga el paquete descargado con el siguiente comando, reemplazando el valor entre corchetes [] (incluidos los paréntesis) por el nombre del archivo de paquete:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

4. Extraiga el archivo resultante en la `/sf/etc/mnode-archive` directorio:

```
tar -C /sf/etc/mnode/mnode-archive -xvf /sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Crear un archivo de configuración para cuentas y volúmenes:

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name": "[persistent volume account name]}' | sudo tee /sf/etc/mnode/mnode-archive/management-services-metadata.json
```

- a. Sustituya el valor entre corchetes [] (incluidos los corchetes) para cada uno de los siguientes parámetros necesarios:

- **[mvip IP address]:** La dirección IP virtual de administración del clúster de almacenamiento. Configure el nodo de gestión con el mismo clúster de almacenamiento que utilizó durante ["Configuración de servidores NTP"](#).
- **[nombre de cuenta de volumen persistente]:** Nombre de la cuenta asociada a todos los volúmenes persistentes en este clúster de almacenamiento.

6. Configure y ejecute el comando de nueva puesta en marcha del nodo de gestión para conectarse a los volúmenes persistentes alojados en el clúster e inicie servicios con datos de configuración de nodos de gestión anteriores:



Se le pedirá que introduzca contraseñas en un mensaje seguro. Si su clúster de está situado detrás de un servidor proxy, debe configurar el proxy de manera que pueda llegar a una red pública.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```


- a. Sustituya el valor entre corchetes [] (incluidos los corchetes) por el nombre de usuario de la cuenta de administrador del nodo de gestión. Probablemente este sea el nombre de usuario de la cuenta de usuario que utilizó para iniciar sesión en el nodo de gestión.



Puede agregar el nombre de usuario o permitir que la secuencia de comandos le solicite la información.

- b. Ejecute el `redeploy-mnode` comando. El script muestra un mensaje de éxito una vez que se ha completado la reimplantación.
- c. Si accede a las interfaces web de Element o NetApp HCI (como el nodo de gestión o Hybrid Cloud Control de NetApp) mediante el nombre de dominio completamente cualificado (FQDN) del sistema, "[volver a configurar la autenticación del nodo de gestión](#)".



Funcionalidad SSH que proporciona "[Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support](#)" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 y posteriores. Si ya había habilitado la funcionalidad SSH en el nodo de gestión, es posible que deba hacerlo "[Vuelva a deshabilitar SSH](#)" en el nodo de gestión recuperado.

Obtenga más información

- "[Volúmenes persistentes](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"
- "[Página de recursos de NetApp HCI](#)"

Acceda al nodo de gestión

A partir de la versión 11.3 del software NetApp Element, el nodo de gestión contiene dos interfaces de usuario: Una interfaz de usuario para gestionar los servicios basados en REST y una interfaz de usuario por nodo para gestionar la configuración de red y de clúster, así como las pruebas y utilidades del sistema operativo.

Para los clústeres que ejecutan el software Element de la versión 11.3 o posterior, es posible usar una de dos interfaces:

- Con la interfaz de usuario del nodo de gestión (`https:// [mNode IP]:442`), puede realizar cambios en la configuración de la red y del clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.
- Mediante el uso de la interfaz de usuario de API de REST integrada (`https:// [mNode IP]/mnode`), puede ejecutar o comprender las API relacionadas con los servicios del nodo de administración, incluida la configuración del servidor proxy, las actualizaciones de nivel de servicio o la administración de activos.

Acceda a la interfaz de usuario de cada nodo de gestión

Desde la interfaz de usuario por nodo, puede acceder a la configuración de red y clúster y utilizar las pruebas y las utilidades del sistema.

Pasos

1. Para acceder a la interfaz de usuario por nodo de gestión, introduzca la dirección IP del nodo de gestión seguida de `:442`

```
https://[IP address]:442
```

Support and Documentation Enable Debug Info: Requests Responses Logout

NetApp

Network Settings Cluster Settings System Tests System Utilities

Management

Network Settings - Management

Method: static

Link Speed: 1000

IPv4 Address: 10.117.148.201

IPv4 Subnet Mask: 255.255.248.0

IPv4 Gateway Address: 10.117.131.254

IPv6 Address:

IPv6 Gateway Address:

MTU: 1500

DNS Servers: 10.117.20.40, 10.116.133.40

Search Domains: den.scoloffre.net, ora.den.scoloffre

Status: UpAndRunning

Routes

+ Add

Reset Changes Save Changes

2. Introduzca el nombre de usuario y la contraseña del nodo de gestión cuando se le solicite.

Acceda a la interfaz de usuario de API DE REST del nodo de gestión

Desde la interfaz de usuario de la API DE REST, puede acceder a un menú de API relacionadas con el servicio que controlan los servicios de gestión en el nodo de gestión.

Pasos

1. Para acceder a la interfaz de usuario de la API DE REST para los servicios de gestión, introduzca la dirección IP del nodo de gestión seguida de /mnode:

```
https://[IP address]/mnode
```

MANAGEMENT SERVICES API^{1.0}

[Base URL: /mnode]
https://10.117.1.10/mnode/swagger/json

The configuration REST service for MANAGEMENT SERVICES

NetApp - Website

NetApp Commercial Software License

Authorize 

logs Log service

GET /logs Get logs from the MNODE service(s)

assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute_node_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage_cluster_id} Get a specific storage cluster by ID

PUT /assets/{asset_id} Modify an asset with a specific ID

DELETE /assets/{asset_id} Delete an asset with a specific ID

GET /assets/{asset_id} Get an asset by it's ID

POST /assets/{asset_id}/compute-nodes Add a compute asset

GET /assets/{asset_id}/compute-nodes Get compute assets

PUT /assets/{asset_id}/compute-nodes/{compute_id} Update a specific compute node asset

DELETE /assets/{asset_id}/compute-nodes/{compute_id} Delete a specific compute node asset

2. Haga clic en **autorizar** o en cualquier icono de bloqueo e introduzca las credenciales de administración del clúster para los permisos de uso de las API.

Obtenga más información

- ["Habilite la supervisión de Active IQ y NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Cambie el certificado SSL predeterminado del nodo de gestión

Es posible cambiar el certificado SSL predeterminado y la clave privada del nodo de gestión mediante la API de NetApp Element.

Cuando se configura un nodo de gestión, crea un certificado único de capa de sockets seguros (SSL) con firma automática y una clave privada que se utiliza para todas las comunicaciones HTTPS mediante la interfaz de usuario de Element, la interfaz de usuario por nodo o las API. El software Element admite certificados

autofirmados, así como certificados que una entidad de certificación (CA) de confianza emite y verifica.

Puede utilizar los siguientes métodos API para obtener más información sobre el certificado SSL predeterminado y realizar cambios.

- **GetNodeSSLCertificate**

Puede utilizar el "[Método GetNodeSSLCertificate](#)" Para recuperar información acerca del certificado SSL instalado actualmente, incluidos todos los detalles del certificado.

- **SetNodeSSLCertificate**

Puede utilizar el "[Método SetNodeSSLCertificate](#)" Para establecer los certificados SSL por clúster y por nodo en el certificado y la clave privada que suministre. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

- **RemoveNodeSSLCertificate**

Este "[Método RemoveNodeSSLCertificate](#)" Quita el certificado SSL y la clave privada instalados actualmente. A continuación, el clúster genera un nuevo certificado autofirmado y una clave privada.

Obtenga más información

- "[Cambie el certificado SSL predeterminado del software Element](#)"
- "[¿Cuáles son los requisitos para configurar certificados SSL personalizados en el software Element?](#)"
- "[Documentación de SolidFire y el software Element](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"

Trabaje con la interfaz de usuario del nodo de gestión

Información general de la interfaz de usuario del nodo de gestión

Con la interfaz de usuario del nodo de gestión (<https://<mNodeIP>:442>), puede realizar cambios en la configuración de la red y del clúster, ejecutar pruebas del sistema o utilizar utilidades del sistema.

Tareas que se pueden realizar con la interfaz de usuario del nodo de gestión:

- "[Configure la supervisión de alertas en NetApp HCI](#)"
- "[Modifique y pruebe la red, el clúster y la configuración del sistema de los nodos de gestión](#)"
- "[Ejecute las utilidades del sistema desde el nodo de gestión](#)"

Obtenga más información

- "[Acceda al nodo de gestión](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"
- "[Página de recursos de NetApp HCI](#)"

Configure la supervisión de alertas en NetApp HCI



Puede configurar los ajustes para supervisar las alertas en el sistema NetApp HCI.

La supervisión de alertas de NetApp HCI reenvía las alertas del sistema de clúster de almacenamiento de NetApp HCI a vCenter Server, lo que permite ver todas las alertas de NetApp HCI desde la interfaz de vSphere Web Client.

1. Abra la interfaz de usuario de cada nodo de gestión ([https://\[IP address\]:442](https://[IP address]:442)).
2. Haga clic en la ficha **Monitor de alerta**.
3. Configure las opciones de supervisión de alertas.

Opciones de supervisión de alertas

opciones	Descripción
Ejecutar pruebas de monitor de alerta	Ejecuta pruebas del sistema de supervisión para comprobar lo siguiente: <ul style="list-style-type: none">• Conectividad de NetApp HCI y VMware vCenter• Emparejamiento de NetApp HCI y VMware vCenter mediante información del almacén de datos suministrada por el servicio QoSSIOC• Listas actuales de alarmas de NetApp HCI y de vCenter
Recoger alertas	Habilita o deshabilita el reenvío de alarmas de almacenamiento de NetApp HCI a vCenter. El clúster de almacenamiento de destino se puede seleccionar en la lista desplegable. El valor predeterminado de esta opción es <code>Enabled</code> .
Recopilación de alertas de prácticas recomendadas	Habilita o deshabilita el reenvío de alertas de prácticas recomendadas de almacenamiento de NetApp HCI a vCenter. Las alertas de prácticas recomendadas son errores que se activan mediante una configuración del sistema que no es óptima. El valor predeterminado de esta opción es <code>Disabled</code> . Cuando se deshabilitan, las alertas de prácticas recomendadas de almacenamiento de NetApp HCI no aparecen en vCenter.

opciones	Descripción
Envíe datos de soporte a AIQ	<p>Controla el flujo de datos de soporte y supervisión de VMware vCenter a SolidFire Active IQ de NetApp.</p> <p>Las opciones son las siguientes:</p> <ul style="list-style-type: none"> • Enabled: Se envían todas las alarmas de vCenter, las alarmas de almacenamiento de NetApp HCI y los datos de soporte a SolidFire Active IQ de NetApp. Esto permite que NetApp respalde y supervise de forma proactiva la instalación de NetApp HCI a fin de detectar y resolver posibles problemas antes de que afecten el sistema. • Disabled: No se envía ninguna alarma de vCenter, alarma de almacenamiento de NetApp HCI ni dato de soporte a SolidFire Active IQ de NetApp. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Si desactiva la opción Enviar datos a AIQ mediante el motor de implementación de NetApp, debe hacerlo "habilite la telemetría" De nuevo a través de la API DE REST del nodo de gestión para configurar el servicio desde esta página.</p> </div>
Envíe datos del nodo de computación a AIQ	<p>Controla el flujo de datos de soporte y supervisión de los nodos de computación a SolidFire Active IQ de NetApp.</p> <p>Las opciones son las siguientes:</p> <ul style="list-style-type: none"> • Enabled: Se transmiten datos de soporte y supervisión acerca de los nodos de computación a SolidFire Active IQ de NetApp para permitir el soporte proactivo del hardware de los nodos de computación. • Disabled: No se transmiten datos de soporte y supervisión acerca de los nodos de computación a SolidFire Active IQ de NetApp. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Si desactiva la opción Enviar datos a AIQ mediante el motor de implementación de NetApp, debe hacerlo "habilite la telemetría" De nuevo a través de la API DE REST del nodo de gestión para configurar el servicio desde esta página.</p> </div>

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Modifique y pruebe la red, el clúster y la configuración del sistema de los nodos de gestión


Puede modificar y probar la red de los nodos de gestión, el clúster y la configuración del sistema.

- [Actualice la configuración de red del nodo de gestión](#)
- [Actualice la configuración del clúster del nodo de gestión](#)
- [Pruebe los ajustes del nodo de gestión](#)

Actualice la configuración de red del nodo de gestión

En la pestaña Network Settings de la interfaz de usuario de nodo de gestión por nodo, puede modificar los campos de la interfaz de red de los nodos de gestión.

1. Abra la interfaz de usuario de cada nodo de gestión.
2. Haga clic en la ficha **Configuración de red**.
3. Vea o introduzca la siguiente información:
 - a. **Método:** Elija uno de los siguientes métodos para configurar la interfaz:
 - `loopback`: Utilice para definir la interfaz de bucle invertido de IPv4.
 - `manual`: Se utiliza para definir interfaces para las que no se realiza ninguna configuración de forma predeterminada.
 - `dhcp`: Se utiliza para obtener una dirección IP a través de DHCP.
 - `static`: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.
 - b. **Velocidad de enlace:** La velocidad negociada por la NIC virtual.
 - c. **Dirección IPv4:** La dirección IPv4 de la red eth0.
 - d. **Máscara de subred IPv4:** Subdivisiones de dirección de la red IPv4.
 - e. **Dirección de puerta de enlace IPv4:** Dirección de red del router para enviar paquetes fuera de la red local.
 - f. **Dirección IPv6:** La dirección IPv6 de la red eth0.
 - g. **Dirección de puerta de enlace IPv6:** Dirección de red del enrutador para enviar paquetes fuera de la red local.



Las opciones IPv6 no son compatibles con las versiones 11.3 o posteriores del nodo de gestión.
 - h. **MTU:** Tamaño de paquete más grande que un protocolo de red puede transmitir. Debe ser mayor o igual que 1500. Si se añade un segundo NIC de almacenamiento, el valor debería ser 9000.
 - i. **Servidores DNS:** Interfaz de red utilizada para la comunicación de clústeres.
 - j. **Buscar dominios:** Busque direcciones MAC adicionales disponibles para el sistema.
 - k. **Estado:** Valores posibles:
 - `UpAndRunning`

- Down
- Up

I. **Rutas:** Rutas estáticas a hosts o redes específicos a través de la interfaz asociada que las rutas están configuradas para utilizar.

Actualice la configuración del clúster del nodo de gestión

En la pestaña Cluster Settings de la interfaz de usuario por nodo para la gestión de los nodos, los campos de la interfaz de clúster se pueden modificar cuando un nodo está en el estado Available, Pending, PendingActive y Active.

1. Abra la interfaz de usuario de cada nodo de gestión.
2. Haga clic en la ficha **Configuración de clúster**.
3. Vea o introduzca la siguiente información:
 - **Rol:** Función que tiene el nodo de administración en el clúster. El posible valor es: Management.
 - **Versión:** Versión del software Element que se ejecuta en el cluster.
 - **Interfaz predeterminada:** Interfaz de red predeterminada utilizada para la comunicación del nodo de administración con el clúster que ejecuta el software Element.

Pruebe los ajustes del nodo de gestión

Después de cambiar la configuración de red y de gestión del nodo de gestión y confirmar los cambios, puede ejecutar pruebas para validar los cambios realizados.

1. Abra la interfaz de usuario de cada nodo de gestión.
2. En la interfaz de usuario del nodo de gestión, haga clic en **pruebas del sistema**.
3. Realice alguna de las siguientes acciones:
 - a. Para comprobar que la configuración de red configurada es válida para el sistema, haga clic en **probar configuración de red**.
 - b. Para probar la conectividad de red a todos los nodos del clúster en las interfaces 1G y 10G mediante paquetes ICMP, haga clic en **probar ping**.
4. Vea o introduzca lo siguiente:
 - **Hosts:** Especifique una lista separada por comas de direcciones o nombres de host de los dispositivos que se van a hacer ping.
 - **Intentos:** Especifique el número de veces que el sistema debe repetir la prueba ping. El valor predeterminado es 5.
 - **Tamaño de paquete:** Especifique el número de bytes que se enviarán en el paquete ICMP que se envía a cada IP. El número de bytes debe ser inferior al MTU máximo especificado en la configuración de red.
 - **Tiempo de espera msec:** Especifique el número de milisegundos que se deben esperar para cada respuesta de ping individual. Valor predeterminado: 500 ms.
 - **Tiempo de espera total Sec:** Especifique el tiempo en segundos que el ping debe esperar a una respuesta del sistema antes de emitir el siguiente intento de ping o de terminar el proceso. El valor predeterminado es 5.
 - **Prohibir fragmentación:** Activar el indicador DF (no fragmentar) para los paquetes ICMP.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Ejecute las utilidades del sistema desde el nodo de gestión

Se puede usar la interfaz de usuario por nodo para el nodo de gestión a fin de crear o eliminar paquetes de soporte de clústeres, restablecer la configuración de nodos o reiniciar las redes.

Pasos

1. Abra la interfaz de usuario de cada nodo de gestión con las credenciales de administrador del nodo de gestión.
2. Haga clic en **Utilidades del sistema**.
3. Haga clic en el botón de la utilidad que desea ejecutar:
 - a. **Potencia de control:** Reinicia, enciende o apaga el nodo. Especifique cualquiera de las siguientes opciones.



Esta operación provoca la pérdida temporal de conectividad de red.

- **Acción:** Las opciones incluyen `Restart` y `Halt` (apagado).
 - **Retardo de activación:** Cualquier tiempo adicional antes de que el nodo vuelva a estar en línea.
- b. **Crear paquete de soporte de clúster:** Crea el paquete de soporte de clúster para ayudar a las evaluaciones de diagnóstico del soporte de NetApp de uno o más nodos de un clúster. Especifique las siguientes opciones:
 - **Nombre del paquete:** Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, "supportBundle" y el nombre de nodo se utilizan como nombre de archivo.
 - **Mvip:** La MVIP del cluster. Los paquetes se agrupan en todos los nodos del clúster. Este parámetro es obligatorio si no se especifica el parámetro `Nodes`.
 - **Nodes:** Las direcciones IP de los nodos de los que se van a recopilar paquetes. Use nodos o `Mvip`, pero no ambos, para especificar los nodos a partir de los cuales se van a formar paquetes. Este parámetro es obligatorio si no se especifica `Mvip`.
 - **Nombre de usuario:** El nombre de usuario administrador del clúster.
 - **Contraseña:** La contraseña de administrador del clúster.
 - **Permitir incompleto:** Permite que la secuencia de comandos continúe ejecutándose si los paquetes no se pueden recopilar de uno o más de los nodos.
 - **Extra args:** Este parámetro se carga al `sf_make_support_bundle` guión. Este parámetro solo se debe usar si lo solicita el soporte de NetApp.
 - c. **Eliminar todos los paquetes de soporte:** Elimina los paquetes de soporte actuales del nodo de administración.
 - d. **Restablecer nodo:** Restablece el nodo de administración a una nueva imagen de instalación. Esto cambia todas las opciones, excepto la configuración de red al estado predeterminado. Especifique las siguientes opciones:
 - **Build:** La dirección URL de una imagen de software de elemento remoto a la que se restablecerá el nodo.

- **Opciones:** Especificaciones para ejecutar las operaciones de restablecimiento. El soporte de NetApp puede proporcionar detalles si es necesario.



Esta operación provoca la pérdida temporal de conectividad de red.

- e. **Reiniciar red:** Reinicia todos los servicios de red en el nodo de gestión.



Esta operación provoca la pérdida temporal de conectividad de red.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Trabaje con la API DE REST del nodo de gestión

Información general de la interfaz de usuario de la API DE REST del nodo de

Mediante el uso de la interfaz de usuario de API de REST integrada (<https://<ManagementNodeIP>/mnode>), puede ejecutar o comprender las API relacionadas con los servicios del nodo de administración, incluida la configuración del servidor proxy, las actualizaciones de nivel de servicio o la administración de activos.

Tareas que se pueden realizar con API de REST:

Autorización

- ["Obtenga autorización para utilizar las API de REST"](#)

Configuración de activos

- ["Habilite la supervisión de Active IQ y NetApp HCI"](#)
- ["Configure un servidor proxy para el nodo de gestión"](#)
- ["Configure Cloud Control de NetApp híbrido para varias instancias de vCenter"](#)
- ["Añada activos de computación y de controladora al nodo de gestión"](#)
- ["Crear y gestionar activos de clúster de almacenamiento"](#)

Gestión de activos

- ["Ver o editar activos de controladora existentes"](#)
- ["Crear y gestionar activos de clúster de almacenamiento"](#)
- ["Quite un activo del nodo de gestión"](#)
- ["Use la API DE REST para recoger registros de NetApp HCI"](#)
- ["Verifique el sistema operativo del nodo de gestión y las versiones de servicios"](#)
- ["Obtener registros de los servicios de gestión"](#)

Obtenga más información

- ["Acceda al nodo de gestión"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Obtenga autorización para utilizar las API de REST

Se debe autorizar para poder usar las API de para los servicios de gestión en la interfaz de usuario de la API de REST. Para ello, obtenga un token de acceso.

Para obtener un token, debe proporcionar credenciales de administrador del clúster y un ID de cliente. Cada ficha dura aproximadamente diez minutos. Después de que caduque un token, puede volver a autorizarse para un nuevo token de acceso.

La funcionalidad de autorización se configura durante la instalación y la puesta en marcha del nodo de gestión. El servicio de token se basa en el clúster de almacenamiento que haya definido durante la configuración.

Antes de empezar

- La versión del clúster debe ejecutar el software NetApp Element 11.3 o una versión posterior.
- Debe haber implementado un nodo de gestión que ejecute la versión 11.3 o posterior.

Comando API

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-client -F grant_type=password -F username=CLUSTER_ADMIN -F password=CLUSTER_PASSWORD|awk -F':' '{print $2}'|awk -F',' '{print $1}'|sed s/\"//g`
```

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Para acceder a la interfaz de usuario de API DE REST del servicio, introduzca la dirección IP del nodo de gestión seguida del nombre de servicio, por ejemplo /mnode/:

```
https://<ManagementNodeIP>/mnode/
```

2. Haga clic en **autorizar**.



Como alternativa, puede hacer clic en un icono de bloqueo situado junto a cualquier API de servicio.

3. Complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. No introduzca un valor para el secreto de cliente.
 - d. Haga clic en **autorizar** para iniciar una sesión.
4. Cierre el cuadro de diálogo **autorizaciones disponibles**.



Si intenta ejecutar un comando después de que caduque el token, a. 401 Error: UNAUTHORIZED aparece el mensaje. Si ve esto, vuelva a autorizar.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Habilite la supervisión de Active IQ y NetApp HCI

Puede habilitar la supervisión del almacenamiento de Active IQ para la supervisión de la computación NetApp HCI y NetApp HCI si aún no lo hizo durante la instalación o la actualización. Es posible que deba utilizar este procedimiento si deshabilitó la telemetría con el motor de puesta en marcha de NetApp HCI.

El servicio del recopilador Active IQ reenvía los datos de configuración y los indicadores de rendimiento del clúster basados en software Element a Active IQ de NetApp para realizar informes históricos y supervisar el rendimiento casi en tiempo real. El servicio de supervisión de NetApp HCI permite el reenvío de errores del clúster de almacenamiento a vCenter para notificaciones de alerta.

Antes de empezar

- El clúster de almacenamiento ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.
- Tienes acceso a Internet. El servicio de recopilador Active IQ no se puede utilizar de sitios oscuros que no tienen conectividad externa.

Pasos

1. Obtenga el ID de activo base para la instalación:
 - a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Haga clic en **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Haga clic en **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana.
- c. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /Installations**.
- d. Haga clic en **probar**.
- e. Haga clic en **Ejecutar**.
- f. Del cuerpo de respuesta del código 200, copie el `id` para la instalación.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

2. Activar telemetría:

- a. Acceda a la interfaz de usuario de API de servicio mnode en el nodo de gestión introduciendo la dirección IP del nodo de gestión seguida de /mnode:

```
https://<ManagementNodeIP>/mnode
```

- b. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
- ii. Introduzca el ID de cliente as `mnode-client`.
- iii. Haga clic en **autorizar** para iniciar una sesión.
- iv. Cierre la ventana.

- c. Configure el activo base:

- i. Haga clic en **PUT /assets/{asset_id}**.
- ii. Haga clic en **probar**.
- iii. Introduzca lo siguiente en la carga útil de JSON:

```
{
  "telemetry_active": true
  "config": {}
}
```

- iv. Introduzca el ID base del paso anterior en **Asset_ID**.
- v. Haga clic en **Ejecutar**.

El servicio Active IQ se reinicia automáticamente cada vez que cambian los activos. La modificación de activos produce un breve retraso antes de aplicar la configuración.

3. Si todavía no lo ha hecho, añada un activo de controladora de vCenter para la supervisión de NetApp HCI (solo instalaciones NetApp HCI) y el control de cloud híbrido (en todas las instalaciones) a los activos conocidos del nodo de gestión:



Se requiere un activo de controlador para los servicios de supervisión de NetApp HCI.

- a. Haga clic en **POST /Asset/{Asset_id}/Controller** para agregar un subactivo de controlador.
- b. Haga clic en **probar**.
- c. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
- d. Introduzca los valores de carga útil requeridos con `type` como `vCenter` De aplicaciones y `vCenter`.

```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



`ip` Es la dirección IP de vCenter.

- e. Haga clic en **Ejecutar**.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Configure Cloud Control de NetApp híbrido para varias instancias de vCenter

Es posible configurar NetApp Hybrid Cloud Control para gestionar activos desde dos o más vCenter que no utilicen Linked Mode.

Debe utilizar este proceso después de la instalación inicial cuando necesite añadir activos para una instalación a escala reciente o cuando no se agreguen automáticamente activos nuevos a la configuración. Utilice estas API para añadir activos que se han añadido recientemente a su instalación.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Pasos

1. ["Añada nuevas instancias de vCenter como activos de la controladora"](#) a la configuración del nodo de gestión.
2. ["Añada nuevos nodos de computación como activos de computación"](#) a la configuración del nodo de gestión.



Puede que necesite hacerlo "[Cambie las credenciales de BMC para los nodos de computación](#)" para resolver un Hardware ID not available o. Unable to Detect El error aparece en el control del cloud híbrido de NetApp.

3. Actualice la API del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```



Como alternativa, puede esperar 2 minutos para que el inventario se actualice en la interfaz de usuario de control del cloud híbrido de NetApp.

- a. Haga clic en **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Haga clic en **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana.
 - b. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /Installations**.
 - c. Haga clic en **probar**.
 - d. Haga clic en **Ejecutar**.
 - e. Desde la respuesta, copie el ID del activo de instalación ("`id`").
 - f. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /Installations/{id}**.
 - g. Haga clic en **probar**.
 - h. Establezca Refresh a `True`.
 - i. Pegue el ID de activo de instalación en el campo **id**.
 - j. Haga clic en **Ejecutar**.
4. Actualice el explorador de NetApp Hybrid Cloud Control para ver los cambios.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Añada activos de computación y de controladora al nodo de gestión

Es posible añadir activos de computación y controladora a la configuración del nodo de gestión mediante la interfaz de usuario de API DE REST.

Es posible que tenga que agregar un activo si ha escalado recientemente su instalación y no se han añadido automáticamente nuevos activos a la configuración. Utilice estas API para añadir activos que se han añadido recientemente a su instalación.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.

- Un nodo de gestión se implementó con la versión 11.3 o posterior.
- Ya tienes "[Se ha creado un nuevo rol HCC de NetApp en vCenter](#)" Para limitar la vista de servicios de nodos de gestión a activos de solo NetApp.
- Tiene la dirección IP de gestión de vCenter y las credenciales.
- Tiene la dirección IP de gestión y las credenciales raíz del nodo de computación (ESXi).
- Tiene la dirección IP de administración del hardware (BMC) y las credenciales de administrador.

Acerca de esta tarea

(Solo NetApp HCI) Si no ve nodos de computación en control de cloud híbrido (HCC) después de escalar el sistema NetApp HCI, puede añadir un nodo de computación con el `POST /assets/{asset_id}/compute-nodes` se describe en este procedimiento.



Quando agregue nodos de computación manualmente, asegúrese de que también agrega los activos de BMC; de lo contrario, se devuelve un error.

Pasos

1. Obtenga el ID de activo base para la instalación:
 - a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana.
- c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
- d. Seleccione **probar**.
- e. Seleccione **Ejecutar**.
- f. Del cuerpo de respuesta del código 200, copie el `id` para la instalación.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```




Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

- g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.
 - h. Seleccione **probar**.
 - i. Pegue el ID de activo de instalación en el campo **id**.
 - j. Seleccione **Ejecutar**.
 - k. En la respuesta, copie y guarde el ID de controladora del clúster ("`controllerId`") para usar en un paso posterior.
2. (Solo para nodos de computación) [Busque la etiqueta de hardware para el nodo de computación](#) En vSphere.
 3. Para añadir un activo de controladora (vCenter), nodo de computación (ESXi) o hardware (BMC) a un activo base existente, seleccione una de las siguientes opciones.

Opción	Descripción
POST /assets/{asset_id}/controladoras	<ol style="list-style-type: none">a. Abra la interfaz de usuario de API DE REST de mNode Service en el nodo de gestión: <div style="border: 1px solid #ccc; border-radius: 5px; padding: 10px; margin: 10px 0;"><code>https://<ManagementNodeIP>/mnode</code></div>i. Seleccione autorizar y complete lo siguiente:<ol style="list-style-type: none">A. Introduzca el nombre de usuario y la contraseña del clúster.B. Introduzca el ID de cliente as <code>mnode-client</code>.C. Seleccione autorizar para iniciar una sesión.D. Cierre la ventana.b. Seleccione POST /Asset/{Asset_id}/controllers.c. Seleccione probar.d. Introduzca el ID de activo base principal en el campo Asset_id.e. Añada los valores necesarios a la carga útil.f. Seleccione Ejecutar.

Opción	Descripción
POST /Asset/{Asset_id}/Compute-Nodes	<p>a. Abra la interfaz de usuario de API DE REST de mNode Service en el nodo de gestión:</p> <div data-bbox="760 258 1485 352" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <pre>https://<ManagementNodeIP>/mnode</pre> </div> <p>i. Seleccione autorizar y complete lo siguiente:</p> <ul style="list-style-type: none"> A. Introduzca el nombre de usuario y la contraseña del clúster. B. Introduzca el ID de cliente as <code>mnode-client</code>. C. Seleccione autorizar para iniciar una sesión. D. Cierre la ventana. <p>b. Seleccione POST /Asset/{Asset_id}/Compute-Nodes.</p> <p>c. Seleccione probar.</p> <p>d. Introduzca el ID de activo base principal que copió en un paso anterior en el campo Asset_id.</p> <p>e. En la carga útil, haga lo siguiente:</p> <ul style="list-style-type: none"> i. Introduzca la IP de gestión para el nodo en la <code>ip</code> campo. ii. Para <code>hardwareTag</code>, introduzca el valor de etiqueta de hardware que guardó en un paso anterior. iii. Introduzca otros valores, según sea necesario. <p>f. Seleccione Ejecutar.</p>

Opción	Descripción
POST /assets/{asset_id}/hardware-nodos	<p>a. Abra la interfaz de usuario de API DE REST de mNode Service en el nodo de gestión:</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0; background-color: #f9f9f9;"> <pre>https://<ManagementNodeIP>/mnode</pre> </div> <p>i. Seleccione autorizar y complete lo siguiente:</p> <ul style="list-style-type: none"> A. Introduzca el nombre de usuario y la contraseña del clúster. B. Introduzca el ID de cliente as <code>mnode-client</code>. C. Seleccione autorizar para iniciar una sesión. D. Cierre la ventana. <p>b. Seleccione POST /assets/{asset_id}/hardware-nodes.</p> <p>c. Seleccione probar.</p> <p>d. Introduzca el ID de activo base principal en el campo Asset_id.</p> <p>e. Añada los valores necesarios a la carga útil.</p> <p>f. Seleccione Ejecutar.</p>

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Cómo localizar una etiqueta de hardware para un nodo de computación

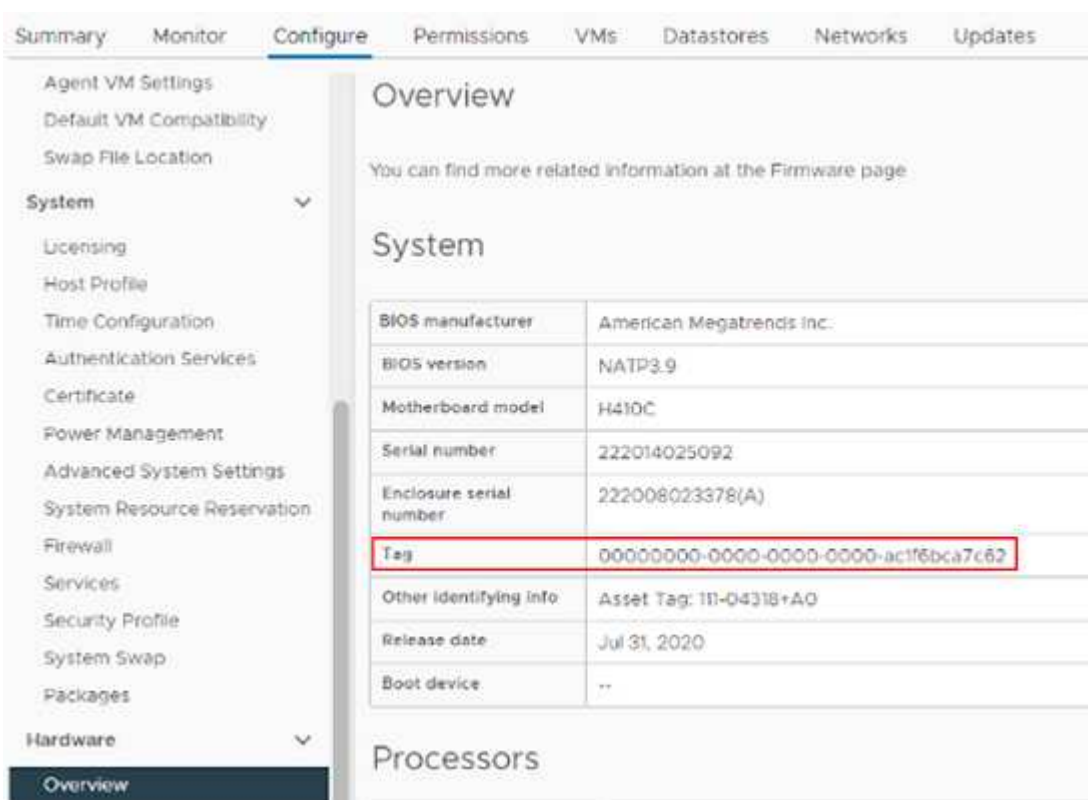
Es necesario usar la etiqueta de hardware para añadir los activos del nodo de computación a la configuración del nodo de gestión mediante la interfaz de usuario de la API DE REST.

VMware vSphere 8.0 y 7.0

Busque la etiqueta de hardware para un nodo de computación en VMware vSphere Web Client 8.0 y 7.0.

Pasos

1. Seleccione el host en el navegador vSphere Web Client.
2. Seleccione la ficha **Configurar**.
3. En la barra lateral, seleccione **hardware** > **Descripción general**. Compruebe si la etiqueta de hardware aparece en la System tabla.



The screenshot shows the VMware vSphere Web Client interface. The 'Configure' tab is active, and the 'System' section is expanded. The 'System' table is visible, with the 'Tag' row highlighted by a red box. The 'Tag' value is '00000000-0000-0000-0000-ac1f6bca7c62'. Below the table, the 'Processors' section is partially visible.

Property	Value
BIOS manufacturer	American Megatrends inc.
BIOS version	NATP3.9
Motherboard model	H410C
Serial number	222014025092
Enclosure serial number	222008023378(A)
Tag	00000000-0000-0000-0000-ac1f6bca7c62
Other identifying info	Asset Tag: 111-04318rA0
Release date	Jul 31, 2020
Boot device	--

4. Copie y guarde el valor para **Tag**.
5. [Añada los activos de computación y de controladora al nodo de gestión.](#)

VMware vSphere 6.7 y 6.5

Busque la etiqueta de hardware para un nodo de computación en VMware vSphere Web Client 6.7 y 6.5.

Pasos

1. Seleccione el host en el navegador vSphere Web Client.
2. Seleccione la ficha **Monitor** y seleccione **Estado del hardware**.
3. Compruebe si la etiqueta aparece en la lista con el fabricante del BIOS y el número de modelo.

Summary **Monitor** Configure Permissions VMs Datastores Networks Updates

▼ Issues and Alarms
 All Issues
 Triggered Alarms
 ▼ Performance
 Overview
 Advanced
 ▼ Tasks and Events
 Tasks
 Events
 Hardware Health
 Health

Hardware Health

BIOS Manufacturer: , BIOS Version: NA2.1
 Model: H700E, Serial Number: 000172000247, **Tag: 00000000-0000-0000-0000-0cc47ad47cac** OTH
 No alerts or warnings out of 59 sensors.

SENSORS ALERTS AND WARNINGS SYSTEM EVENT LOG

Expand rows to view more information about SEL entries and FRU data

REFRESH EXPORT

ID	Sensors	Status	Reading	SI
0,29,1,65	Fan Device 1 FAN1	✓ Normal	10300 RPM	C

4. Copie y guarde el valor para **Tag**.
5. [Añada los activos de computación y de controladora al nodo de gestión.](#)

Crear y gestionar activos de clúster de almacenamiento

Es posible añadir activos de clúster de almacenamiento nuevos al nodo de gestión, editar las credenciales almacenadas para activos de clúster de almacenamiento conocidos y eliminar activos de clúster de almacenamiento del nodo de gestión mediante la API REST.

Lo que necesitará

- Asegúrese de que la versión del clúster de almacenamiento ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.

Opciones de gestión de los activos del clúster de almacenamiento

Seleccione una de las siguientes opciones:

- [Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento](#)
- [Añada un nuevo activo de clúster de almacenamiento](#)
- [Editar las credenciales almacenadas de un activo de clúster de almacenamiento](#)
- [Eliminar un activo de clúster de almacenamiento](#)

Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento

Puede usar la API REST para obtener el ID de instalación y el ID de clúster de almacenamiento. Es necesario que el ID de instalación añada un nuevo activo de clúster de almacenamiento y el ID de clúster para modificar o eliminar un activo de clúster de almacenamiento específico.

Pasos

1. Acceda a la interfaz de usuario de LA API DE REST para el servicio de inventario introduciendo la dirección IP del nodo de gestión seguida de `/inventory/1/`:

```
https://<ManagementNodeIP>/inventory/1/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
3. Haga clic en **GET /Installations**.
4. Haga clic en **probar**.
5. Haga clic en **Ejecutar**.

La API muestra una lista de todas las instalaciones conocidas.

6. Desde el cuerpo de respuesta de código 200, guarde el valor en `id` en la lista de instalaciones encontrará. Este es el ID de instalación. Por ejemplo:

```
"installations": [  
  {  
    "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",  
    "name": "my-hci-installation",  
    "_links": {  
      "collection": "https://localhost/inventory/1/installations",  
      "self": "https://localhost/inventory/1/installations/1234a678-  
12ab-35dc-7b4a-1234a5b6a7ba"  
    }  
  }  
]
```

7. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
9. Haga clic en **GET /Clusters**.
10. Haga clic en **probar**.

11. Introduzca el ID de instalación que guardó anteriormente en la `installationId` parámetro.

12. Haga clic en **Ejecutar**.

La API muestra una lista de todos los clústeres de almacenamiento conocidos en esta instalación.

13. En el cuerpo de respuesta del código 200, busque el clúster de almacenamiento correcto y guarde el valor en el clúster `storageId` campo. Este es el ID del clúster de almacenamiento.

Añada un nuevo activo de clúster de almacenamiento

Es posible usar la API DE REST para añadir uno o varios activos nuevos del clúster de almacenamiento al inventario de nodos de gestión. Cuando se añade un nuevo activo de clúster de almacenamiento, se registra automáticamente con el nodo de gestión.

Lo que necesitará

- Ha copiado la [El ID del clúster de almacenamiento y el ID de instalación](#) para los clústeres de almacenamiento que desea añadir.
- Si va a añadir más de un nodo de almacenamiento, ha leído y comprendido las limitaciones de "[cluster de autoridad](#)" compatibilidad con varios clústeres de almacenamiento.



Todos los usuarios definidos en el clúster autorizado se definen como usuarios en todos los demás clústeres vinculados a la instancia de Hybrid Cloud Control.

Pasos

1. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:

- a. Introduzca el nombre de usuario y la contraseña del clúster.
- b. Introduzca el ID de cliente as `mnode-client`.
- c. Haga clic en **autorizar** para iniciar una sesión.
- d. Cierre la ventana.

3. Haga clic en **POST /cluster**.

4. Haga clic en **probar**.

5. Introduzca la información del nuevo clúster de almacenamiento en los siguientes parámetros en el campo **cuerpo de la solicitud**:

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

Parámetro	Tipo	Descripción
installationId	cadena	La instalación en la que añadir el nuevo clúster de almacenamiento. Introduzca el ID de instalación que guardó anteriormente en este parámetro.
mvip	cadena	La dirección IP virtual de gestión de IPv4 (MVIP) del clúster de almacenamiento.
password	cadena	La contraseña que se utiliza para comunicarse con el clúster de almacenamiento de.
userId	cadena	El ID de usuario que se utiliza para comunicarse con el clúster de almacenamiento (el usuario debe tener privilegios de administrador).

6. Haga clic en **Ejecutar**.

La API muestra un objeto que contiene información acerca del activo del clúster de almacenamiento recién añadido, como información del nombre, la versión y la dirección IP.

Editar las credenciales almacenadas de un activo de clúster de almacenamiento

Puede editar las credenciales almacenadas que utiliza el nodo de gestión para iniciar sesión en un clúster de almacenamiento. El usuario que seleccione debe tener acceso de administrador del clúster.



Asegúrese de haber seguido los pasos de [Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento](#) antes de continuar.

Pasos

1. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:

- a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
3. Haga clic en **PUT /Clusters/{storageId}**.
 4. Haga clic en **probar**.
 5. Pegue el ID del clúster de almacenamiento que ha copiado anteriormente en el `storageId` parámetro.
 6. Cambie uno o ambos de los siguientes parámetros en el campo **cuerpo de solicitud**:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parámetro	Tipo	Descripción
password	cadena	La contraseña que se utiliza para comunicarse con el clúster de almacenamiento de.
userId	cadena	El ID de usuario que se utiliza para comunicarse con el clúster de almacenamiento (el usuario debe tener privilegios de administrador).

7. Haga clic en **Ejecutar**.

Eliminar un activo de clúster de almacenamiento

Es posible eliminar un activo de clúster de almacenamiento si el clúster de almacenamiento ya no está en servicio. Cuando se quita un activo de clúster de almacenamiento, este se cancela automáticamente del nodo de gestión.



Asegúrese de haber seguido los pasos de [Recuperar el ID de instalación y el ID de clúster de un activo de clúster de almacenamiento](#) antes de continuar.

Pasos

1. Acceda a la interfaz de usuario de API DE REST del servicio de almacenamiento introduciendo la dirección IP del nodo de gestión seguida de `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.

- b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
3. Haga clic en **DELETE /Clusters/{storageId}**.
4. Haga clic en **probar**.
5. Introduzca el ID del clúster de almacenamiento que copió anteriormente en el `storageId` parámetro.
6. Haga clic en **Ejecutar**.

Una vez realizado correctamente, la API devuelve una respuesta vacía.

Obtenga más información

- ["Cluster de autoridad"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Ver o editar activos de controladora existentes

Es posible ver información y editar las controladoras VMware vCenter existentes en la configuración del nodo de gestión mediante la API DE REST. Las controladoras son instancias de VMware vCenter registradas en el nodo de gestión para su instalación de NetApp HCI.

Antes de empezar

- Asegúrese de que la versión de su clúster ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.

Acceda a la API DE REST de servicios de gestión

Pasos

1. Acceda a la interfaz de usuario de la API DE REST para servicios de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/vcenter/1/`:

```
https://<ManagementNodeIP>/vcenter/1/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.

Ver la información almacenada sobre las controladoras existentes

Es posible ver una lista de las controladoras de vCenter existentes que están registradas con el nodo de gestión y ver información almacenada sobre ellas mediante la API DE REST.

Pasos

1. Haga clic en **GET /Compute/controllers**.
2. Haga clic en **probar**.
3. Haga clic en **Ejecutar**.

La API muestra una lista de todas las controladoras de vCenter conocidas, junto con la dirección IP, el ID de controladora, el nombre de host y el ID de usuario que se utilizan para comunicarse con cada controladora.

4. Si desea el estado de conexión de una controladora determinada, copie el ID de controladora del `id` de esa controladora en el portapapeles y consulte [Ver el estado de una controladora existente](#).

Ver el estado de una controladora existente

Es posible ver el estado de cualquiera de las controladoras existentes de vCenter que estén registradas en el nodo de gestión. La API muestra un estado que indica si el control de cloud híbrido de NetApp puede conectarse con la controladora de vCenter, así como el motivo de dicho estado.

Pasos

1. Haga clic en **GET /Compute/controllers/{Controller_id}/status**.
2. Haga clic en **probar**.
3. Introduzca el ID de controladora que copió anteriormente en la `controller_id` parámetro.
4. Haga clic en **Ejecutar**.

La API muestra el estado de esta controladora de vCenter en particular, junto con un motivo por el cual ese estado.

Edite las propiedades almacenadas de un controlador

Es posible editar el nombre de usuario o la contraseña almacenados de cualquiera de las controladoras existentes de vCenter registradas en el nodo de gestión. No se puede editar la dirección IP almacenada de una controladora de vCenter existente.

Pasos

1. Haga clic en **PUT /compute/controllers/{Controller_id}**.
2. Introduzca el ID de la controladora de una controladora de vCenter en el `controller_id` parámetro.
3. Haga clic en **probar**.
4. Cambie uno de los siguientes parámetros en el campo **cuerpo de solicitud**:

Parámetro	Tipo	Descripción
<code>userId</code>	cadena	Cambie el ID de usuario usado para comunicarse con la controladora de vCenter (el usuario debe tener privilegios de administrador).
<code>password</code>	cadena	Cambie la contraseña usada para comunicarse con la controladora de vCenter.

5. Haga clic en **Ejecutar**.

La API muestra información actualizada de la controladora.

Obtenga más información

- ["Añada activos de computación y de controladora al nodo de gestión"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Quite un activo del nodo de gestión

Si sustituye físicamente un nodo de computación o es necesario quitarlo del clúster NetApp HCI, debe quitar el activo del nodo de computación mediante las API del nodo de gestión.

Lo que necesitará

- El clúster de almacenamiento ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Pasos

1. Introduzca la dirección IP del nodo de gestión seguida de `/mnode/1/`:

```
https://<ManagementNodeIP>/mnode/1/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo e introduzca las credenciales de administración del clúster para los permisos de uso de las API.
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Seleccione **solicitar cuerpo** en la lista desplegable Tipo si el valor no está seleccionado.
 - c. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
 - d. No introduzca un valor para el secreto de cliente.
 - e. Haga clic en **autorizar** para iniciar una sesión.
 - f. Cierre la ventana.
3. Cierre el cuadro de diálogo **autorizaciones disponibles**.
4. Haga clic en **GET/Assets**.
5. Haga clic en **probar**.
6. Haga clic en **Ejecutar**.
7. Desplácese hacia abajo en el cuerpo de respuesta hasta la sección **cálculo** y copie la `parent y. id` valores para el nodo de computación con fallos.
8. Haga clic en **ELIMINAR/assets/{Asset_id}/compute-Nodes/{Compute_id}**.
9. Haga clic en **probar**.
10. Introduzca el `parent y. id` valores copiados en un paso anterior.

11. Haga clic en **Ejecutar**.

Configure un servidor proxy

Si su clúster de está situado detrás de un servidor proxy, debe configurar el proxy de manera que pueda llegar a una red pública.

Un servidor proxy se utiliza para recopiladores de telemetría y conexiones de túnel inverso. Puede habilitar y configurar un servidor proxy con la interfaz de usuario de la API de REST si aún no configuró un servidor proxy durante la instalación o la actualización. También puede modificar la configuración existente del servidor proxy o deshabilitar un servidor proxy.

El comando para configurar un servidor proxy se actualiza y, a continuación, devuelve la configuración del proxy actual del nodo de gestión. Active IQ utiliza la configuración de proxy, el servicio de supervisión de NetApp HCI implementado por el motor de puesta en marcha de NetApp y otras utilidades de software Element instaladas en el nodo de gestión, incluido el túnel de soporte inverso para el soporte de NetApp.

Antes de empezar

- Debe conocer información sobre el host y las credenciales del servidor proxy que desea configurar.
- Asegúrese de que la versión de su clúster ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.
- (Nodo de gestión 12.0 y posterior) ha actualizado NetApp Hybrid Cloud Control a los servicios de gestión versión 2.16 antes de configurar un servidor proxy.

Pasos

1. Acceda a la interfaz de usuario de API DE REST en el nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode`:

```
https://<ManagementNodeIP>/mnode
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
3. Haga clic en **PONER /settings**.
4. Haga clic en **probar**.
5. Para habilitar un servidor proxy, debe definir `use_proxy` a verdadero. Introduzca el nombre de host o la IP y los destinos de puerto proxy.

El nombre de usuario del proxy, la contraseña del proxy y el puerto SSH son opcionales y deben omitirse si no se usan.

```
{
  "proxy_ip_or_hostname": "[IP or name]",
  "use_proxy": [true/false],
  "proxy_username": "[username]",
  "proxy_password": "[password]",
  "proxy_port": [port value],
  "proxy_ssh_port": [port value: default is 443]
}
```

6. Haga clic en **Ejecutar**.



Es posible que deba reiniciar su nodo de gestión según su entorno.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Verifique el sistema operativo del nodo de gestión y las versiones de servicios

Puede verificar los números de versión del sistema operativo del nodo de gestión, del paquete de servicios de gestión y de los servicios individuales que se ejecutan en el nodo de gestión mediante la API DE REST en el nodo de gestión.

Lo que necesitará

- El clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Opciones

- [Comandos API](#)
- [PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST](#)

Comandos API

- Obtenga información de la versión acerca del sistema operativo del nodo de gestión, el paquete de servicios de gestión y el servicio API del nodo de gestión (mnode-api) que se ejecutan en el nodo de gestión:

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H "accept:
application/json"
```

- Obtenga información de versión sobre los servicios individuales que se ejecutan en el nodo de gestión:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H "accept: */*" -H "Authorization: Bearer ${TOKEN}"
```



Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza "autorizar". El portador `${TOKEN}` está en la respuesta curl.

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de la API DE REST del servicio introduciendo la dirección IP del nodo de gestión seguida de `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Debe realizar una de las siguientes acciones:

- Obtenga información de la versión acerca del sistema operativo del nodo de gestión, el paquete de servicios de gestión y el servicio API del nodo de gestión (`mnode-api`) que se ejecutan en el nodo de gestión:
 - i. Seleccione **GET /about**.
 - ii. Seleccione **probar**.
 - iii. Seleccione **Ejecutar**.

La versión del paquete de servicios de gestión ("`mnode_bundle_version`"), versión del sistema operativo del nodo de gestión ("`os_version`") Y la versión de la API del nodo de gestión ("`version`") se indican en el cuerpo de respuesta.

- Obtenga información de versión sobre los servicios individuales que se ejecutan en el nodo de gestión:
 - i. Seleccione **GET /Services**.
 - ii. Seleccione **probar**.
 - iii. Seleccione el estado como **en ejecución**.
 - iv. Seleccione **Ejecutar**.

Los servicios que se ejecutan en el nodo de gestión se indican en el cuerpo de respuesta.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Obtener registros de los servicios de gestión

Es posible recuperar registros de los servicios que se ejecutan en el nodo de gestión mediante la API DE REST. Puede extraer registros de todos los servicios públicos o especificar servicios específicos y utilizar parámetros de consulta para definir mejor los resultados devueltos.

Lo que necesitará

- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Un nodo de gestión se implementó con la versión 11.3 o posterior.

Pasos

1. Abra la interfaz de usuario de API de REST en el nodo de gestión.

- A partir de los servicios de administración 2.21.61:

```
https://<ManagementNodeIP>/mnode/4/
```

- Para los servicios de gestión 2.20.69 o anteriores:

```
https://<ManagementNodeIP>/mnode
```

2. Seleccione **autorizar** o cualquier icono de bloqueo y complete lo siguiente:

- Introduzca el nombre de usuario y la contraseña del clúster.
- Introduzca el ID de cliente como mnode-client si el valor no está ya rellenado.
- Seleccione **autorizar** para iniciar una sesión.
- Cierre la ventana.

3. Seleccione **GET /logs**.

4. Seleccione **probar**.

5. Especifique los siguientes parámetros:

- `Lines`: Introduzca el número de líneas que desea que devuelva el registro. Este parámetro es un entero que se establece de manera predeterminada en 1000.



Evite solicitar el historial completo del contenido de registro estableciendo líneas en 0.

- `since`: Agrega una Marca de tiempo ISO-8601 para el punto de inicio de los registros de servicio.



Usar un razonable `since` parámetro cuando se recogen registros de timespans más amplios.

- `service-name`: Introduzca un nombre de servicio.



Utilice la `GET /services` comando para mostrar los servicios del nodo de gestión.

- `stopped`: Establecer en `true` para recuperar registros de servicios detenidos.

6. Seleccione **Ejecutar**.

7. En el cuerpo de la respuesta, seleccione **Descargar** para guardar la salida del registro.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Gestión de conexiones de soporte

Inicie una sesión de soporte remota de NetApp

Si necesita soporte técnico para su sistema NetApp HCI, el soporte de NetApp puede conectarse de forma remota con su sistema. Para iniciar una sesión y tener acceso remoto, el soporte de NetApp puede abrir una conexión de Secure Shell (SSH) inversa a su entorno.

Puede abrir un puerto TCP para una conexión de túnel SSH inverso con el soporte de NetApp. Gracias a esta conexión, el soporte de NetApp puede iniciar sesión en su nodo de gestión.

Antes de empezar

- Para los servicios de gestión 2.18 y posteriores, la funcionalidad para el acceso remoto se deshabilita en el nodo de gestión de manera predeterminada. Para activar la función de acceso remoto, consulte ["Gestione la funcionalidad SSH en el nodo de gestión"](#).
- Si el nodo de gestión está detrás de un servidor proxy, se necesitan los siguientes puertos TCP en el archivo sshd.config:

Puerto TCP	Descripción	Dirección de conexión
443	Llamadas API/HTTPS para un reenvío de puertos inverso a través de un túnel de soporte abierto a la interfaz de usuario web	Del nodo de gestión a los nodos de almacenamiento
22	Acceso de inicio de sesión SSH	Del nodo de gestión a los nodos de almacenamiento o desde los nodos de almacenamiento al nodo de gestión

Pasos

- Inicie sesión en su nodo de almacenamiento y abra una sesión de terminal.
- En un símbolo del sistema, introduzca lo siguiente:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Para cerrar el túnel de soporte remoto, introduzca lo siguiente:

```
rst --killall
```

- (Opcional) Deshabilitar ["función de acceso remoto"](#) de nuevo.



SSH permanece habilitado si no lo deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Gestione la funcionalidad SSH en el nodo de gestión

Es posible deshabilitar, volver a habilitar o determinar el estado de la funcionalidad SSH en el nodo de gestión (mNode) mediante la API DE REST. Funcionalidad SSH que proporciona ["Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support"](#) está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posterior.

A partir de los servicios de gestión 2.20.69, puede habilitar y deshabilitar la funcionalidad SSH en el nodo de gestión mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Lo que necesitará

- **Permisos de control del cloud híbrido de NetApp:** Tiene permisos como administrador.
- **Permisos de administrador de clúster:** Tiene permisos como administrador en el clúster de almacenamiento.
- **Software Element:** El clúster ejecuta el software NetApp Element 11.3 o posterior.
- **Nodo de gestión:** Ha implementado un nodo de gestión que ejecuta la versión 11.3 o posterior.
- **Actualizaciones de servicios de administración:**
 - Para utilizar la interfaz de usuario de control del cloud híbrido de NetApp, ha actualizado el ["paquete de servicios de gestión"](#) a la versión 2.20.69 o posterior.
 - Para usar la interfaz de usuario de la API DE REST, se ha actualizado el ["paquete de servicios de gestión"](#) a la versión 2.17.

Opciones

- [Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante la IU de control de cloud híbrido de NetApp](#)

Puede realizar cualquiera de las siguientes tareas después de realizar ["autenticar"](#):

- [Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante las API de](#)
- [Determine el estado de la capacidad SSH en el nodo de gestión mediante las API de](#)

Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante la IU de control de cloud híbrido de NetApp

Es posible deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de gestión. Funcionalidad SSH que proporciona ["Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support"](#) está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posterior. Al deshabilitar SSH, no se finalizan ni desconectan las sesiones de cliente SSH existentes en el nodo de gestión. Si deshabilita SSH y opta por volver a habilitarla más adelante, puede hacerlo mediante la interfaz de usuario de control de cloud híbrido de NetApp.



Para habilitar o deshabilitar el acceso de soporte con SSH para un clúster de almacenamiento, debe usar el ["Página de configuración del clúster de la interfaz de usuario de Element"](#).

Pasos

1. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
2. En la pantalla **Support Access for Management Node**, cambie el conmutador para activar el SSH del nodo de administración.
3. Después de completar la solución de problemas, en la pantalla **Support Access for Management Node**, cambie el conmutador para desactivar el SSH del nodo de gestión.

Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante las API de

Es posible deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de gestión. Funcionalidad SSH que proporciona ["Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support"](#) está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posterior. Al deshabilitar SSH, no se finalizan ni desconectan las sesiones de cliente SSH existentes en el nodo de gestión. Si deshabilita SSH y opta por volver a habilitarla más adelante, puede hacerlo mediante la misma API.

Comando API

Para los servicios de gestión 2.18 o posterior:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Para los servicios de gestión 2.17 o anteriores:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza **"autorizar"**. El portador `${TOKEN}` está en la respuesta curl.

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de API DE REST para el servicio API del nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Seleccione **autorizar** y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Seleccione **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.

3. En la interfaz de usuario DE LA API DE REST, seleccione **PUT /settings/ssh**.
 - a. Haga clic en **probar**.
 - b. Establezca el parámetro **Enabled** en `false` Para deshabilitar SSH o `true` Para volver a habilitar la funcionalidad SSH que estaba deshabilitada anteriormente.
 - c. Haga clic en **Ejecutar**.

Determine el estado de la capacidad SSH en el nodo de gestión mediante las API de

Puede determinar si la capacidad SSH está habilitada o no en el nodo de gestión mediante una API de servicio de nodo de gestión. SSH está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posteriores.

Comando API

Para los servicios de gestión 2.18 o posterior:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Para los servicios de gestión 2.17 o anteriores:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza **"autorizar"**. El portador `${TOKEN}` está en la respuesta curl.

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de API DE REST para el servicio API del nodo de gestión. Para ello, introduzca la dirección IP del nodo de gestión seguida de `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Seleccione **autorizar** y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Seleccione **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
3. En la interfaz de usuario DE LA API DE REST, seleccione **GET /settings/ssh**.
 - a. Haga clic en **probar**.
 - b. Haga clic en **Ejecutar**.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Apaga o enciende el sistema NetApp HCI

Apagar o encender el sistema NetApp HCI

Puede apagar o encender el sistema NetApp HCI si tiene una interrupción programada, si necesita realizar mantenimiento en el hardware o si necesita expandir el sistema. Utilice las siguientes tareas para apagar o encender el sistema NetApp HCI según sea necesario.

Es posible que deba apagar el sistema NetApp HCI en diferentes circunstancias, como:

- Se han programado interrupciones del servicio
- Sustituciones de ventiladores del chasis
- Actualizaciones de firmware
- Ampliación de recursos de almacenamiento o computación

A continuación se ofrece información general de las tareas que debe realizar para apagar un sistema NetApp HCI:

- Apague todas las máquinas virtuales, excepto VMware vCenter Server (vcsa).
- Apague todos los servidores ESXi, excepto el que aloja la instancia de vcsa.
- Apague la instancia de vcsa.
- Apague el sistema de almacenamiento NetApp HCI.

A continuación se ofrece una descripción general de las tareas que necesita completar para encender un sistema NetApp HCI:

- Encienda todos los nodos de almacenamiento físico.
- Encienda todos los nodos de computación físicos.
- Encienda la instancia de vcsa.
- Compruebe el sistema y encienda equipos virtuales adicionales.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Apague los recursos informáticos de un sistema NetApp HCI

Para apagar los recursos de computación de NetApp HCI, debe apagar hosts VMware ESXi individuales, así como el dispositivo de VMware vCenter Server en un orden determinado.

Pasos

1. Inicie sesión en la instancia de vCenter que controla el sistema NetApp HCI y determine la máquina ESXi donde se aloja la instancia de vCenter Server Virtual Appliance (vcsa).
2. Después de determinar el host ESXi que ejecuta vcsa, apague todas las demás máquinas virtuales que no sean la instancia de vcsa de la siguiente manera:
 - a. Seleccione una máquina virtual.
 - b. Haga clic con el botón derecho del ratón y seleccione **Alimentación > Apagar sistema operativo invitado**.
3. Apague todos los hosts ESXi que no sean el host ESXi que ejecute la instancia de vcsa.
4. Apague la instancia de vcsa.

Esto provocará que la sesión de vCenter finalice porque la instancia de vcsa se desconecta durante el proceso de apagado. Todas las máquinas virtuales ahora deben apagarse con solo un host ESXi encendido.

5. Inicie sesión en el host ESXi que ejecuta.
6. Verifique que todas las máquinas virtuales del host estén apagadas.
7. Apague el host ESXi.

Esto desconectará todas las sesiones iSCSI abiertas en el clúster de almacenamiento de NetApp HCI.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Apague los recursos de almacenamiento de un sistema NetApp HCI

Al apagar los recursos de almacenamiento de NetApp HCI, debe utilizar el `Shutdown` El método API Element para detener correctamente los nodos de almacenamiento.

Pasos

Después de apagar los recursos de computación, utilice un explorador web para apagar todos los nodos del clúster de almacenamiento de NetApp HCI.

1. Inicie sesión en el clúster de almacenamiento y compruebe que está conectado a la MVIP correcta.
2. (Opcional) verifique que todas las operaciones de I/O de los hosts se hayan detenido:
 - a. Desactive la actividad de I/O en el lado del host mediante los comandos adecuados para uno o más hipervisores que se utilizan.
 - b. En la interfaz de usuario del clúster, seleccione **Reporting > Overview**. No debe haber ninguna actividad en el gráfico "Cluster Input/Output".
 - c. Una vez que se hayan detenido todas las operaciones de I/O, espere 20 minutos antes de apagar el clúster.
3. Compruebe que el número de sesiones iSCSI sea cero.
4. Vaya a **Cluster > Nodes > Active** y registre los identificadores de nodo de todos los nodos activos del clúster.

5. Para apagar el clúster de almacenamiento de NetApp HCI, abra un explorador web y utilice la siguiente URL para invocar el procedimiento de apagado y detención, donde {MVIP} Es la dirección IP de administración del sistema de almacenamiento NetApp HCI y del `nodes=[]` La matriz incluye los ID de nodo que registró en el paso 4. Por ejemplo:

```
https://{MVIP}/json-rpc/1.0?method=Shutdown&nodes=[1,2,3,4]&option=halt
```



Puede ejecutar el comando en una ventana de incógnito para evitar ejecutarlo de nuevo en una fase posterior desde la URL guardada.

6. Introduzca el nombre de usuario y la contraseña de administrador del clúster.
7. Compruebe que la llamada API se devolvió correctamente verificando que todos los nodos del clúster de almacenamiento están incluidos en la `successful` Del resultado de la API.

Apagó correctamente todos los nodos de almacenamiento NetApp HCI.

8. Cierre el explorador o la pestaña para evitar seleccionar el botón "atrás" y repetir la llamada a la API.

Cuando reinicia el clúster, debe seguir algunos pasos para verificar que todos los nodos entran en línea:

1. Compruebe que todas las gravedad crítica y. `volumesOffline` se resolvieron errores del clúster.
2. Espere de 10 a 15 minutos para que el clúster se asiente.
3. Empiece a poner los hosts a acceder a los datos.



Si desea permitir más tiempo al encender los nodos y verificar que su estado sea después del mantenimiento, póngase en contacto con el soporte técnico para obtener ayuda con la demora de la sincronización de datos para evitar la sincronización innecesaria de bandejas.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Activar recursos de almacenamiento para un sistema NetApp HCI

NetApp HCI se puede encender después de completar la interrupción programada.

Pasos

1. Encienda todos los nodos de almacenamiento usando el botón de encendido físico o el BMC.
2. Si utiliza el BMC, inicie sesión en cada nodo y desplácese a **Control remoto > Control de alimentación > servidor de encendido**.
3. Cuando todos los nodos de almacenamiento estén en línea, inicie sesión en el sistema de almacenamiento de NetApp HCI y verifique que todos los nodos estén operativos.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Encienda los recursos informáticos para un sistema NetApp HCI

Una vez finalizada la interrupción programada, puede encender los recursos de computación para un sistema NetApp HCI.

Pasos

1. Encienda los nodos de computación con los mismos pasos que realizó para encender los nodos de almacenamiento.
2. Cuando todos los nodos de computación estén operativos, inicie sesión en el host ESXi que ejecutaba vcsa.
3. Inicie sesión en el host de computación y compruebe que ve todos los almacenes de datos NetApp HCI. Para un sistema NetApp HCI típico, debe ver todos los almacenes de datos locales ESXi y, al menos, los siguientes almacenes de datos compartidos:

```
NetApp-HCI-Datastore-[01,02]
```

1. Suponiendo que se pueda acceder a todo el almacenamiento, encienda la instancia de vcsa y cualquier otra máquina virtual necesaria de la siguiente forma:
 - a. Seleccione las máquinas virtuales del navegador, seleccione todas las máquinas virtuales que desee encender y haga clic en el botón **encendido**.
2. Después de encender las máquinas virtuales, espere aproximadamente 5 minutos y luego utilice un explorador web para acceder a la dirección IP o el FQDN de la aplicación vcsa.

Si no espera lo suficiente, aparece un mensaje que indica que el servidor web de vSphere Client se está inicializando.

3. Una vez que se inicializa vSphere Client, inicie sesión y verifique que todos los hosts ESXi y las máquinas virtuales estén en línea.

Obtenga más información

- ["Versiones de firmware y controlador ESXi compatibles para las versiones de NetApp HCI y firmware para los nodos de almacenamiento NetApp HCI"](#)

Supervise su sistema NetApp HCI con el control del cloud híbrido de NetApp

Supervise los recursos de almacenamiento y computación en la consola de control de cloud híbrido

Con la consola de control del cloud híbrido de NetApp, puede ver todos sus recursos de almacenamiento y computación de un solo vistazo. Además, puede supervisar la capacidad de almacenamiento, el rendimiento del almacenamiento y el aprovechamiento de la computación.



Cuando inicia una nueva sesión de control del cloud híbrido de NetApp por primera vez, es posible que haya un retraso al cargar la vista de la consola de control del cloud híbrido de NetApp cuando el nodo de gestión gestiona muchos clústeres. El tiempo de carga varía en función del número de clústeres que gestiona el nodo de gestión activamente. Para lanzamientos posteriores, experimentará tiempos de carga más rápidos.

Solo se muestran en la consola de control de cloud híbrido los nodos de computación que se gestionan y los clústeres con al menos un nodo gestionado en hardware H-Series.

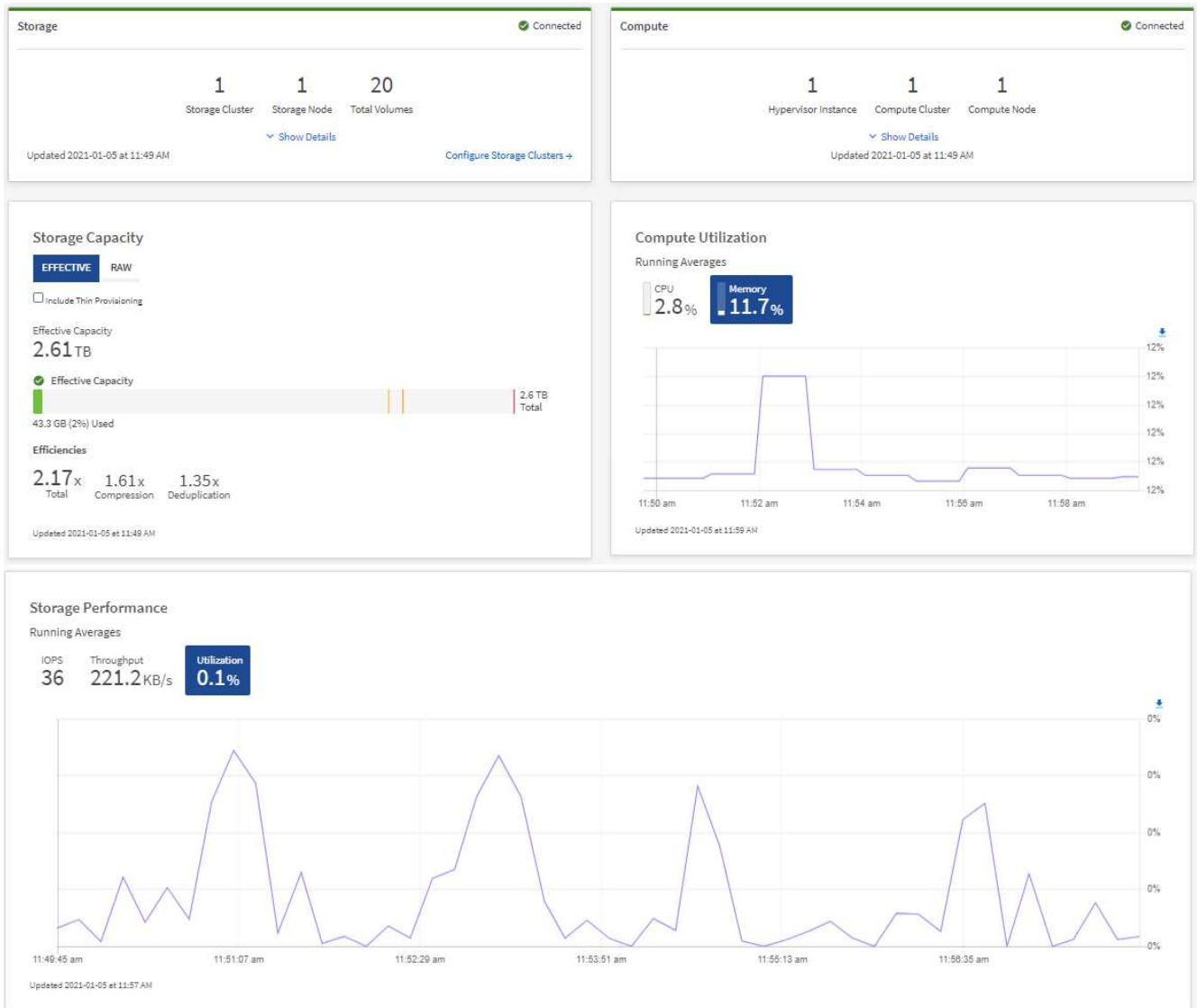
- [Acceda a la consola HCC de NetApp](#)
- [Supervise los recursos de almacenamiento](#)
- [Supervise los recursos de computación](#)
- [Supervise la capacidad de almacenamiento](#)
- [Supervise el rendimiento del almacenamiento](#)
- [Supervise el uso de los recursos informáticos](#)

Acceda a la consola HCC de NetApp

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. Consulte la consola de control del cloud híbrido.



Puede que vea algunos o todos estos paneles, según su instalación. Por ejemplo, para instalaciones solo de almacenamiento, la consola de control de cloud híbrido muestra solo el panel almacenamiento, el panel capacidad de almacenamiento y el panel rendimiento de almacenamiento.

Supervise los recursos de almacenamiento

Utilice el panel **almacenamiento** para ver su entorno de almacenamiento total. Es posible supervisar el número de clústeres de almacenamiento, los nodos de almacenamiento y el total de volúmenes.

Para ver los detalles, en el panel almacenamiento, seleccione **Mostrar detalles**.

Storage
✔ Connected

1
2
16

Storage Cluster
Total Storage Nodes
Total Volumes

[^ Hide Details](#)

Cluster Name ↑	Nodes	Volumes	Connection Status
hci-tt-test8-cluster	4	16	✔ Connected

Updated 2021-10-04 at 4:52 PM
[Configure Storage Clusters →](#)



El número total de nodos de almacenamiento no incluye nodos de testigos de clústeres de almacenamiento de dos nodos. Los nodos de testigos se incluyen en el número de nodos de la sección de detalles de ese clúster.



Para ver los datos más recientes del clúster de almacenamiento, use la página Storage Clusters, donde el sondeo se produce con más frecuencia que en la consola.

Supervise los recursos de computación

Utilice el panel **Compute** para ver su entorno informático total de NetApp H-Series. Es posible supervisar el número de clústeres de computación y el total de nodos de computación.

Para ver detalles, en los paneles computación, seleccione **Mostrar detalles**.



Las instancias de vCenter solo se muestran en el panel Compute cuando al menos un nodo de computación de NetApp HCI está asociado a esa instancia. Para enumerar las instancias de vCenter vinculadas en NetApp Hybrid Cloud Control, puede utilizar el "API".



Para gestionar un nodo de computación en NetApp Hybrid Cloud Control, debe hacerlo "[Añada el nodo de computación a un clúster de hosts de vCenter](#)".

Supervise la capacidad de almacenamiento

Supervisar la capacidad de almacenamiento del entorno es crucial. Mediante el panel capacidad de almacenamiento, puede determinar sus ganancias en eficiencia de la capacidad del almacenamiento con o sin funciones de compresión, deduplicación y thin provisioning habilitadas.

Puede ver el espacio de almacenamiento físico total disponible en su clúster en la ficha **RAW** e información sobre el almacenamiento aprovisionado en la ficha **EFFECTIVO**.



Para ver el estado del clúster, también consulte la consola de SolidFire Active IQ. Consulte ["Supervise el rendimiento, la capacidad y el estado del clúster en SolidFire Active IQ de NetApp"](#).

Pasos

1. Seleccione la ficha **RAW** para ver el espacio de almacenamiento físico total utilizado y disponible en el clúster.

Observe las líneas verticales para determinar si la capacidad que ha utilizado es inferior al total o inferior a los umbrales de advertencia, error o crítico. Pase el ratón por las líneas para ver los detalles.



Puede establecer el umbral de Advertencia, que por defecto es 3% inferior al umbral de error. Los umbrales error y crítico están predefinidos y no se pueden configurar por diseño. El umbral de error indica que aún hay menos de un nodo de capacidad en el clúster. Para conocer los pasos para establecer el umbral, consulte ["Configurar el umbral completo del clúster"](#).



Para obtener más detalles sobre la API de Element de umbrales de clúster relacionados, consulte ["GetClusterFullThreshold"](#) En la documentación de la API del software *Element*. Para ver detalles sobre la capacidad de metadatos y bloques, consulte ["Niveles de llenado de clústeres"](#) En la documentación del software *Element*.

2. Seleccione la ficha **EFFECTIVO** para ver información sobre el almacenamiento total aprovisionado a los hosts conectados y para ver los índices de eficiencia.
 - a. Opcionalmente, compruebe **incluir Thin Provisioning** para ver las tasas de eficiencia de Thin Provisioning en el gráfico de barras de capacidad efectiva.
 - b. **Cuadro de barras de capacidad efectiva:** Observe las líneas verticales para determinar si la capacidad utilizada es inferior o inferior a los umbrales de advertencia, error o crítico. De forma similar a la ficha RAW, puede pasar el ratón por encima de las líneas verticales para ver los detalles.
 - c. **Efficiencias:** Examine estas calificaciones para determinar el aumento de la eficiencia de la capacidad de almacenamiento con las funciones de compresión, deduplicación y thin provisioning activadas. Por ejemplo, si la compresión se muestra como «1,3x», esto significa que la eficiencia del almacenamiento con compresión habilitada es 1.3 veces más eficiente que sin ella.



Las eficiencias totales son iguales a (factor de eficiencia maxUsedSpace *) / 2, donde $\text{efficiencyfactor} = (\text{thinProvisioningfactor} * \text{deDuplicationfactor} * \text{compressionfactor})$. Cuando no se selecciona thin provisioning, no se incluye en la eficiencia total.

- d. Si la capacidad de almacenamiento efectiva se acerca a un umbral de error o crítico, considere borrar los datos de su sistema. También puede ampliar el sistema.

Consulte "[Visión general de la ampliación](#)".

3. Para un análisis más profundo y un contexto histórico, mire "[Detalles de SolidFire Active IQ de NetApp](#)".

Supervise el rendimiento del almacenamiento

Puede ver cuántas IOPS o rendimiento puede obtener de un clúster sin superar el rendimiento útil de ese recurso mediante el panel rendimiento del almacenamiento. El rendimiento del almacenamiento es el punto en el que se obtiene la utilización máxima antes de que la latencia empeore.

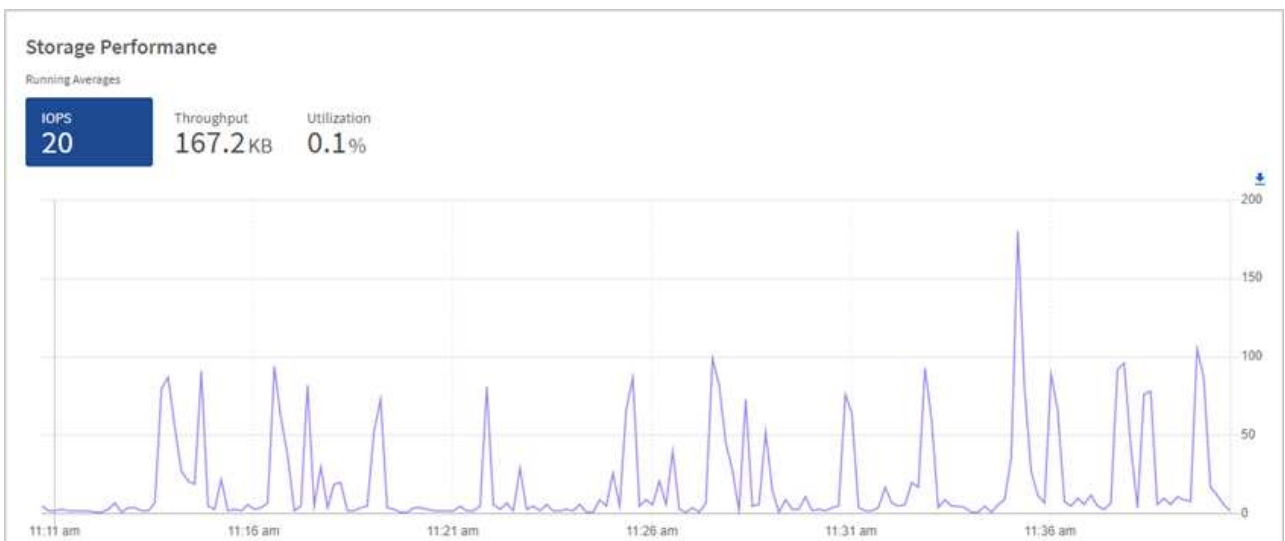
El panel rendimiento del almacenamiento le ayuda a identificar si el rendimiento se está alcanzando el punto en el que el rendimiento podría degradarse si las cargas de trabajo aumentan.

La información de este panel se actualiza cada 10 segundos y muestra un promedio de todos los puntos del gráfico.

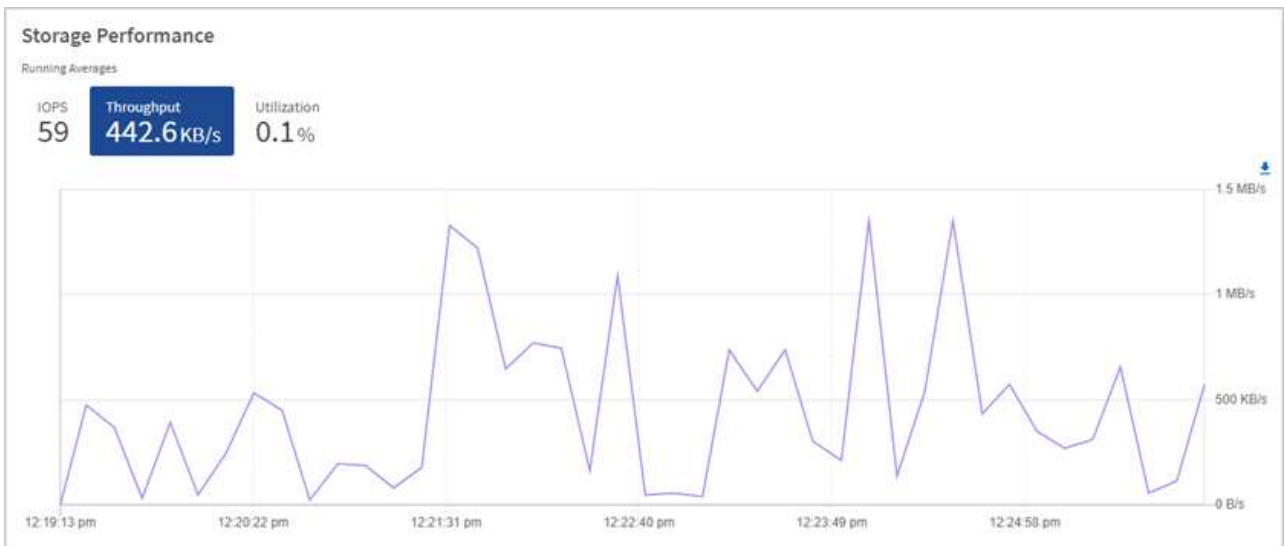
Para obtener detalles sobre el método API de Element asociado, consulte "[GetClusterStats](#)" Método en la documentación de la API del software *Element*.

Pasos

1. Consulte el panel Storage Performance. Para obtener detalles, pase el ratón sobre los puntos del gráfico.
 - a. **Pestaña IOPS:** Consulte las operaciones actuales por segundo. Busque tendencias de datos o picos. Por ejemplo, si observa que el número máximo de IOPS es 160 000 y 100 000 de IOPS libres o disponibles, puede considerar la posibilidad de añadir más cargas de trabajo a este clúster. Por otro lado, si observa que solo 140K está disponible, puede considerar la descarga de cargas de trabajo o la ampliación del sistema.



- b. **Ficha de rendimiento:** Patrones de monitor o picos de rendimiento. Además, supervise constantemente valores de rendimiento elevados, lo que podría indicar que se está acercando al rendimiento máximo útil del recurso.



- c. **Ficha utilización:** Controlar la utilización de IOPS en relación con el total de IOPS disponibles resumido a nivel de clúster.



2. Para obtener más análisis, observe el rendimiento del almacenamiento mediante el complemento de NetApp Element para vCenter Server.

["Rendimiento que se muestra en el plugin de NetApp Element para vCenter Server"](#).

Supervise el uso de los recursos informáticos

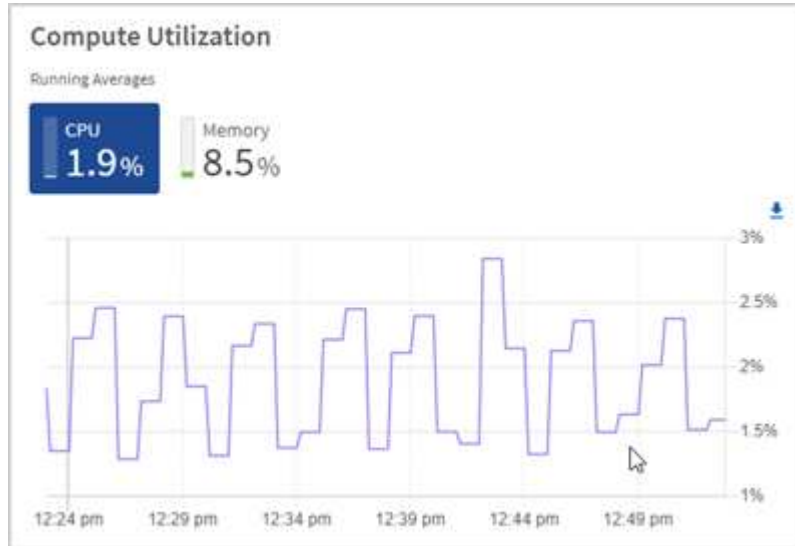
Además de supervisar las IOPS y el rendimiento de los recursos de almacenamiento, quizás también desee ver el uso de la CPU y la memoria de sus activos de computación. El número total de IOPS que puede proporcionar un nodo depende de las características físicas del nodo; por ejemplo, el número de CPU, la velocidad de CPU y la cantidad de RAM.

Pasos

1. Consulte el panel **utilización de computación**. Usando las pestañas CPU y memoria, busque patrones o picos de utilización. También busque un uso continuamente alto, que indica que podría estar cerca del uso máximo para los clústeres de computación.



Este panel muestra datos solo para los clústeres de computación que gestiona esta instalación.



- a. **Pestaña CPU:** Consulte el promedio actual de utilización de CPU en el cluster informático.
 - b. **Ficha memoria:** Consulte el uso medio actual de memoria en el cluster informático.
2. Para obtener más análisis sobre la información de computación, consulte ["SolidFire Active IQ de NetApp para datos históricos"](#).

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)
- ["Documentación de SolidFire Active IQ de NetApp"](#)

Consulte el inventario en la página Nodes

Puede ver tanto los activos de almacenamiento como los activos de computación en el sistema y determinar sus direcciones IP, sus nombres y sus versiones de software.

Se puede ver información de almacenamiento de los sistemas de varios nodos y todos los nodos de observación de NetApp HCI asociados con clústeres de dos o tres nodos. Si ["dominios de protección personalizados"](#) se asignan, puede ver qué dominios de protección se asignan a nodos específicos.

Los nodos de testigos gestionan el quórum dentro del clúster, no se utilizan para el almacenamiento. Los nodos de testigos se aplican solo a NetApp HCI y no a los entornos de almacenamiento all-flash.

Para obtener más información sobre los nodos de testigos, consulte ["Definiciones de nodos"](#).

Para los nodos SDS de SolidFire Enterprise, puede supervisar el inventario en la pestaña Storage.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

https://<ManagementNodeIP>

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. En la navegación de la izquierda, haga clic en **Nodes**.

Nodes

Only NetApp HCI Nodes are displayed on this page.

STORAGE COMPUTE

Cluster1 1 of 1 Two-nodes

Hostname	Node Model	Element Version	Management IP Address
stg01	H410S-0	12.0.0.318	- VLAN 1184
stg02	H410S-0	12.0.0.318	- VLAN 1184

1 - 2 of 2 results

Witness Nodes

Hostname	Management IP Address	Storage (iSCSI) IP Address
wit01		
wit02		



Cuando inicia una nueva sesión de control del cloud híbrido de NetApp por primera vez, es posible que haya un retraso en la carga de la página nodos de control del cloud híbrido de NetApp cuando el nodo de gestión gestiona muchos clústeres. El tiempo de carga varía en función del número de clústeres que gestiona el nodo de gestión activamente. Para lanzamientos posteriores, experimentará tiempos de carga más rápidos.

4. En la ficha **almacenamiento** de la página Nodes, revise la siguiente información:
 - a. Clústeres de dos nodos: Aparece una etiqueta de “dos nodos” en la ficha almacenamiento y se muestran los nodos de testigos asociados.
 - b. Clústeres de tres nodos: Se enumeran los nodos de almacenamiento y los nodos testigo asociados. Los clústeres de tres nodos tienen un nodo testigo puesto en marcha en espera para mantener la alta disponibilidad en caso de fallo del nodo.
 - c. Clústeres con cuatro nodos o más: Se muestra información para los clústeres con cuatro o más nodos. Los nodos de testigos no se aplican. Si comenzó con dos o tres nodos de almacenamiento y añadió más nodos, los nodos testigos seguirán apareciendo. De lo contrario, la tabla de nodos de testigos no aparecerá.
 - d. La versión del paquete de firmware: A partir de la versión 2.14 de los servicios de gestión, si los clústeres ejecutan Element 12.0 o una versión posterior, es posible ver la versión del paquete de firmware de estos clústeres. Si los nodos de un clúster tienen diferentes versiones de firmware en ellos, puede ver **multiple** en la columna **Versión de paquete de firmware**.
 - e. Dominios de protección personalizados: Si en el clúster se usan dominios de protección personalizados, puede ver asignaciones de dominios de protección personalizadas para cada nodo del

clúster. Si los dominios de protección personalizados no están habilitados, esta columna no aparece.

5. Para ver la información de inventario de computación, haga clic en **calcular**.
6. Puede manipular la información de estas páginas de varias maneras:
 - a. Para filtrar la lista de elementos de los resultados, haga clic en el icono **filtro** y seleccione los filtros. También puede introducir texto para el filtro.
 - b. Para mostrar u ocultar columnas, haga clic en el icono **Mostrar/ocultar columnas**.
 - c. Para descargar la tabla, haga clic en el icono **Descargar**.
 - d. Para agregar o editar las credenciales de BMC almacenadas para un nodo de computación con errores de conexión de BMC, haga clic en **Editar configuración de conexión** en el texto del mensaje de error en la columna **BMC Connection Status**. Solo si el intento de conexión falla para un nodo de computación, se muestra un mensaje de error en esta columna para ese nodo.



Para ver el número de recursos de almacenamiento y computación, observe la consola de control del cloud híbrido (HCC) de NetApp. Consulte ["Supervise los recursos de almacenamiento y computación con la consola de HCC"](#).



Para gestionar un nodo de computación en NetApp Hybrid Cloud Control, debe hacerlo ["Añada el nodo de computación a un clúster de hosts de vCenter"](#).

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Edite la información de conexión de la controladora de gestión de placa base

Puede cambiar las credenciales de administrador de la controladora de gestión de placa base (BMC) en el control de cloud híbrido de NetApp para cada uno de los nodos de computación. Es posible que deba cambiar las credenciales antes de actualizar el firmware de BMC o resolver un `Hardware ID not available` o `Unable to Detect`. El error aparece en el control del cloud híbrido de NetApp.

Lo que necesitará

Permisos de administrador de clúster para cambiar las credenciales de BMC.



Si establece credenciales de BMC durante una comprobación de estado, puede haber un retraso de hasta 2 minutos antes de que el cambio se refleje en la página **nodos**.

Opciones

Elija una de las siguientes opciones para cambiar las credenciales de BMC:

- [Utilice el control del cloud híbrido de NetApp para editar la información de BMC](#)
- [Use la API DE REST para editar información de BMC](#)

Utilice el control del cloud híbrido de NetApp para editar la información de BMC

Puede editar las credenciales de BMC almacenadas mediante la consola de Cloud Control de cloud híbrido de NetApp.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. En el cuadro azul de navegación izquierdo, seleccione la instalación de NetApp HCI.

Aparece la consola de control del cloud híbrido de NetApp.

4. En la navegación de la izquierda, haga clic en **Nodes**.
5. Para ver la información de inventario de computación, haga clic en **calcular**.

Se muestra una lista de los nodos de computación. La columna **BMC Connection Status** muestra el resultado de los intentos de conexión BMC para cada nodo de computación. Si el intento de conexión falla para un nodo de computación, se muestra un mensaje de error en esta columna para ese nodo.

6. Para agregar o editar las credenciales de BMC almacenadas para un nodo de computación con errores de conexión de BMC, haga clic en **Editar configuración de conexión** en el texto del mensaje de error.
7. En el cuadro de diálogo que aparece, agregue el nombre de usuario y la contraseña de administrador correctos para el BMC de este nodo de computación.
8. Haga clic en **Guardar**.
9. Repita los pasos 6 a 8 para cualquier nodo de computación que tenga credenciales de BMC almacenadas ausentes o incorrectas.



Al actualizar la información de BMC, se actualiza el inventario y se garantiza que los servicios del nodo de gestión conozcan todos los parámetros de hardware necesarios para completar la actualización.

Use la API DE REST para editar información de BMC

Puede editar las credenciales de BMC almacenadas mediante la API DE REST de NetApp Hybrid Cloud Control.

Pasos

1. Busque la etiqueta de hardware del nodo de computación y la información de BMC:
 - a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Haga clic en **autorizar** y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Haga clic en **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
- c. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /Installations**.
- d. Haga clic en **probar**.
- e. Haga clic en **Ejecutar**.
- f. Desde la respuesta, copie el ID del activo de instalación (`id`).
- g. En la interfaz de usuario DE LA API DE REST, haga clic en **GET /Installations/{id}**.
- h. Haga clic en **probar**.
- i. Pegue el ID de activo de instalación en el campo `id`.
- j. Haga clic en **Ejecutar**.
- k. Desde la respuesta, copie y guarde el ID de activo del nodo (`id`), Dirección IP del BMC (`bmcAddress`) y el número de serie del nodo (`chassisSerialNumber`) para usar en un paso posterior.

```
"nodes": [  
  {  
    "bmcDetails": {  
      "bmcAddress": "10.117.1.111",  
      "credentialsAvailable": false,  
      "credentialsValidated": false  
    },  
    "chassisSerialNumber": "221111019323",  
    "chassisSlot": "C",  
    "hardwareId": null,  
    "hardwareTag": "00000000-0000-0000-0000-ac1f6ab4ecf6",  
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
```

2. Abra la interfaz de usuario de API DE REST del servicio de hardware en el nodo de gestión:

```
https://<ManagementNodeIP>/hardware/2/
```

3. Haga clic en **autorizar** y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
 - c. Haga clic en **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
4. Haga clic en **PUT /Nodes/{hardware_id}**.
5. Haga clic en **probar**.

6. Introduzca el ID de activo de nodo que guardó anteriormente en la `hardware_id` parámetro.

7. Introduzca la siguiente información en la carga útil:

Parámetro	Descripción
<code>assetId</code>	El ID del activo de instalación (<code>id</code>) que guardó en el paso 1(f).
<code>bmcIp</code>	La dirección IP del BMC (<code>bmcAddress</code>) que guardó en el paso 1(k).
<code>bmcPassword</code>	Una contraseña actualizada para iniciar sesión en el BMC.
<code>bmcUsername</code>	Nombre de usuario actualizado para iniciar sesión en el BMC.
<code>serialNumber</code>	El número de serie del chasis del hardware.

Carga útil de ejemplo:

```
{
  "assetId": "7bb41e3c-2e9c-2151-b00a-8a9b49c0b0fe",
  "bmcIp": "10.117.1.111",
  "bmcPassword": "mypassword1",
  "bmcUsername": "admin1",
  "serialNumber": "221111019323"
}
```

8. Haga clic en **Ejecutar** para actualizar las credenciales del BMC. Un resultado satisfactorio devuelve una respuesta similar a la siguiente:

```
{
  "credentialid": "33333333-cccc-3333-cccc-333333333333",
  "host_name": "hci-host",
  "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
  "ip": "1.1.1.1",
  "parent": "abcd01y3-ab30-1ccc-11ee-11f123zx7d1b",
  "type": "BMC"
}
```

Obtenga más información

- ["Problemas conocidos y soluciones alternativas para actualizaciones de nodos de computación"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Supervise los volúmenes en el clúster de almacenamiento de

El sistema SolidFire aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que los clientes iSCSI o Fibre Channel acceden a través de la red. Es posible supervisar detalles sobre los grupos de acceso, las cuentas, los iniciadores, la capacidad utilizada, el estado de protección de datos de Snapshot, el número de sesiones iSCSI y la política de calidad de servicio asociada con el volumen.

También se pueden ver detalles sobre los volúmenes activos y eliminados.

Con esta vista, es posible que primero desee supervisar la columna capacidad utilizada.

Solo puede acceder a esta información si tiene privilegios administrativos de Hybrid Cloud Control de NetApp.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

`https://<ManagementNodeIP>`

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. En el cuadro azul de navegación izquierdo, seleccione la instalación de NetApp HCI.
Aparece la consola de control de cloud híbrido.
4. En la navegación de la izquierda, seleccione el clúster y seleccione **almacenamiento > volúmenes**.

ID ↑	Name	Account	Access Groups	Access	Used	Size	Snapshots	QoS Policy	Min IOPS	Max IOPS	Burst IOPS	iSCSI Sessions	Actions
1	NetApp-HCI-Datastore-01	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	4%	2.15 TB	0		50	15000	15000	2	⋮
2	NetApp-HCI-Datastore-02	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	0%	2.15 TB	0		50	15000	15000	2	⋮
3	NetApp-HCI-credential...			Read/Write	0%	5.37 GB	0		1000	2000	4000	1	⋮
4	NetApp-HCI-mnode-api			Read/Write	0%	53.69 GB	0		1000	2000	4000	1	⋮
5	NetApp-HCI-hci-monitor			Read/Write	0%	1.07 GB	0		1000	2000	4000	1	⋮

5. En la página Volumes, utilice las siguientes opciones:



- a. Filtre los resultados haciendo clic en el icono **filtro**.
- b. Oculte o muestre columnas haciendo clic en el icono **Ocultar/Mostrar**.
- c. Actualice los datos haciendo clic en el icono **Actualizar**.

- d. Descargue un archivo CSV haciendo clic en el icono **Descargar**.
6. Supervise la columna capacidad utilizada. Si se alcanzan los umbrales Advertencia, error o crítico, el color representa el estado de capacidad utilizada:
 - a. Advertencia - Amarillo
 - b. Error: Naranja
 - c. Crítico: Rojo
 7. En la vista Volumes, haga clic en las pestañas para ver detalles adicionales sobre los volúmenes:
 - a. **Grupos de acceso:** Puede ver los grupos de acceso de volúmenes que están asignados de iniciadores a una colección de volúmenes para un acceso seguro.

Consulte la información acerca de "[los grupos de acceso de volúmenes](#)".
 - b. **Cuentas:** Puede ver las cuentas de usuario, que permiten a los clientes conectarse a volúmenes en un nodo. Cuando crea un volumen, este se asigna a una cuenta de usuario específica.

Consulte la información acerca de "[Cuentas de usuario de NetApp HCI](#)".
 - c. **Initiators:** Puede ver el IQN del iniciador iSCSI o los WWPN de Fibre Channel para el volumen. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de contar con autenticación CHAP. Cada WWPN que se añade a un grupo de acceso habilita el acceso a la red de Fibre Channel a los volúmenes del grupo de acceso.
 - d. **Políticas de QoS:** Puede ver la política de QoS aplicada al volumen. Una política de calidad de servicio aplica ajustes estandarizados para IOPS mínimos, IOPS máximos y IOPS de ráfaga en varios volúmenes.

Consulte la información acerca de "[Políticas de rendimiento y calidad de servicio](#)".

Obtenga más información

- "[Documentación de SolidFire y Element](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"
- "[Página de recursos de NetApp HCI](#)"

Supervise el rendimiento, la capacidad y el estado del clúster con SolidFire Active IQ

Mediante SolidFire Active IQ, es posible supervisar los eventos, el rendimiento y la capacidad de los clústeres. Puede acceder a SolidFire Active IQ desde la consola de control del cloud híbrido de NetApp.

Antes de empezar

- Debe tener una cuenta de soporte de NetApp para poder aprovechar este servicio.
- Debe tener autorización para usar las API de REST de nodos de gestión.
- Un nodo de gestión se implementó con la versión 12.0 o posterior.
- La versión del clúster ejecuta el software NetApp Element 12.0 o una versión posterior.

- Tiene acceso a Internet. El servicio de recopilador Active IQ no se puede utilizar de sitios oscuros.

Acerca de esta tarea puede obtener vistas históricas actualizadas continuamente de estadísticas de todo el clúster. Puede configurar notificaciones para que le avisen de eventos, umbrales o métricas especificados en un clúster para que puedan abordarse rápidamente.

Como parte del contrato de soporte normal, el soporte de NetApp supervisa estos datos y alerta al usuario sobre los posibles problemas del sistema.

- Pasos*

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. En el panel de control, seleccione el menú de la parte superior derecha.
4. Seleccione **Ver Active IQ**.

La "[Consola de SolidFire Active IQ](#)" aparece.

5. Para obtener más información sobre SolidFire Active IQ, consulte "[Documentación de SolidFire Active IQ](#)".

También puede acceder a la documentación de SolidFire Active IQ desde el panel de control seleccionando el icono de menú en la parte superior derecha y seleccionando **Documentación**.

6. Desde la interfaz de SolidFire Active IQ, compruebe que los nodos de computación y de almacenamiento de NetApp HCI notifican correctamente en Active IQ:
 - a. Si tiene más de una instalación de NetApp HCI, seleccione **Seleccionar un clúster** y elija el clúster de la lista.
 - b. En el panel de navegación izquierdo, seleccione **Nodes**.
7. Si faltan un nodo o nodos en la lista, póngase en contacto con el soporte de NetApp.



Para ver el número de recursos de almacenamiento y computación, observe la consola de control del cloud híbrido (HCC). Consulte "[Supervise los recursos de almacenamiento y computación con la consola de HCC](#)".

Obtenga más información

- "[Documentación de SolidFire Active IQ de NetApp](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"
- "[Página de recursos de NetApp HCI](#)"

Recopile registros para solucionar problemas

Si tiene problemas con la instalación de su almacenamiento all-flash de NetApp HCI o SolidFire, puede recopilar registros para enviar al soporte de NetApp que le ayuden en el

diagnóstico. Es posible usar el control de cloud híbrido de NetApp o la API DE REST para recoger registros en sistemas NetApp HCI o Element.

Lo que necesitará

- Asegúrese de que la versión del clúster de almacenamiento ejecute la versión 11.3 o posterior del software NetApp Element.
- Asegúrese de haber implementado un nodo de gestión que ejecuta la versión 11.3 o una versión posterior.

Opciones de recopilación de registros

Seleccione una de las siguientes opciones:

- [Utilice el control del cloud híbrido de NetApp para recopilar registros](#)
- [Use la API DE REST para recoger registros](#)

Utilice el control del cloud híbrido de NetApp para recopilar registros

Puede acceder al área de recogida de registros desde la consola de Cloud Control híbrido de NetApp.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
3. En el panel de control, haga clic en el menú de la parte superior derecha.
4. Seleccione **recopilar registros**.

Aparecerá la página **registros de recopilación**. Si recogió los registros antes, puede descargar el paquete de registros existente o iniciar una nueva recopilación de registros.

5. Seleccione un intervalo de fechas en el menú desplegable **intervalo de fechas** para especificar las fechas que deben incluir los registros.

Si especifica una fecha de inicio personalizada, puede seleccionar la fecha para comenzar el rango de fechas. Los registros se recogerán a partir de esa fecha hasta la hora actual.

6. En la sección **Log Collection**, seleccione los tipos de archivos de registro que debe incluir el paquete de registro.

Para los registros de computación y de almacenamiento, puede ampliar la lista de nodos de computación o de almacenamiento, y seleccionar nodos individuales para recoger registros (o de todos los nodos de la lista).

7. Haga clic en **recopilar registros** para iniciar la recopilación de registros.

La recogida de registros se ejecuta en segundo plano y la página muestra el progreso.



Dependiendo de los registros que recoja, la barra de progreso puede permanecer en un porcentaje determinado durante varios minutos o avanzar muy lentamente en algunos puntos.

8. Haga clic en **Descargar registros** para descargar el paquete de registro.

Este paquete de registro está en un formato de archivo .tgz comprimido.

Use la API DE REST para recoger registros

Es posible usar la API DE REST para recoger registros de NetApp HCI o Element.

Pasos

1. Busque el ID del clúster de almacenamiento:

a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/logs/1/
```

b. Haga clic en **autorizar** y complete lo siguiente:

i. Introduzca el nombre de usuario y la contraseña del clúster.

ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.

iii. Haga clic en **autorizar** para iniciar una sesión.

2. Recopile registros de NetApp HCI o Element:

a. Haga clic en **POST /paquete**.

b. Haga clic en **probar**.

c. Cambie los valores de los siguientes parámetros en el campo **cuerpo de la solicitud** dependiendo del tipo de registros que necesite recopilar y del intervalo de tiempo:

Parámetro	Tipo	Descripción
<code>modifiedSince</code>	Cadena de fecha	Solo incluya los registros modificados después de esta fecha y hora. Por ejemplo, el valor "2020-07-14T20:19:00.000Z" define una fecha de inicio del 14 de julio de 2020 a las 20:19 UTC.
<code>computeLogs</code>	Booleano	Configure este parámetro en <code>true</code> para incluir los registros del nodo de computación.

Parámetro	Tipo	Descripción
computeIds	Cabina de UUID	Si computeLogs se establece en true, Rellene este parámetro con los Id. De activo de nodo de gestión de los nodos de computación para limitar la colección de registros a esos nodos de computación específicos. Utilice la GET <a href="https://<ManagementNodeIP>/logs/1/bundle/options">https://<ManagementNodeIP>/logs/1/bundle/options Extremo para ver todos los posibles ID de nodo que puede utilizar.
mnodeLogs	Booleano	Configure este parámetro en true para incluir los registros del nodo de gestión.
storageCrashDumps	Booleano	Configure este parámetro en true para incluir los registros de depuración de fallos del nodo de almacenamiento.
storageLogs	Booleano	Configure este parámetro en true para incluir los registros del nodo de almacenamiento.
storageNodeIds	Cabina de UUID	Si storageLogs se establece en true, Rellene este parámetro con los Id. De nodo del clúster de almacenamiento para limitar la colección de registros a esos nodos de almacenamiento específicos. Utilice la GET <a href="https://<ManagementNodeIP>/logs/1/bundle/options">https://<ManagementNodeIP>/logs/1/bundle/options Extremo para ver todos los posibles ID de nodo que puede utilizar.

- d. Haga clic en **Ejecutar** para iniciar la recopilación de registros. La respuesta debe devolver una respuesta similar a la siguiente:

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. Compruebe el estado de la tarea de recopilación de registros:
 - a. Haga clic en **GET /Bundle**.
 - b. Haga clic en **probar**.
 - c. Haga clic en **Ejecutar** para devolver un estado de la tarea de recopilación.
 - d. Desplácese hasta la parte inferior del cuerpo de respuesta.

Debería ver un `percentComplete` atributo que detalla el progreso de la colección. Si la colección está completa, el `downloadLink` atributo contiene el enlace de descarga completo, incluido el nombre de archivo del paquete de registro.

- e. Copie el nombre del archivo al final del `downloadLink` atributo.

4. Descargue el paquete de registro recopilado:

- a. Haga clic en **GET /Bundle/{filename}**.
 - b. Haga clic en **probar**.
 - c. Pegue el nombre de archivo que copió anteriormente en la `filename` campo de texto de parámetros.
 - d. Haga clic en **Ejecutar**.

Después de la ejecución, aparece un enlace de descarga en el área del cuerpo de respuesta.

- e. Haga clic en **Descargar archivo** y guarde el archivo resultante en el equipo.

Este paquete de registro está en un formato de archivo `.tgz` comprimido.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualice su sistema NetApp HCI versión 1.9 o 1.9P1

Información general sobre la secuencia de actualización

Es posible mantener actualizado el sistema NetApp HCI después de la puesta en marcha actualizando secuencialmente todos los componentes de software de NetApp HCI.

Estos componentes incluyen servicios de gestión, HealthTools, NetApp Hybrid Cloud Control, software Element, nodo de gestión, firmware de computación, controladores de computación, Y el plugin de Element para vCenter Server.



A partir del 2023 de noviembre, no puede iniciar una actualización de componente con control de nube híbrida de NetApp o API de REST porque los certificados de clave de firma (privados y públicos) caducaron el 5 de noviembre de 2023. Puede resolver este problema siguiendo la solución que se explica en el artículo de la base de conocimientos ["No se pueden iniciar las actualizaciones de SolidFire y HCI debido a un error de carga del paquete de actualización"](#).

La [secuencia de actualización del sistema](#) Contenido describe las tareas necesarias para completar una actualización del sistema NetApp HCI. Lo ideal es realizar estos procedimientos como parte de la secuencia de actualización más grande y no de forma aislada. Si es necesaria una actualización o actualización basada en componentes, consulte los requisitos previos del procedimiento para garantizar que se aborden complejidades adicionales.

La [Secuencia de actualización de vSphere](#) Incluir el contenido del plugin de Element para vCenter Server describe los pasos adicionales previos y posteriores a la actualización necesarios para volver a instalar el plugin de Element para vCenter Server.

Lo que necesitará

- Ejecuta el nodo de gestión 11.3 o una versión posterior. Las versiones más recientes del nodo de gestión tienen una arquitectura modular que proporciona servicios individuales.



Para comprobar la versión, inicie sesión en el nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión. Si no tiene 11.3, consulte ["Actualice su nodo de gestión"](#).

- Ha actualizado sus servicios de administración a al menos la versión 2.1.326.

Las actualizaciones con Hybrid Cloud Control de NetApp no están disponibles en versiones anteriores del paquete de servicio.

- Debe asegurarse de que la hora del sistema en todos los nodos esté sincronizada y que NTP esté correctamente configurado para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz de usuario web por nodo (`https://[IP address]:442`) sin fallos de clúster sin resolver relacionados con la desviación de tiempo.

secuencia de actualización del sistema

Puede usar la siguiente secuencia para actualizar el sistema NetApp HCI.

Pasos

1. ["Actualice los servicios de gestión de Hybrid Cloud Control"](#).



Si actualiza los servicios de gestión a la versión 2.16 o posterior y ejecuta un nodo de gestión de 11.3 a 11.8, deberá aumentar la RAM de la máquina virtual del nodo de gestión antes de actualizar los servicios de gestión.



Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element.

2. ["\(Opcional\) Actualice a la versión más reciente de HealthTools"](#).



Actualizar HealthTools solo es necesario si el nodo de gestión y el software Element que está ejecutando es 11.1 o anterior. HealthTools no es necesario para realizar actualizaciones de elementos mediante el control de cloud híbrido de NetApp.

3. ["Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento"](#).

4. ["Actualice el software Element y el firmware de almacenamiento"](#).

5. ["\(Opcional\) Actualice solo el firmware de almacenamiento de Element"](#).



Puede realizar esta tarea cuando haya una nueva actualización del firmware de almacenamiento disponible fuera de una versión principal.

6. ["\(Opcional\) Actualice el nodo de gestión"](#).



Ya no se necesita actualizar el sistema operativo del nodo de gestión para actualizar el software Element en el clúster de almacenamiento. Si el nodo de gestión es la versión 11.3 o posterior, solo tiene que actualizar los servicios de gestión a la versión más reciente para realizar actualizaciones de Element mediante el control de cloud híbrido de NetApp. Siga el procedimiento de actualización del nodo de gestión para su escenario si desea actualizar el sistema operativo del nodo de gestión por otros motivos, como la corrección de seguridad.

7. ["Actualice el plugin de Element para vCenter Server"](#).

8. ["Ejecute comprobaciones de estado del nodo de computación antes de actualizar el firmware de computación"](#).

9. ["Actualice las controladoras del nodo de computación"](#).

10. ["Actualice el firmware de su nodo de computación mediante NetApp Hybrid Cloud Control"](#) o. ["Automatice las actualizaciones del firmware informático con Ansible"](#).

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)
- ["Actualice un sistema de almacenamiento all-flash SolidFire de NetApp"](#)

Procedimientos de actualización del sistema

Actualice los servicios de gestión

Es posible actualizar los servicios de gestión a la versión de paquete más reciente después de haber instalado el nodo de gestión 11.3 o una versión posterior.

A partir del lanzamiento del nodo de gestión Element 11.3, el diseño del nodo de gestión se ha modificado en función de una nueva arquitectura modular que proporciona servicios individuales. Estos servicios modulares proporcionan funcionalidades de gestión centrales y ampliadas para los sistemas NetApp HCI. Los servicios de gestión incluyen servicios de telemetría, de registro y de actualización, el servicio QoSSIOC para el plugin de Element para vCenter Server, Cloud Control de NetApp, etc.

Acerca de esta tarea

- Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element.



- Los servicios de gestión 2.22.7 incluyen el plugin de Element para vCenter Server 5.0, que contiene el plugin remoto. Si usa el plugin de Element, debe actualizar a los servicios de gestión 2.22.7 o una versión posterior para cumplir con la directiva de VMware que elimina la compatibilidad con los plugins locales. ["Leer más"](#).
- Para obtener las notas de la versión de los servicios de gestión más recientes, en las que se describen servicios principales, funciones nuevas, correcciones de errores y soluciones alternativas para cada paquete de servicio, consulte ["las notas de la versión de los servicios de gestión"](#)

Lo que necesitará

A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el contrato de licencia de usuario final (CLUF) antes de utilizar la API o la interfaz de usuario de control de cloud híbrido de NetApp para actualizar los servicios de gestión:

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Los servicios de gestión se pueden actualizar con la interfaz de usuario de Hybrid Cloud Control de NetApp o la API DE REST del nodo de gestión:

- [Actualice los servicios de gestión con Hybrid Cloud Control](#) (Método recomendado)
- [Actualice los servicios de gestión mediante la API del nodo de gestión](#)

Actualice los servicios de gestión con Hybrid Cloud Control

Puede actualizar los servicios de gestión de NetApp mediante Hybrid Cloud Control de NetApp.

Los paquetes de servicios de gestión ofrecen funcionalidades y correcciones mejoradas para la instalación fuera de las versiones principales.

Antes de empezar

- Ejecuta el nodo de gestión 11.3 o una versión posterior.
- Si actualiza los servicios de gestión a la versión 2.16 o posterior y ejecuta un nodo de gestión de 11.3 a 11.8, deberá aumentar la RAM de la máquina virtual del nodo de gestión antes de actualizar los servicios de gestión:
 - a. Apague la máquina virtual del nodo de gestión.
 - b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de gestión.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Ha actualizado sus servicios de administración a al menos la versión 2.1.326. Las actualizaciones de control del cloud híbrido de NetApp no están disponibles en paquetes de servicio anteriores.



Para obtener una lista de los servicios disponibles para cada versión del paquete de servicio, consulte ["Notas de la versión de los servicios de gestión"](#).

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página actualizaciones, seleccione la ficha **Servicios de administración**.
5. Siga las instrucciones de la página para descargar y guardar un paquete de actualización de servicios de administración en su equipo.
6. Seleccione **examinar** para localizar el paquete que guardó y cargarlo.

Después de cargar el paquete, la actualización se inicia automáticamente.

Después de comenzar la actualización, puede ver el estado de la actualización en esta página. Durante la actualización, es posible que pierda la conexión con NetApp Hybrid Cloud Control y tenga que volver a iniciar sesión para ver los resultados de la actualización.

Actualice los servicios de gestión mediante la API del nodo de gestión

Los usuarios deberían llevar a cabo, idealmente, actualizaciones de los servicios de gestión desde el control del cloud híbrido de NetApp. Sin embargo, puede cargar, extraer y poner en marcha manualmente una actualización de paquete de servicio para los servicios de gestión en el nodo de gestión mediante la API DE REST. Puede ejecutar cada comando desde la interfaz de usuario de la API de REST para el nodo de gestión.

Antes de empezar

- Implementó un nodo de gestión de software de NetApp Element 11.3 o posterior.
- Si actualiza los servicios de gestión a la versión 2.16 o posterior y ejecuta un nodo de gestión de 11.3 a 11.8, deberá aumentar la RAM de la máquina virtual del nodo de gestión antes de actualizar los servicios de gestión:
 - a. Apague la máquina virtual del nodo de gestión.
 - b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de gestión.
- La versión del clúster ejecuta el software NetApp Element 11.3 o una versión posterior.
- Ha actualizado sus servicios de administración a al menos la versión 2.1.326. Las actualizaciones de control del cloud híbrido de NetApp no están disponibles en paquetes de servicio anteriores.



Para obtener una lista de los servicios disponibles para cada versión del paquete de servicio, consulte ["Notas de la versión de los servicios de gestión"](#).

Pasos

1. Abra la interfaz de usuario de API DE REST en el nodo de gestión: <https://<ManagementNodeIP>/mnode>
2. Seleccione **autorizar** y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
 - c. Seleccione **autorizar** para iniciar una sesión.
 - d. Cierre la ventana.
3. Cargue y extraiga el paquete de servicio en el nodo de gestión mediante este comando: `PUT /services/upload`
4. Ponga en marcha los servicios de gestión en el nodo de gestión: `PUT /services/deploy`
5. Supervise el estado de la actualización: `GET /services/update/status`

Una actualización correcta devuelve un resultado similar al siguiente ejemplo:

```
{
  "current_version": "2.10.29",
  "details": "Updated to version 2.17.52",
  "status": "success"
}
```

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualice a la versión más reciente de HealthTools

Antes de iniciar una actualización del almacenamiento de Element desde 11.1 o una versión anterior, debe actualizar el paquete HealthTools. Actualizar HealthTools solo es necesario si el nodo de gestión y el software Element que está ejecutando es 11.1 o anterior. HealthTools no es necesaria para ["Realizar actualizaciones de Element mediante el control de cloud híbrido de NetApp"](#).



El software Element 12.3.2 es la versión final que se puede actualizar a mediante NetApp HealthTools. Si ejecuta el software Element 11.3 o posterior, debe usar NetApp Hybrid Cloud Control para actualizar el software Element. Es posible actualizar las versiones de Element 11.1 o anteriores mediante NetApp HealthTools.

Lo que necesitará

- Este sistema ejecuta el nodo de gestión 11.0, 11.1 o posterior.
- Ha actualizado sus servicios de administración a al menos la versión 2.1.326.

Las actualizaciones de control de cloud híbrido de NetApp no están disponibles en versiones anteriores del paquete de servicio.

- Ha descargado la última versión de ["HealthTools"](#) y copió el archivo de instalación en el nodo de gestión.



Puede comprobar la versión instalada localmente de HealthTools ejecutando el `sfupdate-healthtools -v` comando.

- Para usar HealthTools con sitios oscuros, debe realizar estos pasos adicionales:
 - Descargar una ["Archivo JSON"](#) En el sitio de soporte de NetApp de un equipo que no es el nodo de gestión y cambie su nombre `metadata.json`.
 - Deje que el nodo de gestión esté activo y en funcionamiento en el sitio oscuro.

Acerca de esta tarea

Los comandos del conjunto HealthTools requieren privilegios escalados para ejecutarse. Cualquiera de los comandos de prefacio con `sudo` o bien, remita al usuario a privilegios de usuario raíz.



La versión de HealthTools que utilice podría estar más actualizada que la entrada de muestra y la respuesta que se muestra a continuación.

Pasos

1. Ejecute el `sfupdate-healthtools <path to install file>` Comando para instalar el nuevo software HealthTools.

Entrada de muestra:

```
sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
```

Respuesta de ejemplo:

```
Checking key signature for file /tmp/solidfirehealthtools-
2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. Ejecute el `sfupdate-healthtools -v` comando para comprobar que la versión instalada se ha actualizado.

Respuesta de ejemplo:

```
Currently installed version of HealthTools:
2020.03.01.09
```

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento

Debe ejecutar comprobaciones del estado antes de actualizar el almacenamiento Element para garantizar que todos los nodos de almacenamiento del clúster estén listos para la siguiente actualización de almacenamiento de Element.

Lo que necesitará

- **Servicios de administración:** Ha actualizado el último paquete de servicios de administración (2.10.27 o posterior).



Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element.

- **Nodo de gestión:** Está ejecutando el nodo de gestión 11.3 o posterior.
- **Software Element:** La versión del clúster ejecuta el software NetApp Element 11.3 o posterior.
- **Contrato de licencia para el usuario final (CLUF):** A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la IU o API de control de cloud híbrido de NetApp para ejecutar comprobaciones del estado del almacenamiento de Element:
 - a. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

- b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de comprobación del estado

Puede realizar comprobaciones del estado con la interfaz de usuario de control de cloud híbrido (HCC) de NetApp, la API de HCC o la suite HealthTools:

- [Utilice Cloud Control de NetApp híbrido para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento](#) (Método preferido)
- [Utilice API para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento](#)
- [Utilice HealthTools para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento](#)

También puede obtener más información sobre las comprobaciones del estado del almacenamiento que realiza el servicio:

- [Comprobaciones del estado del almacenamiento realizadas por el servicio](#)


Utilice Cloud Control de NetApp híbrido para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento

Con el control de cloud híbrido (HCC) de NetApp, puede verificar que un clúster de almacenamiento está listo para actualizarse.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione la ficha **almacenamiento**.
5. Seleccione la comprobación del estado  para el clúster que desea comprobar si está listo para la actualización.
6. En la página **Comprobación del estado del almacenamiento**, seleccione **Ejecutar comprobación del estado**.
7. Si hay problemas, haga lo siguiente:
 - a. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la

solución especificada.

- b. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente.
- c. Después de resolver los problemas del clúster, seleccione **Volver a ejecutar comprobación del estado**.

Una vez que la comprobación del estado se completa sin errores, el clúster de almacenamiento está listo para actualizar. Consulte actualización del nodo de almacenamiento ["instrucciones"](#) para continuar.

Utilice API para ejecutar comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento

Es posible utilizar API DE REST para verificar que un clúster de almacenamiento esté listo para actualizarse. La comprobación del estado verifica que no hay obstáculos para la actualización, como los nodos pendientes, los problemas de espacio en disco y los fallos del clúster.

Pasos

1. Busque el ID del clúster de almacenamiento:
 - a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/mnode
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
 - c. En la interfaz de usuario de API de REST, seleccione `GET /assets`.
 - d. Seleccione **probar**.
 - e. Seleccione **Ejecutar**.
 - f. De la respuesta, copie la `"id"` desde la `"storage"` sección del clúster que pretende comprobar si está listo para la actualización.



No utilice la `"parent"` Valor de esta sección porque éste es el ID del nodo de administración, no el ID del clúster de almacenamiento.

```
"config": {},
"credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",
"host_name": "SF_DEMO",
"iid": "12cc3a45-e6e7-8d91-a2bb-0bdb3456b789",
"ip": "10.123.12.12",
"parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",
"sshcredentialid": null,
"ssl_certificate": null
```

2. Ejecute las comprobaciones del estado en el clúster de almacenamiento:

- a. Abra la interfaz de usuario de API DE REST de almacenamiento en el nodo de gestión:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
- ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
- iii. Seleccione **autorizar** para iniciar una sesión.
- iv. Cierre la ventana de autorización.

- c. Seleccione **POST /Health-checks**.

- d. Seleccione **probar**.

- e. En el campo Parameter, introduzca el ID del clúster de almacenamiento obtenido en el paso 1.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

- f. Seleccione **Ejecutar** para ejecutar una comprobación del estado en el clúster de almacenamiento especificado.

La respuesta debe indicar el estado como `initializing`:

```

{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}

```

- a. Copie el `healthCheckID` eso es parte de la respuesta.
3. Compruebe los resultados de las comprobaciones de estado:
 - a. Seleccione **GET /Health-checks/{healthCheckId}**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de comprobación del estado en el campo parámetro.
 - d. Seleccione **Ejecutar**.
 - e. Desplácese hasta la parte inferior del cuerpo de respuesta.

Si todas las comprobaciones del estado se realizan correctamente, la devolución es similar al ejemplo siguiente:

```

"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"

```

4. Si la `message` return indica que se han producido problemas con el estado del clúster, haga lo siguiente:
 - a. Seleccione **GET /Health-checks/{healthCheckId}/log**
 - b. Seleccione **probar**.
 - c. Introduzca el ID de comprobación del estado en el campo parámetro.
 - d. Seleccione **Ejecutar**.
 - e. Revise cualquier error específico y obtenga los enlaces asociados del artículo de la base de conocimientos.
 - f. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la

solución especificada.

- g. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente.
- h. Después de resolver los problemas del clúster, ejecute **GET /health-checks/{healthCheckId}/log** de nuevo.

Utilice HealthTools para ejecutar comprobaciones del estado del almacenamiento Element antes de actualizar el almacenamiento

Puede verificar que el clúster de almacenamiento esté listo para actualizar mediante el `sfupgradecheck` comando. Este comando verifica información como nodos pendientes, espacio de disco y fallos de clúster.

Si el nodo de gestión se encuentra en un sitio oscuro sin conectividad externa, la comprobación de preparación para la actualización necesita el `metadata.json` archivo descargado durante "[Actualizaciones de HealthTools](#)" para funcionar correctamente.

Acerca de esta tarea

Este procedimiento describe cómo tratar las comprobaciones de actualización que generan uno de los siguientes resultados:

- Ejecutando el `sfupgradecheck` el comando se ejecuta correctamente. Su clúster está listo para la actualización.
- Comprobaciones dentro de `sfupgradecheck` la herramienta falla con un mensaje de error. Su clúster no está listo para la actualización y se requieren pasos adicionales.
- Se produce un error en la comprobación de actualización porque HealthTools no está actualizado.
- Se produce un error en la comprobación de la actualización porque el nodo de gestión está en un sitio oscuro.

Pasos

1. Ejecute el `sfupgradecheck` comando:

```
sfupgradecheck -u <cluster-user-name> MVIP
```



Para las contraseñas que contienen caracteres especiales, añada una barra diagonal inversa (\) antes de cada carácter especial. Por ejemplo: `mypass!@1` debe introducirse como `mypass!\!@.`

Comando de entrada de muestra con salida de muestra en la que no aparecen errores y está listo para la actualización:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/kallA00000081tOQQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/kallA00000081tTQQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/kallA00000081tYQQAQ/mNodeconnecti
vity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. Si hay errores, se requieren acciones adicionales. Consulte las siguientes subsecciones para obtener detalles.

Su clúster no está listo para la actualización

Si ve un mensaje de error relacionado con una de las comprobaciones del estado, siga estos pasos:

1. Revise la `sfupgradcheck` mensaje de error.

Respuesta de ejemplo:

The following tests failed:

check_root_disk_space:

Test Description: Verify node root directory has at least 12 GBs of available disk space

Severity: ERROR

Failed node IDs: 2

Remedy: Remove unneeded files from root drive

More information:

<https://kb.netapp.com/support/s/article/ka11A00000081tTQAQ/SolidFire-Disk-space-error>

check_pending_nodes:

Test Description: Verify no pending nodes in cluster

More information:

<https://kb.netapp.com/support/s/article/ka11A00000081tOQAQ/pendingnodes>

check_cluster_faults:

Test Description: Report any cluster faults

check_root_disk_space:

Test Description: Verify node root directory has at least 12 GBs of available disk space

Passed node IDs: 1, 3

More information:

<https://kb.netapp.com/support/s/article/ka11A00000081tTQAQ/SolidFire-Disk-space-error>

check_mnode_connectivity:

Test Description: Verify storage nodes can communicate with management node

Passed node IDs: 1, 2, 3

More information:

<https://kb.netapp.com/support/s/article/ka11A00000081tYQAQ/mNodeconnectivity>

check_files:

Test Description: Verify options file exists

Passed node IDs: 1, 2, 3

check_cores:

Test Description: Verify no core or dump files exists

Passed node IDs: 1, 2, 3

check_upload_speed:

Test Description: Measure the upload speed between the storage node and the management node

Node ID: 1 Upload speed: 86518.82 KBs/sec

Node ID: 3 Upload speed: 84112.79 KBs/sec

Node ID: 2 Upload speed: 93498.94 KBs/sec

En este ejemplo, el nodo 1 tiene poco espacio en disco. Puede encontrar más información en la "[base de conocimientos](#)" (KB) artículo incluido en el mensaje de error.

HealthTools está desfasada

Si aparece un mensaje de error que indica que HealthTools no es la última versión, siga estas instrucciones:

1. Revise el mensaje de error y tenga en cuenta que la comprobación de actualización falla.

Respuesta de ejemplo:

```
sfupgradecheck failed: HealthTools is out of date:
installed version: 2018.02.01.200
latest version: 2020.03.01.09.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/
Or rerun with the -n option
```

2. Siga las instrucciones descritas en la respuesta.

Su nodo de gestión está en un sitio oscuro

1. Revise el mensaje y tenga en cuenta que la comprobación de actualización falla:

Respuesta de ejemplo:

```
sfupgradecheck failed: Unable to verify latest available version of
healthtools.
```

2. Descargar una ["Archivo JSON"](#) En el sitio de soporte de NetApp de un equipo que no es el nodo de gestión y cambie su nombre `metadata.json`.
3. Ejecute el siguiente comando:

```
sfupgradecheck -l --metadata=<path-to-metadata-json>
```

4. Para obtener información detallada, consulte adicional ["Actualizaciones de HealthTools"](#) información para sitios oscuros.
5. Compruebe que el conjunto HealthTools está actualizado ejecutando el siguiente comando:

```
sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
```

Comprobaciones del estado del almacenamiento realizadas por el servicio

Las comprobaciones del estado del almacenamiento realizan las siguientes comprobaciones por clúster.

Nombre de comprobación	Nodo/clúster	Descripción
check_async_results	Clúster	Verifica que el número de resultados asincrónicos en la base de datos está por debajo de un número de umbral.
check_cluster_errantes	Clúster	Comprueba que no hay errores del clúster de bloqueo de actualizaciones (tal y como se define en el origen de elementos).
compruebe_upload_speed	Nodo	Mide la velocidad de carga entre el nodo de almacenamiento y el nodo de gestión.
comprobación_velocidad_conexión	Nodo	Verifica que los nodos tienen conectividad con el nodo de gestión que sirve paquetes de actualización y realiza una estimación de la velocidad de conexión.
comprobar_núcleos	Nodo	Comprueba si hay volcado de bloqueo del kernel y archivos principales en el nodo. Se produce un error en la comprobación de cualquier bloqueo en un período de tiempo reciente (umbral de 7 días).
check_root_disk_space	Nodo	Verifica que el sistema de archivos raíz tiene suficiente espacio libre para realizar una actualización.
check_var_log_disk_space	Nodo	Lo verifica <code>/var/log</code> el espacio libre cumple con algún umbral de porcentaje libre. Si no lo hace, la comprobación girará y purgará los registros más antiguos para caer por debajo del umbral. La comprobación falla si no se puede crear suficiente espacio libre.
check_pending_nodes	Clúster	Verifica que no hay nodos pendientes en el clúster.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualice el software Element

Para actualizar el software NetApp Element, puede usar la interfaz de usuario de control de cloud híbrido de NetApp, la API DE REST o la suite de herramientas HealthTools. Ciertas operaciones se eliminan durante una actualización del software Element, como

añadir y quitar nodos, añadir y quitar unidades, y comandos asociados con iniciadores, grupos de acceso de volúmenes y redes virtuales, entre otros.

Lo que necesitará

- **Privilegios de administrador:** Dispone de permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Ruta de actualización válida:** Ha comprobado la información de ruta de actualización para la versión de elemento a la que está actualizando y ha comprobado que la ruta de actualización es válida. [https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Software/What_is_the_upgrade_matrix_for_storage_clusters_running_NetApp_Element_software%3F\[\"Base de conocimientos de NetApp: Matriz de actualización para clústeres de almacenamiento que ejecutan software NetApp Element\"\]](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Software/What_is_the_upgrade_matrix_for_storage_clusters_running_NetApp_Element_software%3F[\)
- **Sincronización de hora del sistema:** Se ha asegurado de que la hora del sistema en todos los nodos está sincronizada y que NTP está correctamente configurado para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz de usuario web por nodo ([https://\[IP address\]:442](https://[IP address]:442)) sin fallos de clúster sin resolver relacionados con la desviación de tiempo.
- **Puertos del sistema:** Si utiliza NetApp Hybrid Cloud Control para actualizaciones, se ha asegurado de que los puertos necesarios están abiertos. Consulte [\"Puertos de red\"](#) si quiere más información.
- **Nodo de gestión:** Para la API e IU de control de cloud híbrido de NetApp, el nodo de gestión de su entorno ejecuta la versión 11.3.
- **Servicios de administración:** Ha actualizado su paquete de servicios de administración a la última versión.



Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el software Element a la versión 12.3.x. Si actualiza el software Element a la versión 12.3.x, necesita servicios de gestión 2.14.60 o posterior para continuar.

- **Estado del clúster:** Ha comprobado que el clúster está listo para actualizarse. Consulte [\"Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento\"](#).
- **BMC actualizado para nodos H610S:** Ha actualizado la versión de BMC para los nodos H610S. Consulte [\"notas de la versión e instrucciones de actualización\"](#).
- **Contrato de licencia para el usuario final (CLUF):** A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la IU o la API de control de cloud híbrido de NetApp para actualizar el software Element:

- a. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

- b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Elija una de las siguientes opciones de actualización del software Element:

- Utilice la IU de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element
- Utilice la API de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element
- Actualice el software Element en sitios conectados mediante HealthTools
- Actualice el software Element en sitios oscuros mediante HealthTools



Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, deberá realizar pasos de actualización adicionales ([fase 2](#)) para cada nodo de almacenamiento. Si ejecuta Element 11.8 o una versión posterior, no será necesario realizar los pasos de actualización adicionales (fase 2).

Utilice la IU de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element

Con la interfaz de usuario de Cloud Control de NetApp, puede actualizar un clúster de almacenamiento.



Para obtener problemas potenciales al actualizar los clústeres de almacenamiento con NetApp Hybrid Cloud Control y sus soluciones alternativas, consulte "[Artículo de base de conocimientos](#)".



En el caso de las plataformas que no H610S, el proceso de actualización tarda aproximadamente 30 minutos por nodo.

Pasos




1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione **almacenamiento**.

La ficha **almacenamiento** muestra los clústeres de almacenamiento que forman parte de la instalación. Si el control de cloud híbrido de NetApp no permite acceder a un clúster, no se mostrará en la página **actualizaciones**.

5. Elija una de las siguientes opciones y realice el conjunto de pasos que se aplican a su clúster:

Opción	Pasos
<p>Todos los clústeres que ejecutan Element 11.8 y versiones posteriores</p>	<p>a. Seleccione examinar para cargar el paquete de actualización que ha descargado.</p> <p>b. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga.</p> <div data-bbox="922 373 976 428" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 352 1430 449" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>La carga del archivo se perderá si se desplaza fuera de la ventana del explorador.</p> </div> <p>Se muestra un mensaje en pantalla después de que el archivo se haya cargado y validado correctamente. La validación puede tardar varios minutos. Si se aleja de la ventana del explorador en este momento, se conserva la carga del archivo.</p> <p>c. Seleccione Iniciar actualización.</p> <div data-bbox="922 940 976 995" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 814 1455 1115" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>Estado de actualización cambia durante la actualización para reflejar el estado del proceso. También cambia en respuesta a las acciones que realice, como la pausa de la actualización o si la actualización devuelve un error. Consulte Cambios de estado de actualización.</p> </div> <div data-bbox="922 1339 976 1394" style="display: inline-block; vertical-align: middle; margin-top: 20px;">  </div> <div data-bbox="1036 1171 1446 1549" style="display: inline-block; vertical-align: middle; margin-left: 10px; margin-top: 20px;"> <p>Mientras la actualización está en curso, puede salir de la página y volver a ella más tarde para continuar supervisando el progreso. La página no actualiza el estado ni la versión actual de forma dinámica si la fila del clúster está contraída. La fila del clúster debe estar ampliada para actualizar la tabla, o bien se puede actualizar la página.</p> </div> <p>Es posible descargar registros una vez completada la actualización.</p>

Opción	Pasos
Actualice un clúster de H610S que ejecuta la versión de Element anterior a 11.8.	<p>a. Seleccione la flecha desplegable junto al clúster que desea actualizar y seleccione una de las versiones de actualización disponibles.</p> <p>b. Seleccione Iniciar actualización. Una vez finalizada la actualización, la interfaz de usuario le solicita que realice la fase 2 del proceso.</p> <p>c. Complete los pasos adicionales necesarios (fase 2) en la "Artículo de base de conocimientos", Y reconocer en la interfaz de usuario que ha completado la fase 2.</p> <p>Es posible descargar registros una vez completada la actualización. Para obtener más información sobre los distintos cambios de estado de actualización, consulte Cambios de estado de actualización.</p>

Cambios de estado de actualización

Estos son los diferentes estados que muestra la columna **Estado de actualización** de la interfaz de usuario antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
Actualizado	El clúster se actualizó a la versión de Element más reciente disponible.
Versiones disponibles	Hay disponibles versiones más recientes del firmware de almacenamiento o Element para su actualización.
En curso	La actualización está en curso. Una barra de progreso muestra el estado de la actualización. Los mensajes en pantalla también muestran los errores a nivel de nodo y muestran el ID de nodo de cada nodo del clúster a medida que avanza la actualización. Es posible supervisar el estado de cada nodo mediante la interfaz de usuario de Element o el plugin de NetApp Element para la interfaz de usuario de vCenter Server.
Actualice la pausa	Puede optar por poner en pausa la actualización. En función del estado del proceso de actualización, la operación de pausa puede realizarse correctamente o fallará. Verá un aviso de la interfaz de usuario que le solicita que confirme la operación de pausa. Para garantizar que el clúster esté en un lugar seguro antes de pausar una actualización, la operación de actualización puede tardar hasta dos horas en detenerse por completo. Para reanudar la actualización, seleccione Reanudar .

Estado de actualización	Descripción
En pausa	Colocó en pausa la actualización. Seleccione Reanudar para reanudar el proceso.
Error	Se produjo un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp. Después de resolver el error, puede volver a la página y seleccionar Reanudar . Al reanudar la actualización, la barra de progreso se retrocede durante unos minutos mientras el sistema ejecuta la comprobación del estado y comprueba el estado actual de la actualización.
Completo con seguimiento	Solo para actualizar los nodos H610S desde una versión de Element anterior a 11.8. Una vez completada la fase 1 del proceso de actualización, este estado le pedirá que realice la fase 2 de la actualización (consulte la " Artículo de base de conocimientos "). Después de completar la fase 2 y confirmar que la ha completado, el estado cambia a hasta la fecha .

Utilice la API de control de cloud híbrido de NetApp para actualizar el almacenamiento de Element

Puede utilizar las API para actualizar los nodos de almacenamiento de un clúster a la versión más reciente del software Element. Puede utilizar una herramienta de automatización que prefiera para ejecutar las API. El flujo de trabajo de API que se documenta aquí, utiliza la interfaz de usuario de API DE REST disponible en el nodo de gestión como ejemplo.

Pasos

1. Descargue el paquete de actualización de almacenamiento en un dispositivo al que se pueda acceder el nodo de gestión; vaya al software NetApp HCI "[descargas](#)" y descargue la imagen del nodo de almacenamiento más reciente.
2. Cargue el paquete de actualización de almacenamiento en el nodo de gestión:
 - a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
- c. En la interfaz de usuario DE LA API DE REST, seleccione **POST /packages**.
- d. Seleccione **probar**.
- e. Seleccione **Browse** y seleccione el paquete de actualización.
- f. Seleccione **Ejecutar** para iniciar la carga.

- g. Desde la respuesta, copie y guarde el ID del paquete ("id") para usar en un paso posterior.
3. Compruebe el estado de la carga.
- a. En la interfaz de usuario de la API DE REST, seleccione **GET /packages/{id}/status**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de paquete que ha copiado en el paso anterior en **id**.
 - d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

La respuesta indica `state` como `SUCCESS` cuando finalice.

4. Busque el ID del clúster de almacenamiento:
- a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
 - c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
 - d. Seleccione **probar**.
 - e. Seleccione **Ejecutar**.
 - f. Desde la respuesta, copie el ID del activo de instalación ("id").
 - g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.
 - h. Seleccione **probar**.
 - i. Pegue el ID de activo de instalación en el campo **id**.
 - j. Seleccione **Ejecutar**.
 - k. En la respuesta, copie y guarde el ID del clúster de almacenamiento ("id") del clúster que desee actualizar para usarlo en un paso posterior.
5. Ejecute la actualización del almacenamiento:
- a. Abra la interfaz de usuario de API DE REST de almacenamiento en el nodo de gestión:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.

- iv. Cierre la ventana de autorización.
- c. Seleccione **POST /upgrades**.
- d. Seleccione **probar**.
- e. Introduzca el ID del paquete de actualización en el campo parámetro.
- f. Introduzca el ID del clúster de almacenamiento en el campo parámetro.

La carga útil debe tener un aspecto similar al siguiente ejemplo:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

- g. Seleccione **Ejecutar** para iniciar la actualización.

La respuesta debe indicar el estado como `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1",
    "log": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-b3fc-2c963f66abc1/log"
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ]
  }
}
```

```

    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}

```

- a. Copie el ID de actualización ("upgradeId") eso es parte de la respuesta.
6. Verifique el progreso y los resultados de la actualización:
- a. Seleccione **GET /upgrades/{actualizeld}**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**.
 - d. Seleccione **Ejecutar**.
 - e. Realice una de las siguientes acciones si existen problemas o requisitos especiales durante la actualización:

Opción	Pasos
<p>Debe corregir los problemas de estado del clúster debido a <code>failedHealthChecks</code> mensaje en el cuerpo de respuesta.</p>	<ol style="list-style-type: none"> i. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la solución especificada. ii. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente. iii. Después de resolver los problemas del clúster, vuelva a autenticarse si es necesario y seleccione PONER /actualizaciones/{actualizable Id}. iv. Seleccione probar. v. Introduzca el ID de actualización desde el paso anterior en Actualizar Id. vi. Introduzca <code>"action": "resume"</code> en el cuerpo de la solicitud. <div data-bbox="914 785 1487 963" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <pre>{ "action": "resume" }</pre> </div> vii. Seleccione Ejecutar.
<p>Debe pausar la actualización porque la ventana de mantenimiento se está cerrando o por otro motivo.</p>	<ol style="list-style-type: none"> i. Vuelva a autenticarse si es necesario y seleccione PONER /actualizaciones/{actualizeld}. ii. Seleccione probar. iii. Introduzca el ID de actualización desde el paso anterior en Actualizar Id. iv. Introduzca <code>"action": "pause"</code> en el cuerpo de la solicitud. <div data-bbox="914 1436 1487 1614" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <pre>{ "action": "pause" }</pre> </div> v. Seleccione Ejecutar.

Opción	Pasos
Si va a actualizar un clúster de H610S que ejecuta una versión de Element anterior a 11.8, consulte el estado <code>finishedNeedsAck</code> en el cuerpo de respuesta. Debe realizar pasos de actualización adicionales (fase 2) para cada nodo de almacenamiento H610S.	<p>i. Consulte [Upgrading H610S storage nodes to Element 12.3.x or later (phase 2)] y complete el proceso de cada nodo.</p> <p>ii. Vuelva a autenticarse si es necesario y seleccione PONER <code>/actualizaciones/{actualizeld}</code>.</p> <p>iii. Seleccione probar.</p> <p>iv. Introduzca el ID de actualización desde el paso anterior en Actualizar Id.</p> <p>v. Introduzca <code>"action": "acknowledge"</code> en el cuerpo de la solicitud.</p> <pre style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;">{ "action": "acknowledge" }</pre> <p>vi. Seleccione Ejecutar.</p>

- f. Ejecute la API **GET** `/upgrades/{actualizable Id}` varias veces, según sea necesario, hasta que el proceso se complete.

Durante la actualización, el `status` lo que indica `running` si no se encuentra ningún error. Cuando cada nodo se actualiza, el `step` el valor cambia a `NodeFinished`.

La actualización se completó correctamente cuando el `percent` el valor es 100 y la `state` lo que indica `finished`.

¿Qué ocurre si se produce un error en una actualización mediante el control del cloud híbrido de NetApp

Si se produce un error en una unidad o un nodo durante una actualización, la interfaz de usuario de Element mostrará errores en el clúster. El proceso de actualización no pasa al siguiente nodo y espera a que se resuelvan los errores del clúster. La barra de progreso de la interfaz de usuario de muestra que la actualización está esperando a que se resuelvan los errores del clúster. En esta fase, la selección de **Pausa** en la interfaz de usuario no funcionará, ya que la actualización espera a que el clúster esté en buen estado. Deberá ponerse en contacto con el servicio de soporte de NetApp para que le ayude con la investigación de un fallo.

El control del cloud híbrido de NetApp tiene un periodo de espera predefinido de tres horas, durante el cual puede suceder una de las siguientes situaciones:

- Los fallos del clúster se resuelven en el plazo de tres horas y se reanuda la actualización. No es necesario realizar ninguna acción en este escenario.
- El problema persiste después de tres horas y el estado de actualización muestra **error** con un banner rojo. Puede reanudar la actualización seleccionando **Reanudar** después de resolver el problema.
- El soporte de NetApp ha determinado que se debe cancelar temporalmente el proceso de actualización

para que pueda tomar medidas correctivas antes del plazo de tres horas. El equipo de soporte utilizará la API para cancelar la actualización.



Si se cancela la actualización del clúster mientras se actualiza un nodo, es posible que las unidades se eliminen sin dignidad del nodo. Si las unidades se quitan sin gracia, el soporte de NetApp deberá volver a añadir las unidades durante la actualización. Es posible que el nodo tarde más en realizar actualizaciones de firmware o actividades de sincronización posteriores a la actualización. Si el progreso de la actualización parece estancado, póngase en contacto con el soporte de NetApp para obtener ayuda.

Actualice el software Element en sitios conectados mediante HealthTools

Pasos

1. Descargue el paquete de actualización del almacenamiento; vaya al software NetApp HCI "[descargas](#)" descargue la imagen del nodo de almacenamiento más reciente en un dispositivo que no sea el nodo de gestión.



Es necesario contar con la versión más reciente de HealthTools para actualizar el software de almacenamiento Element.

2. Copie el archivo ISO en el nodo de gestión en una ubicación accesible como /tmp.

Cuando cargue el archivo ISO, asegúrese de que el nombre del archivo no cambia; de lo contrario, se producirá un error en los pasos posteriores.

3. **Opcional:** Descargue el ISO del nodo de gestión a los nodos del clúster antes de la actualización.

Con este paso se reduce el tiempo de actualización, ya que se preconfigurando la ISO en los nodos de almacenamiento y se ejecutan comprobaciones internas adicionales para garantizar que el clúster tenga un estado adecuado que actualizar. Si realiza esta operación, el clúster no pondrá en modo "actualización" ni restringirá ninguna de las operaciones del clúster.

```
sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
```



Omita la contraseña de la línea de comandos para permitir `sfinstall` para solicitar la información. Para las contraseñas que contienen caracteres especiales, añada una barra diagonal inversa (\) antes de cada carácter especial. Por ejemplo: `mypass!@1` debe introducirse como `mypass!\!@`.

Ejemplo Consulte la siguiente entrada de ejemplo:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso  
--stage
```

El resultado de la muestra que `sfinstall` intenta verificar si una versión más reciente de `sfinstall` está disponible:

```
sfindall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfindall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

Consulte el siguiente extracto de muestra de una operación previa a la etapa correcta:



Cuando finalice la estadificación, se mostrará el mensaje Storage Node Upgrade Staging Successful tras el evento de actualización.

```
flabv0004 ~ # sfindall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfindall Release Version: 2019.01.01.49 Management
Node Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816,
nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2]
(1 of 4 nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command
without the --stage option to start the upgrade.
```

Los ISO preconfigurados se eliminarán automáticamente una vez que finalice la actualización. Sin embargo, si la actualización no se ha iniciado y necesita ser reprogramada, los ISOs pueden ser despreconfigurados manualmente usando el comando:

```
sfindall <MVIP> -u <cluster_username> --destage
```

Una vez iniciada la actualización, la opción de dejar de estar disponible.

4. Inicie la actualización con el `sinstall` Comando y la ruta al archivo ISO:

```
sinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>
```

ejemplo

Consulte el siguiente comando de entrada de ejemplo:

```
sinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-11.0.0.345.iso
```

El resultado de la muestra que `sinstall` intenta verificar si una versión más reciente de `sinstall` está disponible:

```
sinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-11.0.0.345.iso
2018-10-01 16:52:15: Newer version of sinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip-version-check
```

Consulte el siguiente extracto de ejemplo de una actualización correcta. Los eventos de actualización pueden utilizarse para supervisar el progreso de la actualización.

```
# sinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
2018-10-11 18:28
Checking connectivity to MVIP 10.117.0.161
Checking connectivity to node 10.117.0.23
Checking connectivity to node 10.117.0.24
...
Successfully connected to cluster and all nodes
#####
You are about to start a new upgrade
10.117.0.161
10.3.0.161
solidfire-rtfi-sodium-11.0.0.761.iso
Nodes:
10.117.0.23 nlabp1023 SF3010 10.3.0.161
10.117.0.24 nlabp1025 SF3010 10.3.0.161
10.117.0.26 nlabp1027 SF3010 10.3.0.161
10.117.0.28 nlabp1028 SF3010 10.3.0.161
#####
Do you want to continue? ['Yes', 'No']: yes
```



```

...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7]
to new ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check

```



Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, deberá realizar pasos de actualización adicionales ([fase 2](#)) para cada nodo de almacenamiento. Si ejecuta Element 11.8 o una versión posterior, no será necesario realizar los pasos de actualización adicionales (fase 2).

Actualice el software Element en sitios oscuros mediante HealthTools

Puede utilizar el conjunto de herramientas HealthTools para actualizar el software NetApp Element en un sitio oscuro que no tiene conectividad externa.

Lo que necesitará

1. Vaya al software NetApp HCI "[descargas](#)".
2. Seleccione la versión de software correcta y descargue la imagen del nodo de almacenamiento más reciente en un equipo que no es el nodo de gestión.



Es necesario contar con la versión más reciente de HealthTools para actualizar el software de almacenamiento Element.

3. Descargue esto "[Archivo JSON](#)" En el sitio de soporte de NetApp de un equipo que no es el nodo de gestión y cambie su nombre `metadata.json`.
4. Copie el archivo ISO en el nodo de gestión en una ubicación accesible, como `/tmp`.



Puede hacerlo utilizando, por ejemplo, SCP. Cuando cargue el archivo ISO, asegúrese de que el nombre del archivo no cambia; de lo contrario, se producirá un error en los pasos posteriores.

Pasos

1. Ejecute el `sfupdate-healthtools` comando:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Compruebe la versión instalada:

```
sfupdate-healthtools -v
```

3. Compruebe la versión más reciente con respecto al archivo JSON de metadatos:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Asegúrese de que el clúster esté listo:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP  
--metadata=<path-to-metadata-json>
```

5. Ejecute el `sfinstall` Comando con la ruta al archivo ISO y al archivo JSON de metadatos:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO>  
--metadata=<path-to-metadata-json-file>
```

Consulte el siguiente comando de entrada de ejemplo:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso  
--metadata=/tmp/metadata.json
```

Opcional puede añadir el `--stage` marcar con la `sfinstall` comando para preconfigurar la actualización por adelantado.



Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, deberá realizar pasos de actualización adicionales ([fase 2](#)) para cada nodo de almacenamiento. Si ejecuta Element 11.8 o una versión posterior, no será necesario realizar los pasos de actualización adicionales (fase 2).

Qué ocurre si se produce un error en una actualización mediante HealthTools

Si la actualización del software falla, puede pausar la actualización.



Solo debe pausar una actualización con Ctrl-C. Esto permite que el sistema se limpie a sí mismo.

Cuando `sinstall` espera a que se borren los fallos del clúster y si algún fallo provoca que se mantengan, `sinstall` no continuará al siguiente nodo.

Pasos

1. Debe parar `sinstall` Con Ctrl+C.
2. Póngase en contacto con el soporte de NetApp para recibir ayuda con la investigación de fallo.
3. Reanude la actualización con el mismo `sinstall` comando.
4. Cuando una actualización se detiene con Ctrl+C, si la actualización se encuentra actualizando un nodo, elija una de las siguientes opciones:
 - **Wait:** Permita que el nodo que está actualizando finalice antes de restablecer las constantes del clúster.
 - **Continuar:** Continuar la actualización, que cancela la pausa.
 - **Anular:** Restablece las constantes del clúster y anula la actualización inmediatamente.



Si se cancela la actualización del clúster mientras se actualiza un nodo, es posible que las unidades se eliminen sin dignidad del nodo. Si las unidades se quitan sin gracia, el soporte de NetApp deberá volver a añadir las unidades durante la actualización. Es posible que el nodo tarde más en realizar actualizaciones de firmware o actividades de sincronización posteriores a la actualización. Si el progreso de la actualización parece estancado, póngase en contacto con el soporte de NetApp para obtener ayuda.

Actualizar los nodos de almacenamiento H610S a Element 12.3.x (fase 2)

Si va a actualizar un nodo serie H610S a Element 12.3.x y el nodo ejecuta una versión de Element anterior a 11.8, el proceso de actualización implica dos fases.

La fase 1, que se realiza primero, sigue los mismos pasos que la actualización estándar al proceso de Element 12.3.x. Instala el software Element y todas las actualizaciones de firmware de la versión 5 de forma gradual a través del clúster, nodo por nodo. Debido a la carga útil del firmware, se estima que el proceso tardará aproximadamente de 1.5 a 2 horas por nodo H610S, incluido un único ciclo de arranque en frío al final de la actualización de cada nodo.

La fase 2 implica completar los pasos para realizar un apagado completo de un nodo y una desconexión de alimentación para cada nodo H610S que se describe en un requerido "[KB](#)". Se calcula que esta fase tarda aproximadamente una hora por nodo H610S.



Después de completar la fase 1, cuatro de las cinco actualizaciones de firmware se activan durante el arranque en frío en cada nodo H610S; sin embargo, el firmware del dispositivo lógico programable complejo (CPLD) requiere una desconexión de alimentación completa y reconexión para su instalación completa. La actualización de firmware de CPLD protege contra errores NVDIMM y eliminación de unidades de metadatos durante los reinicios o ciclos de apagado y encendido futuros. Se calcula que este restablecimiento de alimentación tarda aproximadamente una hora por nodo H610S. Requiere apagar el nodo, quitar los cables de alimentación o desconectar la alimentación a través de una PDU inteligente, esperar aproximadamente 3 minutos, y volver a conectar la alimentación.

Antes de empezar

- Completó la fase 1 del proceso de actualización de H610S y actualizó los nodos de almacenamiento mediante uno de los procedimientos de actualización de almacenamiento estándar de Element.



La fase 2 requiere personal in situ.

Pasos

1. (Fase 2) complete el proceso de restablecimiento de alimentación necesario para cada nodo H610S del clúster:



Si el clúster también tiene nodos que no son H610S, estos nodos que no son H610S están exentos de la fase 2 y no necesita que se apague o que tenga desconectada la alimentación.

1. Comuníquese con el soporte de NetApp para obtener ayuda y programar esta actualización.
2. Siga el procedimiento de actualización de fase 2 de este procedimiento "KB" Esto es necesario para completar una actualización para cada nodo H610S.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualizar el firmware de almacenamiento

A partir de Element 12.0 y la versión 2.14 de los servicios de gestión, puede realizar actualizaciones solo de firmware en los nodos de almacenamiento mediante la interfaz de usuario de Cloud Control de NetApp híbrido y la API DE REST. Este procedimiento no actualiza el software Element y permite actualizar el firmware de almacenamiento fuera de una versión de Element principal.

Lo que necesitará

- **Privilegios de administrador:** Dispone de permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Sincronización de hora del sistema:** Se ha asegurado de que la hora del sistema en todos los nodos está sincronizada y que NTP está correctamente configurado para el clúster de almacenamiento y los nodos. Cada nodo debe configurarse con un servidor de nombres DNS en la interfaz de usuario web por nodo (`https://[IP address]:442`) sin fallos de clúster sin resolver relacionados con la desviación de tiempo.
- **Puertos del sistema:** Si utiliza NetApp Hybrid Cloud Control para actualizaciones, se ha asegurado de

que los puertos necesarios están abiertos. Consulte ["Puertos de red"](#) si quiere más información.

- **Nodo de gestión:** Para la API e IU de control de cloud híbrido de NetApp, el nodo de gestión de su entorno ejecuta la versión 11.3.
- **Servicios de administración:** Ha actualizado su paquete de servicios de administración a la última versión.



Para los nodos de almacenamiento H610S que ejecutan la versión 12.0 del software Element, debe aplicar D-patch SUST-909 antes de actualizar al paquete de firmware de almacenamiento 2.27. Póngase en contacto con el soporte de NetApp para obtener el parche en D antes de la actualización. Consulte ["Notas de la versión del paquete de firmware de almacenamiento 2.27"](#).



Debe actualizar al paquete de servicios de gestión más reciente antes de actualizar el firmware en los nodos de almacenamiento. Si actualiza el software Element a la versión 12.2 o posterior, debe utilizar los servicios de gestión 2.14.60 o posterior para continuar.



Para actualizar el firmware del iDRAC/BIOS, comuníquese con el soporte de NetApp. Para obtener información adicional, consulte este ["Artículo de base de conocimientos"](#).

- **Cluster Health:** Ha ejecutado comprobaciones de estado. Consulte ["Ejecute comprobaciones del estado del almacenamiento de Element antes de actualizar el almacenamiento"](#).
- **BMC actualizado para nodos H610S:** Ha actualizado la versión de BMC para los nodos H610S. Consulte ["notas de la versión e instrucciones de actualización"](#).



Para obtener una matriz completa de firmware y firmware de controlador para su hardware, consulte ["Versiones de firmware compatibles para los nodos de almacenamiento de NetApp HCI"](#).

- **Contrato de licencia para el usuario final (CLUF):** A partir de los servicios de administración 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la UI o API de control de cloud híbrido de NetApp para actualizar el firmware de almacenamiento:

- a. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

- b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Elija una de las siguientes opciones de actualización del firmware de almacenamiento:

- [Utilice la interfaz de usuario de control del cloud híbrido de NetApp para actualizar el firmware de almacenamiento](#)
- [Utilice la API de control del cloud híbrido de NetApp para actualizar el firmware del almacenamiento](#)

Utilice la interfaz de usuario de control del cloud híbrido de NetApp para actualizar el firmware de almacenamiento

Puede usar la interfaz de usuario de control de cloud híbrido de NetApp para actualizar el firmware de los nodos de almacenamiento del clúster.

Lo que necesitará

Si el nodo de gestión no está conectado a Internet, lo tiene ["Ha descargado el paquete de firmware de almacenamiento para los clústeres de almacenamiento de NetApp HCI"](#).



Para obtener problemas potenciales al actualizar los clústeres de almacenamiento con NetApp Hybrid Cloud Control y sus soluciones alternativas, consulte ["Artículo de base de conocimientos"](#).



El proceso de actualización tarda aproximadamente 30 minutos por nodo de almacenamiento. Si actualiza un clúster de almacenamiento de Element a un firmware de almacenamiento posterior a la versión 2.76, los nodos de almacenamiento individuales solo se reiniciarán durante la actualización si se escribió el nuevo firmware en el nodo.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione **almacenamiento**.



La ficha **almacenamiento** muestra los clústeres de almacenamiento que forman parte de la instalación. Si el control de cloud híbrido de NetApp no permite acceder a un clúster, no se mostrará en la página **actualizaciones**. Si los clústeres ejecutan Element 12.0 o una versión posterior, se mostrará la versión actual del paquete de firmware indicado para estos clústeres. Si los nodos de un solo clúster tienen diferentes versiones de firmware en ellos o mientras la actualización progresa, verá **multiple** en la columna **Versión del paquete de firmware actual**. Puede seleccionar **Multiple** para desplazarse a la página **Nodes** para comparar las versiones de firmware. Si todos los clústeres ejecutan versiones de Element anteriores a 12.0, no se mostrará ninguna información sobre los números de versión del bundle de firmware. Esta información también está disponible en la página **Nodes**. Consulte ["Ver el inventario"](#).

Si el clúster está actualizado y/o no hay paquetes de actualización disponibles, no se muestran las pestañas **Element** y **sólo firmware**. Estas pestañas también no se muestran cuando hay una actualización en curso. Si se muestra la ficha **elemento**, pero no la ficha **sólo firmware**, no hay paquetes de firmware disponibles.

5. Seleccione la flecha desplegable junto al clúster que va a actualizar.
6. Seleccione **examinar** para cargar el paquete de actualización que ha descargado.
7. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga.



La carga del archivo se perderá si se desplaza fuera de la ventana del explorador.

Se muestra un mensaje en pantalla después de que el archivo se haya cargado y validado correctamente. La validación puede tardar varios minutos. Si se aleja de la ventana del explorador en este momento, se conserva la carga del archivo.

8. Seleccione **sólo firmware** y seleccione una de las versiones de actualización disponibles.

9. Seleccione **Iniciar actualización**.



Estado de actualización cambia durante la actualización para reflejar el estado del proceso. También cambia en respuesta a las acciones que realice, como la pausa de la actualización o si la actualización devuelve un error. Consulte [Cambios de estado de actualización](#).



Mientras la actualización está en curso, puede salir de la página y volver a ella más tarde para continuar supervisando el progreso. La página no actualiza el estado ni la versión actual de forma dinámica si la fila del clúster está contraída. La fila del clúster debe estar ampliada para actualizar la tabla, o bien se puede actualizar la página.

Es posible descargar registros una vez completada la actualización.

Cambios de estado de actualización

Estos son los diferentes estados que muestra la columna **Estado de actualización** de la interfaz de usuario antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
Actualizado	El clúster se actualizó a la versión más reciente disponible de Element o el firmware se actualizó a la versión más reciente.
No se puede detectar	Este estado se muestra cuando la API del servicio de almacenamiento devuelve un estado de actualización que no está en la lista enumerada de posibles Estados de actualización.
Versiones disponibles	Hay disponibles versiones más recientes del firmware de almacenamiento o Element para su actualización.
En curso	La actualización está en curso. Una barra de progreso muestra el estado de la actualización. Los mensajes en pantalla también muestran los errores a nivel de nodo y muestran el ID de nodo de cada nodo del clúster a medida que avanza la actualización. Es posible supervisar el estado de cada nodo mediante la interfaz de usuario de Element o el plugin de NetApp Element para la interfaz de usuario de vCenter Server.

Estado de actualización	Descripción
Actualice la pausa	Puede optar por poner en pausa la actualización. En función del estado del proceso de actualización, la operación de pausa puede realizarse correctamente o fallará. Verá un aviso de la interfaz de usuario que le solicita que confirme la operación de pausa. Para garantizar que el clúster esté en un lugar seguro antes de pausar una actualización, la operación de actualización puede tardar hasta dos horas en detenerse por completo. Para reanudar la actualización, seleccione Reanudar .
En pausa	Colocó en pausa la actualización. Seleccione Reanudar para reanudar el proceso.
Error	Se produjo un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp. Después de resolver el error, puede volver a la página y seleccionar Reanudar . Al reanudar la actualización, la barra de progreso se retrocede durante unos minutos mientras el sistema ejecuta la comprobación del estado y comprueba el estado actual de la actualización.

¿Qué ocurre si se produce un error en una actualización mediante el control del cloud híbrido de NetApp

Si se produce un error en una unidad o un nodo durante una actualización, la interfaz de usuario de Element mostrará errores en el clúster. El proceso de actualización no pasa al siguiente nodo y espera a que se resuelvan los errores del clúster. La barra de progreso de la interfaz de usuario muestra que la actualización está esperando a que se resuelvan los errores del clúster. En esta fase, la selección de **Pausa** en la interfaz de usuario no funcionará, ya que la actualización espera a que el clúster esté en buen estado. Deberá ponerse en contacto con el servicio de soporte de NetApp para que le ayude con la investigación de un fallo.

El control del cloud híbrido de NetApp tiene un periodo de espera predefinido de tres horas, durante el cual puede suceder una de las siguientes situaciones:

- Los fallos del clúster se resuelven en el plazo de tres horas y se reanuda la actualización. No es necesario realizar ninguna acción en este escenario.
- El problema persiste después de tres horas y el estado de actualización muestra **error** con un banner rojo. Puede reanudar la actualización seleccionando **Reanudar** después de resolver el problema.
- El soporte de NetApp ha determinado que se debe cancelar temporalmente el proceso de actualización para que pueda tomar medidas correctivas antes del plazo de tres horas. El equipo de soporte utilizará la API para cancelar la actualización.



Si se cancela la actualización del clúster mientras se actualiza un nodo, es posible que las unidades se eliminen sin dignidad del nodo. Si las unidades se quitan sin gracia, el soporte de NetApp deberá volver a añadir las unidades durante la actualización. Es posible que el nodo tarde más en realizar actualizaciones de firmware o actividades de sincronización posteriores a la actualización. Si el progreso de la actualización parece estancado, póngase en contacto con el soporte de NetApp para obtener ayuda.

Utilice la API de control del cloud híbrido de NetApp para actualizar el firmware del almacenamiento

Puede utilizar las API para actualizar los nodos de almacenamiento de un clúster a la versión más reciente del software Element. Puede utilizar una herramienta de automatización que prefiera para ejecutar las API. El flujo de trabajo de API que se documenta aquí, utiliza la interfaz de usuario de API DE REST disponible en el nodo de gestión como ejemplo.

Pasos

1. Descargue el paquete de actualización de firmware de almacenamiento más reciente en un dispositivo al que se pueda acceder el nodo de gestión; vaya al "[Página del paquete de firmware de almacenamiento del software Element](#)" y descargue la imagen del firmware de almacenamiento más reciente.
2. Cargue el paquete de actualización del firmware de almacenamiento en el nodo de gestión:
 - a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
 - c. En la interfaz de usuario DE LA API DE REST, seleccione **POST /packages**.
 - d. Seleccione **probar**.
 - e. Seleccione **Browse** y seleccione el paquete de actualización.
 - f. Seleccione **Ejecutar** para iniciar la carga.
 - g. Desde la respuesta, copie y guarde el ID del paquete ("`id`") para usar en un paso posterior.
3. Compruebe el estado de la carga.
 - a. En la interfaz de usuario de la API DE REST, seleccione **GET /packages/{id}/status**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID del paquete de firmware que ha copiado en el paso anterior en `id`.
 - d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

La respuesta indica `state` como `SUCCESS` cuando finalice.

4. Busque el ID de activo de instalación:
 - a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.

- iii. Seleccione **autorizar** para iniciar una sesión.
- iv. Cierre la ventana de autorización.
- c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
- d. Seleccione **probar**.
- e. Seleccione **Ejecutar**.
- f. Desde la respuesta, copie el ID del activo de instalación (*id*).

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

- g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.
- h. Seleccione **probar**.
- i. Pegue el ID de activo de instalación en el campo **id**.
- j. Seleccione **Ejecutar**.
- k. En la respuesta, copie y guarde el ID del clúster de almacenamiento ("*id*") del clúster que desee actualizar para usarlo en un paso posterior.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Ejecute la actualización del firmware de almacenamiento:

- a. Abra la interfaz de usuario de API DE REST de almacenamiento en el nodo de gestión:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as *mnode-client*.
 - iii. Seleccione **autorizar** para iniciar una sesión.

- iv. Cierre la ventana.
- c. Seleccione **POST /upgrades**.
- d. Seleccione **probar**.
- e. Introduzca el ID del paquete de actualización en el campo parámetro.
- f. Introduzca el ID del clúster de almacenamiento en el campo parámetro.
- g. Seleccione **Ejecutar** para iniciar la actualización.

La respuesta debe indicar el estado como `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",

```

```
    "description": "string",
    "remedy": "string",
    "severity": "string",
    "data": {},
    "nodeID": 0
  }
]
},
"taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
"dateCompleted": "2020-04-21T22:10:57.057Z",
"dateCreated": "2020-04-21T22:10:57.057Z"
}
```

- a. Copie el ID de actualización ("upgradeId") eso es parte de la respuesta.
6. Verifique el progreso y los resultados de la actualización:
- a. Seleccione **GET /upgrades/{actualizeld}**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de actualización desde el paso anterior en **Actualizar Id**.
 - d. Seleccione **Ejecutar**.
 - e. Realice una de las siguientes acciones si existen problemas o requisitos especiales durante la actualización:

Opción	Pasos
<p>Debe corregir los problemas de estado del clúster debido a <code>failedHealthChecks</code> mensaje en el cuerpo de respuesta.</p>	<ol style="list-style-type: none"> i. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la solución especificada. ii. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente. iii. Después de resolver los problemas del clúster, vuelva a autenticarse si es necesario y seleccione PONER /actualizaciones/{actualizable Id}. iv. Seleccione probar. v. Introduzca el ID de actualización desde el paso anterior en Actualizar Id. vi. Introduzca <code>"action": "resume"</code> en el cuerpo de la solicitud. <div style="border: 1px solid #ccc; border-radius: 5px; padding: 10px; margin: 10px 0;"> <pre>{ "action": "resume" }</pre> </div> vii. Seleccione Ejecutar.
<p>Debe pausar la actualización porque la ventana de mantenimiento se está cerrando o por otro motivo.</p>	<ol style="list-style-type: none"> i. Vuelva a autenticarse si es necesario y seleccione PONER /actualizaciones/{actualizeld}. ii. Seleccione probar. iii. Introduzca el ID de actualización desde el paso anterior en Actualizar Id. iv. Introduzca <code>"action": "pause"</code> en el cuerpo de la solicitud. <div style="border: 1px solid #ccc; border-radius: 5px; padding: 10px; margin: 10px 0;"> <pre>{ "action": "pause" }</pre> </div> v. Seleccione Ejecutar.

f. Ejecute la API **GET /upgrades/{actualizable Id}** varias veces, según sea necesario, hasta que el proceso se complete.

Durante la actualización, el `status` lo que indica `running` si no se encuentra ningún error. Cuando cada nodo se actualiza, el `step` el valor cambia a `NodeFinished`.

La actualización se completó correctamente cuando el `percent` el valor es 100 y la `state` lo que indica `finished`.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualice un nodo de gestión

Puede actualizar el nodo de gestión a la versión 12.3.x del nodo de gestión desde la versión 11.0 o posterior.

Ya no se necesita actualizar el sistema operativo del nodo de gestión para actualizar el software Element en el clúster de almacenamiento. Si el nodo de gestión es la versión 11.3 o posterior, solo tiene que actualizar los servicios de gestión a la versión más reciente para realizar actualizaciones de Element mediante el control de cloud híbrido de NetApp. Siga el procedimiento de actualización del nodo de gestión para su escenario si desea actualizar el sistema operativo del nodo de gestión por otros motivos, como la corrección de seguridad.



El plugin de vCenter versión 4.4 o posterior requiere un nodo de gestión 11.3 o posterior que se cree con una arquitectura modular y proporcione servicios individuales.

Opciones de actualización

Elija una de las siguientes opciones de actualización del nodo de gestión:



- El nodo de gestión 12.3.2 contiene una mitigación de seguridad para los clústeres de almacenamiento con la función Virtual Volumes (VVOL) habilitada. Si el clúster de almacenamiento ya está en Element 12.3 y la función VVOL está habilitada, debe actualizarse a 12.3.2.
- No hay cambios de funcionalidad adicionales ni correcciones de errores en el nodo de gestión 12.3.1. Si ya ejecuta el nodo de gestión 12.3, no es necesario actualizarlo a 12.3.1.

- Si va a actualizar desde el nodo de gestión 12.3: No hay cambios de funcionalidad adicionales ni correcciones de errores en el nodo de gestión 12.3.1. Si ya ejecuta el nodo de gestión 12.3, no es necesario actualizarlo a 12.3.1.



Si decide continuar con una actualización de un nodo de gestión 12.3 puesto en marcha mediante NDE, finaliza la actualización a la versión 12.3.x. Sin embargo, es posible que la actualización encuentre un error durante el reinicio. Si esto ocurre, reinicie el nodo de gestión para que muestre correctamente 12.3.x.

- Si va a actualizar desde el nodo de gestión 12.2: [Actualice un nodo de gestión a la versión 12.3.x desde 12.2](#)
- Si va a actualizar desde el nodo de gestión 12.0: [Actualice un nodo de gestión a la versión 12.3.x desde 12.0](#)
- Si va a actualizar desde el nodo de gestión 11.3, 11.5, 11.7 o 11.8: [Actualice un nodo de gestión a la versión 12.3.x de 11.3 a 11.8](#)
- Si va a actualizar desde el nodo de gestión 11.0 o 11.1: [Actualice un nodo de gestión a la versión 12.3.x desde 11.1 o 11.0](#)

- Si va a actualizar desde un nodo de gestión versión 10.x: [Migrar desde el nodo de gestión versión 10.x a 11.x](#).

Elija la siguiente opción si ha * actualizado secuencialmente* (1) la versión de los servicios de administración y (2) la versión de almacenamiento de Element y desea **mantener** su nodo de gestión existente:



Si no actualiza secuencialmente los servicios de gestión seguidos por el almacenamiento de Element, no se puede volver a configurar la autenticación mediante este procedimiento. Siga en su lugar el procedimiento de actualización adecuado.

- Si va a mantener el nodo de gestión existente: [Volver a configurar la autenticación mediante la API DE REST del nodo de gestión](#)

Actualice un nodo de gestión a la versión 12.3.x desde 12.2

Puede realizar una actualización in situ del nodo de gestión de la versión 12.2 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.



El nodo de gestión Element 12.3.x es una actualización opcional. No es necesario para las puestas en marcha existentes.

Lo que necesitará

- La RAM de la máquina virtual del nodo de gestión es 24 GB.
- El nodo de gestión que pretende actualizar es la versión 12.0 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.



Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Ha actualizado su paquete de servicios de gestión a la versión más reciente con control del cloud híbrido de NetApp (HCC). Puede acceder a HCC desde la siguiente IP: `<a href="https://<ManagementNodeIP>" class="bare">https://<ManagementNodeIP>`
- Si actualiza el nodo de gestión a la versión 12.3.x, necesita servicios de gestión 2.14.60 o una versión posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) utilizando las instrucciones para ["Configuración de una NIC de almacenamiento adicional"](#).



Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

Pasos

1. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
2. Descargue el ["Nodo de gestión ISO"](#) Para NetApp HCI desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.



El nombre de la ISO es similar a `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Para comprobar la integridad de la descarga, ejecute `md5sum` en el archivo descargado y compare el resultado con lo disponible en el sitio de soporte de NetApp para el software NetApp HCI o Element, como en el siguiente ejemplo:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Cambie al directorio inicial y desmonte el archivo ISO de `/mnt`:

```
sudo umount /mnt
```

6. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. En el nodo de gestión que desea actualizar, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de gestión. El script conserva todos los archivos de configuración necesarios después de la actualización, como el recopilador Active IQ y la configuración de proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.



Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

8. En el nodo de gestión, ejecute el `redeploy-mnode` secuencia de comandos para mantener los valores de configuración anteriores de los servicios de administración:



El script conserva la configuración anterior de servicios de gestión, incluida la configuración del servicio de recopilador Active IQ, controladoras (vCenter) o proxy, en función de la configuración.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```



Si había deshabilitado anteriormente la funcionalidad SSH en el nodo de gestión, debe hacerlo "[Vuelva a deshabilitar SSH](#)" en el nodo de gestión recuperado. Funcionalidad SSH que proporciona "[Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support](#)" está habilitado en el nodo de gestión de manera predeterminada.

Actualice un nodo de gestión a la versión 12.3.x desde 12.0

Puede realizar una actualización in situ del nodo de gestión de la versión 12.0 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.



El nodo de gestión Element 12.3.x es una actualización opcional. No es necesario para las puestas en marcha existentes.

Lo que necesitará

- El nodo de gestión que pretende actualizar es la versión 12.0 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.



Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Ha actualizado su paquete de servicios de gestión a la versión más reciente con control del cloud híbrido de NetApp (HCC). Puede acceder a HCC desde la siguiente IP: `<a href="https://<ManagementNodeIP>" class="bare">https://<ManagementNodeIP>`
- Si actualiza el nodo de gestión a la versión 12.3.x, necesita servicios de gestión 2.14.60 o una versión posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) utilizando las instrucciones para "[Configuración de una NIC de almacenamiento adicional](#)".



Es posible que los volúmenes persistentes requieran un adaptador de red adicional si `eth0` no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

Pasos

1. Configure la RAM de la máquina virtual del nodo de gestión:
 - a. Apague la máquina virtual del nodo de gestión.
 - b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de gestión.
2. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
3. Descargue el "[Nodo de gestión ISO](#)" Para NetApp HCI desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.



El nombre de la ISO es similar a `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Para comprobar la integridad de la descarga, ejecute `md5sum` en el archivo descargado y compare el resultado con lo disponible en el sitio de soporte de NetApp para el software NetApp HCI o Element, como en el siguiente ejemplo:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

5. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Cambie al directorio inicial y desmonte el archivo ISO de `/mnt`:

```
sudo umount /mnt
```

7. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

8. En el nodo de gestión que desea actualizar, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de gestión. El script conserva todos los archivos de configuración necesarios

después de la actualización, como el recopilador Active IQ y la configuración de proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.



Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

9. En el nodo de gestión, ejecute el `redeploy-mnode` secuencia de comandos para mantener los valores de configuración anteriores de los servicios de administración:



El script conserva la configuración anterior de servicios de gestión, incluida la configuración del servicio de recopilador Active IQ, controladoras (vCenter) o proxy, en función de la configuración.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```



Funcionalidad SSH que proporciona ["Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support"](#) está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 y posteriores. Si ya había habilitado la funcionalidad SSH en el nodo de gestión, es posible que deba hacerlo ["Vuelva a deshabilitar SSH"](#) en el nodo de gestión actualizado.

Actualice un nodo de gestión a la versión 12.3.x de 11.3 a 11.8

Puede realizar una actualización in situ del nodo de gestión desde la versión 11.3, 11.5, 11.7 o 11.8 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.



El nodo de gestión Element 12.3.x es una actualización opcional. No es necesario para las puestas en marcha existentes.

Lo que necesitará

- El nodo de gestión que pretende actualizar es la versión 11.3, 11.5, 11.7 o 11.8 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.



Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Ha actualizado su paquete de servicios de gestión a la versión más reciente con control del cloud híbrido de NetApp (HCC). Puede acceder a HCC desde la siguiente IP: `<a>`

href="https://<ManagementNodeIP>" class="bare">https://<ManagementNodeIP>;</code>

- Si actualiza el nodo de gestión a la versión 12.3.x, necesita servicios de gestión 2.14.60 o una versión posterior para continuar.
- Ha configurado un adaptador de red adicional (si es necesario) utilizando las instrucciones para ["Configuración de una NIC de almacenamiento adicional"](#).



Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.

Pasos

1. Configure la RAM de la máquina virtual del nodo de gestión:
 - a. Apague la máquina virtual del nodo de gestión.
 - b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de gestión.
2. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
3. Descargue el ["Nodo de gestión ISO"](#) Para NetApp HCI desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.



El nombre de la ISO es similar a `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Para comprobar la integridad de la descarga, ejecute md5sum en el archivo descargado y compare el resultado con lo disponible en el sitio de soporte de NetApp para el software NetApp HCI o Element, como en el siguiente ejemplo:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

5. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Cambie al directorio inicial y desmonte el archivo ISO de /mnt:

```
sudo umount /mnt
```

7. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-  
XX.X.X.XXXX.iso
```

8. En el nodo de gestión 11.3, 11.5, 11.7 o 11.8, ejecute el siguiente comando para actualizar la versión del sistema operativo del nodo de gestión. El script conserva todos los archivos de configuración necesarios después de la actualización, como el compilador Active IQ y la configuración de proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.



Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

9. En el nodo de gestión, ejecute el `redeploy-mnode` secuencia de comandos para mantener los valores de configuración anteriores de los servicios de administración:



El script conserva la configuración anterior de servicios de gestión, incluida la configuración del servicio de compilador Active IQ, controladoras (vCenter) o proxy, en función de la configuración.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```



Funcionalidad SSH que proporciona "[Acceso a la sesión del túnel de soporte remoto \(RST\) de NetApp Support](#)" está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 y posteriores. Si ya había habilitado la funcionalidad SSH en el nodo de gestión, es posible que deba hacerlo "[Vuelva a deshabilitar SSH](#)" en el nodo de gestión actualizado.

Actualice un nodo de gestión a la versión 12.3.x desde 11.1 o 11.0

Puede realizar una actualización in situ del nodo de gestión desde 11.0 o 11.1 a la versión 12.3.x sin necesidad de aprovisionar una nueva máquina virtual del nodo de gestión.

Lo que necesitará

- Los nodos de almacenamiento ejecutan Element 11.3 o una versión posterior.



Utilice las últimas HealthTools para actualizar el software Element.

- El nodo de gestión que pretende actualizar es la versión 11.0 o 11.1 y utiliza redes IPv4. La versión 12.3.x del nodo de gestión no es compatible con IPv6.



Para comprobar la versión del nodo de gestión, inicie sesión en su nodo de gestión y vea el número de versión de Element en el banner de inicio de sesión.

- Para el nodo de gestión 11.0, la memoria de la máquina virtual se debe aumentar manualmente a 12 GB.
- Se configuró un adaptador de red adicional (si es necesario) mediante las instrucciones para configurar un NIC de almacenamiento (eth1) en la guía del usuario del nodo de gestión del producto.



Es posible que los volúmenes persistentes requieran un adaptador de red adicional si eth0 no se puede enrutar a la SVIP. Configure un nuevo adaptador de red en la red de almacenamiento iSCSI para permitir la configuración de volúmenes persistentes.

Pasos

1. Configure la RAM de la máquina virtual del nodo de gestión:
 - a. Apague la máquina virtual del nodo de gestión.
 - b. Cambie la RAM de la máquina virtual del nodo de gestión de 12 GB a 24 GB de RAM.
 - c. Encienda la máquina virtual del nodo de gestión.
2. Inicie sesión en la máquina virtual del nodo de gestión mediante SSH o el acceso de consola.
3. Descargue el "[Nodo de gestión ISO](#)" Para NetApp HCI desde el sitio de soporte de NetApp hasta la máquina virtual del nodo de gestión.



El nombre de la ISO es similar a `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Para comprobar la integridad de la descarga, ejecute `md5sum` en el archivo descargado y compare el resultado con lo disponible en el sitio de soporte de NetApp para el software NetApp HCI o Element, como en el siguiente ejemplo:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

5. Monte la imagen ISO del nodo de gestión y copie el contenido en el sistema de archivos mediante los siguientes comandos:

```
sudo mkdir -p /upgrade
```

```
sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Cambie al directorio principal y desmonte el archivo ISO de /mnt:

```
sudo umount /mnt
```

7. Elimine el ISO para conservar espacio en el nodo de gestión:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-  
XX.X.X.XXXX.iso
```

8. Ejecute uno de los siguientes scripts con opciones para actualizar la versión de sistema operativo del nodo de gestión. Ejecute sólo el script que sea apropiado para su versión. Cada script conserva todos los archivos de configuración necesarios después de la actualización, como el recopilador Active IQ y la configuración de proxy.

- a. En un nodo de gestión de 11.1 (11.1.0.73), ejecute el siguiente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1  
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288  
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc  
/sf/packages/nma"
```

- b. En un nodo de gestión de 11.1 (11.1.0.72), ejecute el siguiente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1  
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281  
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc  
/sf/packages/nma"
```

- c. En un nodo de gestión de 11.0 (11.0.0.781), ejecute el siguiente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1  
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253  
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc  
/sf/packages/nma"
```

El nodo de gestión se reinicia con un sistema operativo nuevo una vez que finaliza el proceso de actualización.



Después de ejecutar el comando sudo descrito en este paso, se mata la sesión SSH. Se requiere acceso a la consola para una supervisión continua. Si no tiene acceso a la consola al realizar la actualización, vuelva a intentar el inicio de sesión SSH y verifique la conectividad después de 15 a 30 minutos. Una vez que inicia sesión, puede confirmar la nueva versión del sistema operativo en el banner SSH que indica que la actualización se ha realizado correctamente.

9. En el nodo de gestión 12.3.x, ejecute el `upgrade-mnode` script para conservar los valores de configuración anteriores.



Si va a migrar desde un nodo de gestión 11.0 o 11.1, el script copia el recopilador Active IQ al nuevo formato de configuración.

- a. Para un único clúster de almacenamiento gestionado por un nodo de gestión existente 11.0 o 11.1 con volúmenes persistentes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account>
```

- b. Para un único clúster de almacenamiento gestionado por un nodo de gestión existente 11.0 o 11.1 sin volúmenes persistentes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
```

- c. Para varios clústeres de almacenamiento gestionados por un nodo de gestión existente 11.0 o 11.1 con volúmenes persistentes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account> -pvm <persistent volumes mvip>
```

- d. En el caso de varios clústeres de almacenamiento gestionados por un nodo de gestión existente 11.0 o 11.1 sin volúmenes persistentes (el `-pvm` indicador es proporcionar una de las direcciones MVIP del clúster):

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
persistent volumes>
```

10. (Para todas las instalaciones de NetApp HCI con el plugin de NetApp Element para vCenter Server) actualice el plugin de vCenter en el nodo de gestión 12.3.x siguiendo los pasos del ["Actualice el plugin de Element para vCenter Server"](#) tema.
11. Busque el ID de activo para su instalación con la API del nodo de gestión:
 - a. Desde un explorador, inicie sesión en la API DE REST del nodo de gestión:

- i. Vaya a la MVIP de almacenamiento e inicie sesión. Esta acción hace que se acepte el certificado para el siguiente paso.
- b. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- c. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana.
- d. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
- e. Seleccione **probar**.
- f. Seleccione **Ejecutar**.
- g. Del cuerpo de respuesta del código 200, copie el `id` para la instalación.

Su instalación tiene una configuración de activos base que se creó durante la instalación o la actualización.

12. Busque la etiqueta de hardware para el nodo de computación en vSphere:
 - a. Seleccione el host en el navegador vSphere Web Client.
 - b. Seleccione la ficha **Monitor** y seleccione **Estado del hardware**.
 - c. Se muestran el fabricante del BIOS del nodo y el número de modelo. Copie y guarde el valor para `tag` para su uso en un paso posterior.
13. Añada un activo de controladora de vCenter para la supervisión de HCI y el control de cloud híbrido a los activos conocidos del nodo de gestión:
 - a. Seleccione **POST /assets/{Asset_id}/controllers** para agregar un subactivo de controlador.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
 - d. Introduzca los valores de carga útil necesarios con el tipo `vCenter De aplicaciones y vCenter`.
 - e. Seleccione **Ejecutar**.
14. Añada un activo de nodo de computación a los activos conocidos del nodo de gestión:
 - a. Seleccione **POST /assets/{Asset_id}/Compute-Nodes** para agregar un subactivo de nodo de computación con credenciales para el activo de nodo de computación.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de activo base principal que copió en el portapapeles en el campo **Asset_id**.
 - d. En la carga útil, introduzca los valores de carga útil necesarios tal y como se definen en la ficha **Modelo** . Introduzca `ESXi Host` como `type` y pegue la etiqueta de hardware guardada durante un paso anterior para `hardware_tag`.
 - e. Seleccione **Ejecutar**.

Migrar desde el nodo de gestión versión 10.x a 11.x.

Si tiene un nodo de gestión en la versión 10.x, no puede actualizar de 10.x a 11.x. En su lugar, se puede utilizar este procedimiento de migración para copiar mediante la configuración desde 10.x a un nodo de gestión 11.1 recién implementado. Si el nodo de gestión está actualmente en 11.0 o una versión superior, debe omitir este procedimiento. Necesita el nodo de gestión 11.0 o 11.1 y el "Últimas HealthTools" Para actualizar el software Element de 10.3 + a 11.x.

Pasos

1. Desde la interfaz de VMware vSphere, implemente el OVA del nodo de gestión 11.1 y enciéndalo.
2. Abra la consola de máquina virtual del nodo de gestión, que aparece la interfaz de usuario de terminal (TUI).
3. Use la TUI para crear un nuevo ID de administrador y asignar una contraseña.
4. En la TUI del nodo de gestión, inicie sesión en el nodo de gestión con el ID y la contraseña nuevos y valide que funciona.
5. En la TUI de nodos de gestión o vCenter, obtenga la dirección IP 11.1 del nodo de gestión y busque la dirección IP en el puerto 9443 para abrir la interfaz de usuario del nodo de gestión.

```
https://<mNode 11.1 IP address>:9443
```

6. En vSphere, seleccione **Configuración de NetApp Element > Configuración de mNode**. (En versiones anteriores, el menú de nivel superior es **Configuración de SolidFire de NetApp**).
7. Seleccione **acciones > Borrar**.
8. Para confirmar, seleccione **Sí**. El campo mNode Status debe informar de no configurado.



Cuando vaya a la ficha **mNode Settings** por primera vez, el campo mNode Status puede aparecer como **no configurado** en lugar del **UP** esperado; es posible que no pueda elegir **acciones > Clear**. Actualice el explorador. El campo mNode Status finalmente mostrará **UP**.

9. Cierre la sesión de vSphere.
10. En un explorador web, abra la utilidad de registro del nodo de gestión y seleccione **Administración de servicios QoSSIOC**:

```
https://<mNode 11.1 IP address>:9443
```

11. Establezca la nueva contraseña de QoSSIOC.



La contraseña predeterminada es `solidfire`. Se requiere esta contraseña para establecer la nueva contraseña.

12. Seleccione la pestaña **vCenter Plug-in Registration**.
13. Seleccione **Actualizar Plug-in**.
14. Introduzca los valores necesarios. Cuando haya terminado, seleccione **ACTUALIZAR**.
15. Inicie sesión en vSphere y seleccione **Configuración de NetApp Element > Configuración de mNode**.
16. Seleccione **acciones > Configurar**.

- Proporcione la dirección IP del nodo de gestión y el ID de usuario del nodo de gestión (el nombre de usuario es `admin`), la contraseña que ha establecido en la ficha **QoSSIOC Service Management** de la utilidad de registro y el ID de usuario y la contraseña de vCenter.

En vSphere, la pestaña **mNode Settings** debe mostrar el estado de mNode como **UP**, que indica que el nodo de gestión 11.1 está registrado en vCenter.

- Desde la utilidad de registro del nodo de gestión (<https://<mNode 11.1 IP address>:9443>), reinicie el servicio SIOC desde **QoSSIOC Service Management**.
- Espere un minuto y compruebe la ficha **Configuración de NetApp Element > Configuración de mNode**. Esto debería mostrar el estado de mNode como **UP**.

Si el estado es **DOWN**, compruebe los permisos para `/sf/packages/sioc/app.properties`. El archivo debe tener permisos de lectura, escritura y ejecución para el propietario del archivo. Los permisos correctos deben aparecer de la siguiente manera:

```
-rwx-----
```

- Después de que se inicia el proceso SIOC y vCenter muestra el estado mNode como **UP**, compruebe los registros de la `sf-hci-nma` servicio en el nodo de gestión. No debe haber mensajes de error.
- (Solo para el nodo de gestión 11.1) SSH en la versión 11.1 del nodo de gestión con privilegios raíz e inicie el servicio NMA con los siguientes comandos:

```
# systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
```

```
# systemctl start sf-hci-nma21
```

- Ejecute acciones desde vCenter para quitar una unidad, añadir una unidad o reiniciar nodos. Esto activa las alertas de almacenamiento que se deben notificar en vCenter. Si esto funciona, las alertas del sistema NMA funcionan según lo esperado.
- Si ONTAP Select se configura en vCenter, configure las alertas de ONTAP Select en NMA copiando el `.ots.properties` archivo del nodo de gestión anterior al nodo de gestión, versión 11.1 `/sf/packages/nma/conf/.ots.properties` File, y reinicie el servicio NMA mediante el siguiente comando:

```
systemctl restart sf-hci-nma
```

- Compruebe que ONTAP Select esté funcionando. Para ello, consulte los registros con el siguiente comando:

```
journalctl -f | grep -i ots
```

- Siga estos pasos para configurar Active IQ:

a. SSH en la versión 11.1 del nodo de gestión y vaya al `/sf/packages/collector` directorio.

b. Ejecute el siguiente comando:

```
sudo ./manage-collector.py --set-username netapp --set-password --set-mvip <MVIP>
```

c. Introduzca la contraseña de interfaz de usuario del nodo de gestión cuando se lo solicite.

d. Ejecute los siguientes comandos:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

e. Verificación `sfcollector` registra para confirmar que funciona.

26. En vSphere, la pestaña **Configuración de NetApp Element > Configuración de mNode** debe mostrar el estado de mNode como **UP**.

27. Comprobar que NMA notifica alertas del sistema y alertas ONTAP Select.

28. Si todo funciona según lo esperado, apague y elimine el nodo de gestión 10.x.

Volver a configurar la autenticación mediante la API DE REST del nodo de gestión

Se puede conservar el nodo de gestión existente si se actualizaron secuencialmente (1) y (2) el almacenamiento de Element. Si ha seguido un orden de actualización diferente, consulte los procedimientos para actualizar nodos de gestión sin movimiento.

Antes de empezar

- Ha actualizado sus servicios de administración a 2.10.29 o posterior.
- El clúster de almacenamiento ejecuta Element 12.0 o una versión posterior.
- El nodo de gestión es 11.3 o posterior.
- Actualizó secuencialmente los servicios de gestión a continuación, actualizando el almacenamiento de Element. No puede volver a configurar la autenticación con este procedimiento a menos que haya completado las actualizaciones en la secuencia descrita.

Pasos

1. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/mnode
```

2. Seleccione **autorizar** y complete lo siguiente:

a. Introduzca el nombre de usuario y la contraseña del clúster.

b. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.

- c. Seleccione **autorizar** para iniciar una sesión.
3. En la interfaz DE usuario DE LA API DE REST, seleccione **POST /Services/reconfigure-auth**.
4. Seleccione **probar**.
5. Para el parámetro **LOAD_images**, seleccione `true`.
6. Seleccione **Ejecutar**.

El cuerpo de respuesta indica que la reconfiguración se ha realizado correctamente.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualice el plugin de Element para vCenter Server

Para los entornos de vSphere existentes con un plugin de NetApp Element registrado para VMware vCenter Server, es posible actualizar el registro del plugin después de actualizar por primera vez el paquete de servicios de gestión que contiene el servicio del plugin.

Es posible actualizar el registro del plugin en vCenter Server Virtual Appliance (vcsa) o Windows desde la utilidad de registro. Debe cambiar el registro del plugin de vCenter en cada instancia de vCenter Server donde necesite usar el plugin.



Los servicios de gestión 2.22.7 incluyen el plugin de Element para vCenter Server 5.0, que contiene el plugin remoto. Si usa el plugin de Element, debe actualizar a los servicios de gestión 2.22.7 o una versión posterior para cumplir con la directiva de VMware que elimina la compatibilidad con los plugins locales. ["Leer más"](#).

Plugin de Element para vCenter 5.0 y versiones posteriores

Este procedimiento de actualización cubre los siguientes escenarios de actualización:

- Va a actualizar al plugin de Element para vCenter Server 5,3, 5,2, 5,1 o 5,0.
- Actualice a un HTML5 8.0 o 7.0 vSphere Web Client.



El plugin de Element para vCenter 5,0 o posterior no es compatible con vCenter Server 6,7 y 6,5.



Cuando se actualiza desde el plugin de Element para vCenter Server 4.x a 5.x, los clústeres ya configurados con el plugin se pierden porque no se pueden copiar los datos de una instancia de vCenter en un plugin remoto. Debe volver a añadir los clústeres al plugin remoto. Esta es una actividad que solo debe hacer una vez al actualizar desde un plugin local a un plugin remoto.

Plugin de Element para vCenter 4.10 y versiones anteriores

Este procedimiento de actualización cubre los siguientes escenarios de actualización:

- Actualice al plugin de Element para VMware vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5, o 4.4.
- Va a actualizar a un HTML5 7.0, 6.7 o 6.5 vSphere Web Client.

- El plugin no es compatible con VMware vCenter Server 8.0 para el plugin de Element para VMware vCenter Server 4.x.
- El plugin no es compatible con VMware vCenter Server 6.5 para el plugin de Element para VMware vCenter Server 4.6, 4.7 y 4.8.

- Actualice a una instancia de Flash vSphere Web Client en 6.7.



El plugin no es compatible con la versión 6.7 U2 compilación 13007421 del HTML5 vSphere Web Client y otras versiones de 6.7 U2 publicadas antes de la actualización 2a (compilación 13643870). Para obtener más información sobre las versiones de vSphere compatibles, consulte las notas de la versión de "[la versión del plugin](#)".

Lo que necesitará

- **Privilegios de administrador:** Tiene privilegios de la función de administrador de vCenter para instalar un complemento.
- **Actualizaciones de vSphere:** Ha realizado cualquier actualización de vCenter necesaria antes de actualizar el plugin de NetApp Element para vCenter Server. Este procedimiento da por sentado que ya se completaron las actualizaciones de vCenter.
- **vCenter Server:** El plugin de vCenter versión 5.x o 4.x está registrado en vCenter Server. Desde la utilidad de registro ([https://\[management node IP\]:9443](https://[management node IP]:9443)), seleccione **Registration Status**, complete los campos necesarios y seleccione **Check Status** para comprobar que el complemento de vCenter ya está registrado y que el número de versión de la instalación actual.
- **Actualizaciones de servicios de administración:** Ha actualizado el "[paquete de servicios de gestión](#)" a la última versión. Las actualizaciones en el complemento de vCenter se distribuyen mediante

actualizaciones de servicios de gestión que se publican fuera de las principales versiones de productos para NetApp HCI.

- **Actualizaciones del nodo de administración:**

- A partir del plugin de Element vCenter versión 5.0, se ejecuta un nodo de gestión que haya estado "actualizado" a la versión 12.3.x o posterior.
- Para el plugin de Element vCenter 4.4 a 4.10, ejecuta un nodo de gestión que haya sido "actualizado" a la versión 11.3 o posterior. El complemento de vCenter versión 4.4 o posterior requiere un nodo de gestión de 11.3 o posterior con una arquitectura modular que proporciona servicios individuales. El nodo de gestión debe estar encendido y tener configurada su dirección IP o dirección DHCP.

- **Actualizaciones de almacenamiento de elementos:**

- A partir del plugin de Element vCenter versión 5.0, tiene un clúster que ejecuta el software NetApp Element 12.3.x o una versión posterior.
- Para el plugin de Element vCenter versión 4.10 o una versión anterior, tiene un clúster que ejecuta el software NetApp Element 11.3 o una versión posterior.

- **VSphere Web Client:** Cerró la sesión en vSphere Web Client antes de iniciar cualquier actualización de plugin. Si no cierra sesión, el cliente web no reconocerá las actualizaciones realizadas durante este proceso al plug-in.

Pasos

1. Introduzca la dirección IP para el nodo de gestión en un navegador, incluido el puerto TCP para el registro: `https://[management node IP]:9443` La interfaz de usuario de la utilidad de registro se abre en la página **Manage QoSSIIOC Service Credentials** del plugin.

The screenshot shows the NetApp Element Plug-in for vCenter Server Management Node interface. The page title is "Manage QoSSIIOC Service Credentials". On the left, there is a sidebar with "QoSSIIOC Management" and "Manage Credentials" (selected) and "Restart QoSSIIOC Service". The main content area has three password fields: "Old Password" (with "Current password" and "Current password is required" below it), "New Password" (with "New password" and "Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like #!%&()*-./:;@^_~" below it), and "Confirm Password" (with "Confirm New Password" and "New and confirm passwords must match" below it). A "SUBMIT CHANGES" button is at the bottom.

Contact NetApp Support at <http://mysupport.netapp.com>

2. Seleccione **vCenter Plug-in Registration**.

- La página de registro del plugin de vCenter para el plugin de Element para vCenter Server 5.x:

The screenshot shows the NetApp Element Plug-in for vCenter Server Management Node registration page. The page has a dark blue header with the NetApp logo and the title "Element Plug-in for vCenter Server Management Node". Below the header, there are two tabs: "GoSSIOC Service Management" and "vCenter Plug-in Registration", with the latter being selected. The main content area is divided into two columns. The left column, titled "Manage vCenter Plug-in", contains a list of options: "Register Plug-in" (highlighted), "Update Plug-in", "Unregister Plug-in", and "Registration Status". The right column, titled "vCenter Plug-in - Registration", contains the following text: "Register version 5.0.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration." Below this text are three input fields: "vCenter Address" (with a sub-label "vCenter Server Address" and a note "Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on."), "vCenter User Name" (with a sub-label "vCenter Admin User Name" and a note "Ensure this user is a vCenter user that has administrative privileges for registration."), and "vCenter Password" (with a sub-label "vCenter Admin Password" and a note "The password for the vCenter user name entered."). There is also a checkbox labeled "Customize URL" with a note "Select to customize the Zip file URL." Below this is a "Plug-in Zip URL" field with a sub-label "URL of XML initialization file" and a text input containing "https://10.117.227.44:8333/vcp-ui/plugin.json". At the bottom of the right column is a "REGISTER" button. At the bottom of the page, there is a footer with the text "Contact NetApp Support at <http://mysupport.netapp.com>".

- La página de registro del plugin de vCenter para el plugin de Element para vCenter Server 4.10 o una versión anterior:

Manage vCenter Plug-in

- Register Plug-in
- Update Plug-in
- Unregister Plug-in
- Registration Status

vCenter Plug-in - Registration

Register version of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address vCenter Server Address
Enter the IPv4, IPv6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name vCenter Admin User Name
Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password vCenter Admin Password
The password for the vCenter user name entered.

Customize URL
Select to customize the Zip file URL.

Plug-in Zip URL https://10.117.227.12-9443/solidfire-plugin-4.5.0-bin.zip
URL of XML initialization file.

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

3. En **Manage vCenter Plug-in**, seleccione **Update Plug-in**.

4. Confirme o actualice la siguiente información:

- a. La dirección IPv4 o el nombre de dominio completo del servicio vCenter en el que planea registrar el plugin.
- b. El nombre de usuario administrador de vCenter.



Las credenciales de nombre de usuario y contraseña introducidas deben corresponder a un usuario con privilegios de la función de administrador de vCenter.

- c. La contraseña de administrador de vCenter.
- d. (Para servidores internos/sitios oscuros) dependiendo de la versión de Element para vCenter, una URL personalizada para el archivo JSON del plugin o el ZIP del plugin:
 - i. A partir del plugin de Element para vCenter Server 5.0, una URL personalizada para el archivo JSON del plugin.



Puede seleccionar **URL personalizada** para personalizar la URL si utiliza un servidor HTTP o HTTPS (sitio oscuro) o si ha modificado el nombre del archivo JSON o la configuración de red. Para obtener pasos de configuración adicionales si planea personalizar una URL, consulte la documentación del plugin de Element para vCenter Server sobre la modificación de las propiedades de vCenter para un servidor HTTP interno (sitio oscuro).

- ii. Para el plugin de Element para vCenter Server 4.10 o versiones anteriores, una URL personalizada para el ZIP del plugin.



Puede seleccionar **URL personalizada** para personalizar la URL si utiliza un servidor HTTP o HTTPS (sitio oscuro) o si ha modificado el nombre del archivo ZIP o la configuración de red. Para obtener pasos de configuración adicionales si planea personalizar una URL, consulte la documentación del plugin de Element para vCenter Server sobre la modificación de las propiedades de vCenter para un servidor HTTP interno (sitio oscuro).

5. Seleccione **Actualizar**.

Aparece un banner en la interfaz de usuario de la utilidad de registro cuando el registro se realiza correctamente.

6. Inicie sesión en vSphere Web Client como administrador de vCenter. Si ya ha iniciado sesión en vSphere Web Client, primero debe cerrar la sesión, esperar dos o tres minutos y, a continuación, iniciar sesión de nuevo.



Esta acción crea una base de datos nueva y completa la instalación en vSphere Web Client.

7. En vSphere Web Client, busque las siguientes tareas completadas en el monitor de tareas para garantizar que se haya completado la instalación: `Download plug-in y.. Deploy plug-in`.

8. Verifique que los puntos de extensión del plugin aparezcan en la pestaña **Shortcuts** de vSphere Web Client y en el panel lateral.

- A partir del plugin de Element para vCenter Server 5.0, se muestra el punto de extensión NetApp Element Remote Plugin:
- En el caso del plugin de Element para vCenter Server 4.10 o una versión anterior, los puntos de extensión NetApp Element Configuration y Management aparecen:



Si los iconos del plugin de vCenter no se ven, consulte "[Plugin de Element para vCenter Server](#)" documentación sobre solución de problemas del plugin.



Después de actualizar al plugin de NetApp Element para vCenter Server 4.8 o una versión posterior con VMware vCenter Server 6.7U1, si los clústeres de almacenamiento no se muestran en la lista o se muestra un error de servidor en las secciones **Clusters** y **Configuración de QoSSIOC** de la configuración de NetApp Element, consulte "[Plugin de Element para vCenter Server](#)" documentación sobre la solución de problemas de estos errores.

9. Verifique el cambio de versión en la ficha **Acerca de** del punto de extensión **Configuración NetApp Element** del plugin.

Debería ver los detalles o detalles de la siguiente versión de una versión más reciente:

```
NetApp Element Plug-in Version: 5.3
NetApp Element Plug-in Build Number: 9
```



El plugin de vCenter incluye contenido de ayuda en línea. Para garantizar que la ayuda en línea incluya el contenido más reciente, borre la memoria caché del navegador después de actualizar el plugin.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Ejecute comprobaciones de estado del nodo de computación antes de actualizar el firmware de computación

Debe ejecutar comprobaciones de estado antes de actualizar el firmware de computación para garantizar que todos los nodos de computación del clúster estén listos para la actualización. Las comprobaciones de estado de los nodos de computación solo se pueden ejecutar en clústeres de computación de uno o más nodos de computación de NetApp HCI gestionados.

Lo que necesitará

- **Servicios de administración:** Ha actualizado el último paquete de servicios de administración (2.11 o posterior).
- **Nodo de gestión:** Está ejecutando el nodo de gestión 11.3 o posterior.
- **Software Element:** El clúster de almacenamiento ejecuta el software NetApp Element 11.3 o posterior.
- **Contrato de licencia para el usuario final (CLUF):** A partir de los servicios de gestión 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la IU o API de control de cloud híbrido de NetApp para ejecutar comprobaciones de estado de los nodos de computación:
 - a. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

- b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de comprobación del estado

Puede realizar comprobaciones del estado con la interfaz de usuario de control del cloud híbrido de NetApp o la API de control del cloud híbrido de NetApp:

- [Utilice control de cloud híbrido de NetApp para ejecutar comprobaciones de estado del nodo de computación antes de actualizar el firmware](#) (Método preferido)
- [Utilice API para ejecutar comprobaciones del estado del nodo de computación antes de actualizar el firmware](#)

También puede obtener más información acerca de las comprobaciones de estado de los nodos de computación que ejecuta el servicio:

- [El servicio de computación realiza las comprobaciones de estado del nodo](#)

Utilice control de cloud híbrido de NetApp para ejecutar comprobaciones de estado del nodo de computación antes de actualizar el firmware

Con Hybrid Cloud Control de NetApp, puede verificar que un nodo de computación esté listo para la actualización del firmware.




Si tiene varias configuraciones de clústeres de almacenamiento de dos nodos, cada una dentro de su propia instancia de vCenter, es posible que las comprobaciones del estado de los nodos de testigos no informen de forma precisa. Por lo tanto, cuando esté listo para actualizar hosts ESXi, solo debe apagar el nodo de testigo en el host ESXi que se está actualizando. Debe asegurarse de tener siempre un nodo testigo en ejecución en la instalación de NetApp HCI apagando los nodos testigo de forma alternativa.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>/hcc
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione la ficha **firmware de computación**.
5. Seleccione la comprobación del estado  para el clúster que desea comprobar si está listo para la actualización.
6. En la página **Compute Health Check**, seleccione **Run Health Check**.
7. Si hay problemas, la página proporciona un informe. Haga lo siguiente:
 - a. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la solución especificada.
 - b. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente.
 - c. Después de resolver los problemas del clúster, seleccione **Volver a ejecutar comprobación del estado**.

Cuando la comprobación del estado se completa sin errores, los nodos de computación del clúster están listos para actualizar. Consulte "[Actualice el firmware del nodo de computación](#)" para continuar.

Utilice API para ejecutar comprobaciones del estado del nodo de computación antes de actualizar el firmware

Es posible usar la API DE REST para verificar que los nodos de computación de un clúster estén listos para actualizarse. La comprobación del estado verifica que no haya obstáculos para la actualización, como problemas del host ESXi u otros problemas de vSphere. Tendrá que ejecutar comprobaciones del estado de los nodos de computación para cada clúster de computación del entorno.

Pasos

1. Busque el ID de controladora y el ID de clúster:

- a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
- ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
- iii. Seleccione **autorizar** para iniciar una sesión.

- c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.

- d. Seleccione **probar**.

- e. Seleccione **Ejecutar**.

- f. Del cuerpo de respuesta del código 200, copie el "id" para la instalación que tiene previsto utilizar para las comprobaciones de estado.

- g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /installations/{id}**.

- h. Seleccione **probar**.

- i. Introduzca el ID de instalación.

- j. Seleccione **Ejecutar**.

- k. Desde el cuerpo de respuesta del código 200, copie los ID de cada una de las siguientes opciones:

- i. El ID del clúster ("`clusterID`")
- ii. Un ID de controladora ("`controllerId`")

```

{
  "_links": {
    "collection":
    "https://10.117.187.199/inventory/1/installations",
    "self":
    "https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-
    412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-
          4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ]
    },
  },
}

```

2. Ejecute comprobaciones del estado de los nodos de computación en el clúster:

- a. Abra la interfaz de usuario de API DE REST de servicio de computación en el nodo de gestión:

```
https://<ManagementNodeIP>/vcenter/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
- i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
 - iii. Seleccione **autorizar** para iniciar una sesión.
- c. Seleccione **POST /compute/{CONTROLLER_ID}/health-checks**.
- d. Seleccione **probar**.
- e. Introduzca el "controllerId" Ha copiado desde el paso anterior en el campo de parámetro **Controller_ID**.

- f. En la carga útil, introduzca el "clusterId" que ha copiado del paso anterior como "cluster" y elimine el "nodes" parámetro.

```
{
  "cluster": "domain-1"
}
```

- g. Seleccione **Ejecutar** para ejecutar una comprobación del estado en el clúster.

La respuesta del código 200 da un "resourceLink" Se añade la URL con el ID de tarea que se necesita para confirmar los resultados de la comprobación del estado.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This
is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

- a. Copie la parte ID de tarea de "resourceLink" URL para verificar el resultado de la tarea.
3. Compruebe el resultado de las comprobaciones del estado:
- a. Volver a la interfaz de usuario de API DE REST de servicio de computación en el nodo de gestión:

```
https://<ManagementNodeIP>/vcenter/1/
```

- b. Seleccione **GET /compute/tases/{task_id}**.
- c. Seleccione **probar**.
- d. Introduzca la parte ID de tarea de "resourceLink" URL de la respuesta * POST /compute /{CONTROLLER_ID}/health-checks* code 200 en la task_id campo de parámetros.
- e. Seleccione **Ejecutar**.
- f. Si la status devuelto indica que se han producido problemas relacionados con el estado del nodo de computación, realice lo siguiente:
- Vaya al artículo específico de la KB (KbLink) en la lista de cada problema o realice la solución especificada.
 - Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente.
 - Después de resolver los problemas del clúster, vuelva a ejecutar **POST /compute /{CONTROLLER_ID}/health-checks** (consulte el paso 2).

Si las comprobaciones de estado se completan sin problemas, el código de respuesta 200 indica un resultado satisfactorio.

El servicio de computación realiza las comprobaciones de estado del nodo

Las comprobaciones del estado de computación, ya sea realizadas por los métodos de control del cloud híbrido de NetApp o API, realizan las siguientes comprobaciones por nodo. En función del entorno, es posible que se omitan algunas de estas comprobaciones. Debe volver a ejecutar las comprobaciones del estado después de resolver los problemas detectados.

Compruebe la descripción	Nodo/clúster	Acción necesaria para resolver	Artículo de la base de conocimientos con procedimiento
¿Está DRS habilitado y totalmente automatizado?	Clúster	Active DRS y asegúrese de que está totalmente automatizado.	" Consulte esta base de conocimientos ". NOTA: Si tiene licencia estándar, ponga el host ESXi en modo de mantenimiento y ignore esta advertencia de fallo de comprobación de estado.
¿DPM está deshabilitado en vSphere?	Clúster	Desactive Administración de energía distribuida.	" Consulte esta base de conocimientos ".
¿Está deshabilitado el control de admisión de alta disponibilidad en vSphere?	Clúster	Desactive el control de admisión de alta disponibilidad.	" Consulte esta base de conocimientos ".
¿ESTÁ HABILITADO FT para una máquina virtual en un host del clúster?	Nodo	Suspender tolerancia a fallos en cualquier máquina virtual afectada.	" Consulte esta base de conocimientos ".
¿Hay alarmas críticas en vCenter para el clúster?	Clúster	Inicie vSphere y resuelva y/o reconozca todas las alertas antes de continuar.	No se necesitan KB para resolver el problema.
¿Hay alertas informativas generales/globales en vCenter?	Clúster	Inicie vSphere y resuelva y/o reconozca todas las alertas antes de continuar.	No se necesitan KB para resolver el problema.
¿Están actualizados los servicios de gestión?	Sistema HCI de NetApp	Es necesario actualizar los servicios de gestión antes de realizar una actualización o ejecutar comprobaciones del estado previas a la actualización.	No se necesitan KB para resolver el problema. Consulte " este artículo " si quiere más información.
¿Hay errores en el nodo ESXi actual en vSphere?	Nodo	Inicie vSphere y resuelva y/o reconozca todas las alertas antes de continuar.	No se necesitan KB para resolver el problema.
¿Hay soportes virtuales montados en un equipo virtual en un host del clúster?	Nodo	Desmante todos los discos de medios virtuales (CD/DVD/floppy) de las máquinas virtuales.	No se necesitan KB para resolver el problema.

Compruebe la descripción	Nodo/clúster	Acción necesaria para resolver	Artículo de la base de conocimientos con procedimiento
¿Es la versión de BMC la versión mínima requerida que tiene soporte de redfish?	Nodo	Actualice manualmente el firmware del BMC.	No se necesitan KB para resolver el problema.
¿El host ESXi está en funcionamiento?	Nodo	Inicie el host ESXi.	No se necesitan KB para resolver el problema.
¿Residen máquinas virtuales en el almacenamiento ESXi local?	Nodo/máquina virtual	Quite o migre almacenamiento local conectado a máquinas virtuales.	No se necesitan KB para resolver el problema.
¿Está BMC en funcionamiento?	Nodo	Encienda su BMC y asegúrese de que está conectado a una red a la que puede llegar este nodo de gestión.	No se necesitan KB para resolver el problema.
¿Hay hosts ESXi de partners disponibles?	Nodo	Hacer que uno o más hosts ESXi del clúster estén disponibles (no en modo de mantenimiento) para migrar máquinas virtuales.	No se necesitan KB para resolver el problema.
¿Puede conectarse con BMC a través del protocolo IPMI?	Nodo	Habilite el protocolo IPMI en la controladora de gestión de placa base (BMC).	No se necesitan KB para resolver el problema.
¿El host ESXi se asigna correctamente al host de hardware (BMC)?	Nodo	El host ESXi no está asignado correctamente a la controladora de gestión de placa base (BMC). Corrija la asignación entre el host ESXi y el host hardware.	No se necesitan KB para resolver el problema. Consulte "este artículo" si quiere más información.
¿Cuál es el estado de los nodos testigos en el clúster? Ninguno de los nodos de testigos identificados está en funcionamiento.	Nodo	Un nodo de testigo no funciona en un host ESXi alternativo. Encienda el nodo testigo en un host ESXi alternativo y vuelva a ejecutar la comprobación del estado. Un nodo testigo debe estar en ejecución en la instalación de HCI en todo momento.	"Consulte esta base de conocimientos"

Compruebe la descripción	Nodo/clúster	Acción necesaria para resolver	Artículo de la base de conocimientos con procedimiento
¿Cuál es el estado de los nodos testigos en el clúster? El nodo de observación está activo y en ejecución en este host ESXi, y el nodo de observación alternativo no está en funcionamiento.	Nodo	Un nodo de testigo no funciona en un host ESXi alternativo. Encienda el nodo de testigo en un host ESXi alternativo. Cuando esté listo para actualizar este host ESXi, apague el nodo testigo que se ejecute en este host ESXi y vuelva a ejecutar la comprobación del estado. Un nodo testigo debe estar en ejecución en la instalación de HCI en todo momento.	"Consulte esta base de conocimientos"
¿Cuál es el estado de los nodos testigos en el clúster? El nodo testigo está activo y en ejecución en este host ESXi y el nodo alternativo está en funcionamiento, pero se ejecuta en el mismo host ESXi.	Nodo	Los dos nodos testigos se ejecutan en este host ESXi. Reubique un nodo de testigo en un host ESXi alternativo. Cuando esté listo para actualizar este host ESXi, apague el nodo de testigo que queda en este host ESXi y vuelva a ejecutar la comprobación del estado. Un nodo testigo debe estar en ejecución en la instalación de HCI en todo momento.	"Consulte esta base de conocimientos"
¿Cuál es el estado de los nodos testigos en el clúster? El nodo de testigo está activo y en ejecución en este host ESXi y el nodo de observación alternativo está en funcionamiento en otro host ESXi.	Nodo	Un nodo de testigo se ejecuta localmente en este host ESXi. Cuando esté listo para actualizar este host ESXi, apague el nodo testigo solo en este host ESXi y vuelva a ejecutar la comprobación del estado. Un nodo testigo debe estar en ejecución en la instalación de HCI en todo momento.	"Consulte esta base de conocimientos"

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualice las controladoras del nodo de computación

Para cualquier nodo de computación H-Series, se pueden actualizar los controladores que se usan en los nodos mediante VMware Update Manager.

Lo que necesitará

Consulte la matriz de firmware y controlador para el hardware en "[Versiones de firmware y controlador ESXi compatibles](#)".

Acerca de esta tarea

Ejecute solo una de estas operaciones de actualización a la vez.

Debe comprobar la versión del controlador ESXi actual antes de intentar actualizar el firmware de computación. Si el conductor no está actualizado, actualice primero el controlador. A continuación, actualice el firmware de computación para los nodos de computación.

Pasos

1. Vaya a la "[Descargas de software de NetApp HCI](#)" Y seleccione el enlace de descarga para la versión correcta de NetApp HCI.
2. Seleccione **ESXi_drivers** en la lista desplegable.
3. Acepte el contrato de licencia para usuario final.
4. Descargue el paquete de controladores para el tipo de nodo y la versión ESXi.
5. Extraiga el paquete de controladores descargado en el equipo local.



El paquete de controladores de NetApp incluye uno o varios archivos ZIP del paquete sin conexión de VMware; no extraiga estos archivos ZIP.

6. Vaya a **VMware Update Manager** en VMware vCenter.
7. Importe el archivo del paquete sin conexión del controlador para los nodos de computación al **repositorio de parches**.
 - Para VMware ESXi 7.0, todos los controladores necesarios para los nodos de computación H610C, H615C, H410C y Hx00E de NetApp, y sus componentes del sistema de compilación se incluyen en la imagen ISO estándar de instalación de VMware ESXi 7.0. No se requieren controladores adicionales o actualizados para los nodos de computación de NetApp HCI que ejecuten VMware ESXi 7.0 (y actualizaciones).
 - En el caso de VMware ESXi 6.x, realice los siguientes pasos para importar el archivo del paquete sin conexión del controlador:
 - i. Seleccione la ficha **actualizaciones**.
 - ii. SELECCIONE **CARGAR DESDE ARCHIVO**.
 - iii. Busque el paquete offline que se descargó anteriormente y seleccione **IMPORT**.
8. Cree una nueva base de host para el nodo de computación.
9. Elija **extensión de host** para Nombre y Tipo y seleccione todos los paquetes de controladores importados que se incluirán en la nueva línea de base.
10. En el menú **Host and Clusters** de vCenter, seleccione el clúster con los nodos de computación que desea actualizar y desplácese hasta la pestaña **Update Manager**.
11. Seleccione **solucionar** y seleccione la línea base del host recién creado. Asegúrese de que los

controladores incluidos en la línea de base están seleccionados.

- Continúe con el asistente hasta **Opciones de resolución de host** y asegúrese de que la opción **no cambiar estado de alimentación de VM** está seleccionada para mantener las máquinas virtuales en línea durante la actualización del controlador.



Si está habilitado el programador de recursos distribuidos de VMware (DRS) en el clúster (este es el valor predeterminado en las instalaciones de NetApp HCI), las máquinas virtuales se migrarán automáticamente a otros nodos del clúster.

- Vaya a la página **preparado para completar** del asistente y seleccione **Finalizar**.

Las controladoras para todos los nodos de computación del clúster se actualizan de uno en uno mientras las máquinas virtuales permanecen en línea.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Actualizar el firmware del nodo de computación

Para los nodos de computación H-Series, puede actualizar el firmware para componentes de hardware como BMC, BIOS y NIC. Para actualizar el firmware de los nodos de computación, se puede usar la interfaz de usuario de control de cloud híbrido de NetApp, la API de REST, una unidad USB con la imagen de firmware más reciente o la interfaz de usuario de BMC.

Después de la actualización, el nodo de computación arranca en ESXi y funciona como antes, y se conserva la configuración.

Lo que necesitará

- Controladores de computación:** Ha actualizado los controladores de nodo de computación. Si los controladores del nodo de computación no son compatibles con el nuevo firmware, la actualización no se iniciará. Consulte ["Herramienta de matriz de interoperabilidad \(IMT\)"](#) para obtener información sobre compatibilidad de controladores y firmware, y compruebe la última ["notas de la versión del firmware del nodo de computación"](#) para obtener información importante sobre el controlador y el firmware de última hora.
- Privilegios de administrador:** Dispone de permisos de administrador de clúster y administrador de BMC para realizar la actualización.
- Puertos del sistema:** Si utiliza NetApp Hybrid Cloud Control para actualizaciones, se ha asegurado de que los puertos necesarios están abiertos. Consulte ["Puertos de red"](#) si quiere más información.
- Versiones mínimas de BMC y BIOS:** El nodo que pretende actualizar mediante el control del cloud híbrido de NetApp cumple con los siguientes requisitos mínimos:

Modelo	Versión mínima del BMC	Versión mínima del BIOS
H410C	Todas las versiones compatibles (no se requiere actualización)	Todas las versiones compatibles (no se requiere actualización)
H610C	3.96.07	3B01

Modelo	Versión mínima del BMC	Versión mínima del BIOS
H615C	4.68.07	3B08.CO



Los nodos de computación H615C deben actualizar el firmware de BMC a la versión 4.68 mediante el ["paquete de firmware de computación 2.27"](#) Hacer que el control del cloud híbrido de NetApp pueda realizar futuras actualizaciones de firmware.



Para obtener una matriz completa de firmware y firmware de controlador para su hardware, consulte ["Versiones de firmware y controlador ESXi compatibles"](#).

- **Orden de inicio del BIOS:** Cambie manualmente el orden de inicio en la configuración del BIOS para que cada nodo se asegure USB CD/DVD aparece en la lista de arranque. Vea esto ["artículo"](#) si quiere más información.
- **Credenciales de BMC:** Actualice las credenciales que NetApp Hybrid Cloud Control utiliza para conectarse al nodo de computación BMC. Puede hacerlo utilizando el control del cloud híbrido de NetApp ["UI"](#) o ["API"](#). La actualización de la información de BMC antes de actualizar el inventario y garantiza que los servicios de los nodos de gestión conozcan todos los parámetros de hardware necesarios para completar la actualización.
- **Medios conectados:** Desconecte cualquier USB físico o ISO antes de iniciar una actualización del nodo de computación.
- **Consola KVM ESXi:** Cierre todas las sesiones abiertas Serial-over-LAN (sol) y las sesiones activas KVM en la interfaz de usuario de BMC antes de iniciar una actualización de nodo de computación.
- **Requisitos del nodo testigo:** En clústeres de almacenamiento de dos y tres nodos, uno ["Nodo de testimonio"](#) Debe ejecutarse en todo momento en la instalación de NetApp HCI.
- **Verificación del estado del nodo de computación:** Ha comprobado que el nodo está listo para actualizarse. Consulte ["Ejecute comprobaciones de estado del nodo de computación antes de actualizar el firmware de computación"](#).
- **Contrato de licencia para el usuario final (CLUF):** A partir de los servicios de administración 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la UI o API de control de cloud híbrido de NetApp para actualizar el firmware del nodo de computación:

- Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

- Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
- Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
- Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Acerca de esta tarea

En los entornos de producción, actualice el firmware en un nodo de computación a la vez.



El host ESXi debe estar fuera de modo de bloqueo antes de ejecutar una comprobación de estado y continuar con la actualización del firmware. Consulte ["Cómo deshabilitar el modo de bloqueo en un host ESXi"](#) y.. ["Comportamiento del modo de bloqueo de VMware"](#) si quiere más información.

Para actualizaciones de la API o la interfaz de usuario de control de cloud híbrido de NetApp, el host ESXi se colocará automáticamente en modo de mantenimiento durante el proceso de actualización si tiene la función DRS y la licencia necesaria. El nodo se reiniciará y una vez que finalice el proceso de actualización, el host ESXi se despondrá del modo de mantenimiento. Para las opciones de interfaz de usuario de USB y BMC, deberá colocar el host ESXi en modo de mantenimiento manualmente, tal y como se describe en cada procedimiento.



Antes de la actualización, compruebe la versión actual del controlador ESXi. Si el conductor no está actualizado, actualice primero el controlador. A continuación, actualice el firmware de computación para los nodos de computación.

Opciones de actualización

Elija la opción que sea relevante para su situación de actualización:

- [Utilice la interfaz de usuario de Cloud Control de NetApp para actualizar un nodo de computación](#) (Recomendado)
- [Utilice la API de control de cloud híbrido de NetApp para actualizar un nodo de computación](#)
- [Utilice una unidad USB expuesta con el paquete de firmware de computación más reciente](#)
- [Usar la interfaz de usuario \(UI\) de la controladora de gestión de placa base \(BMC\)](#)

Utilice la interfaz de usuario de Cloud Control de NetApp para actualizar un nodo de computación

A partir de los servicios de gestión 2.14, es posible actualizar un nodo de computación mediante la interfaz de usuario de control de cloud híbrido de NetApp. En la lista de nodos, debe seleccionar el nodo que desea actualizar. La ficha **versiones actuales** muestra las versiones actuales del firmware y la ficha **versiones propuestas** muestra las versiones de actualización disponibles, si las hay.



Para una actualización correcta, compruebe que la comprobación del estado del clúster de vSphere se haya realizado correctamente.



Actualizar el NIC, el BIOS y el BMC pueden tardar aproximadamente 60 minutos por nodo en función de la velocidad de la conectividad de red entre el nodo de gestión y el host BMC.



Ya no se admite el uso de la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el firmware de computación en los nodos de computación H300E/H500E/H700E. Para actualizar, use un [Unidad USB](#) o la [IU DE BMC](#) para montar el bundle de firmware de computación.

Lo que necesitará

- Si el nodo de gestión no está conectado a Internet, se descargó el paquete de firmware de computación del ["Sitio de soporte de NetApp"](#).



Debe extraer el TAR.GZ archivo a TAR y, a continuación, extraiga el TAR archivo al bundle de firmware de computación.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione **firmware de computación**.
5. Seleccione el clúster que desea actualizar.

Verá los nodos del clúster junto con las versiones de firmware actuales y las versiones más recientes, si están disponibles para su actualización.

6. Seleccione **examinar** para cargar el paquete de firmware de computación que descargó de "[Sitio de soporte de NetApp](#)".
7. Espere a que finalice la carga. Una barra de progreso muestra el estado de la carga.



La carga del archivo se realizará en segundo plano si se desplaza fuera de la ventana del explorador.

Se muestra un mensaje en pantalla después de que el archivo se haya cargado y validado correctamente. La validación puede tardar varios minutos.

8. Seleccione el bundle de firmware de computación.
9. Seleccione **Iniciar actualización**.

Después de seleccionar **Iniciar actualización**, la ventana muestra comprobaciones de estado fallidas, si las hay.



La actualización no se puede pausar una vez que se inicia. El firmware se actualizará secuencialmente en el siguiente orden: NIC, BIOS y BMC. No inicie sesión en la interfaz de usuario del BMC durante la actualización. Al iniciar sesión en el BMC se finaliza la sesión de control de nube híbrida en serie en LAN (sol) que supervisa el proceso de actualización.

10. Si las comprobaciones de estado del clúster o del nodo pasan con advertencias, pero sin fallos críticos, verá **preparado para actualizarse**. Seleccione **Actualizar nodo**.



Mientras la actualización está en curso, puede salir de la página y volver a ella más tarde para continuar supervisando el progreso. Durante la actualización, la interfaz de usuario muestra varios mensajes acerca del estado de la actualización.



Al actualizar el firmware en los nodos de computación H610C y H615C, no abra la consola de serie en LAN (sol) a través de la interfaz de usuario web de BMC. Esto puede provocar un error en la actualización.

La interfaz de usuario muestra un mensaje una vez completada la actualización. Es posible descargar registros una vez completada la actualización. Para obtener más información sobre los distintos cambios

de estado de actualización, consulte [Cambios de estado de actualización](#).



Si se produce un fallo durante la actualización, el control de cloud híbrido de NetApp reinicia el nodo, lo desconecta del modo de mantenimiento y muestra el estado del fallo con un enlace al registro de errores. Puede descargar el registro de errores, que contiene instrucciones específicas o vínculos a artículos de la base de conocimientos, para diagnosticar y corregir cualquier problema. Para obtener información adicional sobre los problemas de actualización del firmware de los nodos de computación mediante el control de cloud híbrido de NetApp, consulte este tema "KB" artículo.

Cambios de estado de actualización

A continuación, se muestran los distintos estados que la interfaz de usuario muestra antes, durante y después del proceso de actualización:

Estado de actualización	Descripción
Nodo con errores una o varias comprobaciones de estado. Expanda para ver los detalles.	Error en una o más comprobaciones del estado.
Error	Se produjo un error durante la actualización. Puede descargar el registro de errores y enviarlo al soporte de NetApp.
No se puede detectar	Este estado se muestra si el control de cloud híbrido de NetApp no puede consultar el nodo de computación cuando el activo de nodo de computación no tiene la etiqueta de hardware.
Listo para actualizarse.	Todas las comprobaciones de estado se han pasado correctamente y el nodo está listo para actualizarse.
Se produjo un error durante la actualización.	La actualización genera esta notificación cuando se produce un error grave. Descargue los registros seleccionando el enlace Descargar registros para ayudar a resolver el error. Puede intentar actualizar de nuevo después de resolver el error.
La actualización del nodo está en curso.	La actualización está en curso. Una barra de progreso muestra el estado de la actualización.

Utilice la API de control de cloud híbrido de NetApp para actualizar un nodo de computación

Puede utilizar las API para actualizar cada nodo de computación en un clúster a la versión de firmware más reciente. Puede utilizar una herramienta de automatización que prefiera para ejecutar las API. El flujo de trabajo de API que se documenta aquí, utiliza la interfaz de usuario de API DE REST disponible en el nodo de gestión como ejemplo.



Ya no se admite el uso de la interfaz de usuario de NetApp Hybrid Cloud Control para actualizar el firmware de computación en los nodos de computación H300E/H500E/H700E. Para actualizar, use un [Unidad USB](#) o la [IU DE BMC](#) para montar el bundle de firmware de computación.

Lo que necesitará

Los activos de nodos de computación, incluidos los activos de hardware y vCenter, deben conocer los activos

de los nodos de gestión. Puede usar las API del servicio de inventario para verificar activos (<https://<ManagementNodeIP>/inventory/1/>).

Pasos

1. Vaya al software NetApp HCI "[descargue la página](#)" y descargue el paquete de firmware de computación más reciente en un dispositivo al que se pueda acceder el nodo de gestión.
2. Cargue el paquete de firmware de computación en el nodo de gestión:
 - a. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
 - c. En la interfaz de usuario DE LA API DE REST, seleccione **POST /packages**.
 - d. Seleccione **probar**.
 - e. Seleccione **Browse** y seleccione el paquete de firmware de computación.
 - f. Seleccione **Ejecutar** para iniciar la carga.
 - g. En la respuesta, copie y guarde el ID de bundle de firmware de computación ("`id`") para usar en un paso posterior.
3. Compruebe el estado de la carga.
 - a. En la interfaz de usuario de la API DE REST, seleccione **GET /packages/{id}/status**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de paquete que ha copiado en el paso anterior en `id`.
 - d. Seleccione **Ejecutar** para iniciar la solicitud de estado.

La respuesta indica `state` como `SUCCESS` cuando finalice.

- e. En la respuesta, copie y guarde el nombre de paquete de firmware de computación ("`name`") y la versión ("`version`") para usar en un paso posterior.
4. Busque el ID de controladora de computación y el ID de hardware de nodos para el nodo que planea actualizar:
 - a. Abra la interfaz de usuario de la API DE REST del servicio de inventario en el nodo de gestión:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.

- iii. Seleccione **autorizar** para iniciar una sesión.
- iv. Cierre la ventana de autorización.
- c. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations**.
- d. Seleccione **probar**.
- e. Seleccione **Ejecutar**.
- f. Desde la respuesta, copie el ID del activo de instalación ("id").
- g. En la interfaz de usuario DE LA API DE REST, seleccione **GET /Installations/{id}**.
- h. Seleccione **probar**.
- i. Pegue el ID de activo de instalación en el campo **id**.
- j. Seleccione **Ejecutar**.
- k. En la respuesta, copie y guarde el ID de controladora del clúster ("controllerId")Y el ID de hardware del nodo ("hardwareId") para usar en un paso posterior:

```
"compute": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterId": "Test-1B",
        "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
```

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.111.0.111",
      "credentialsAvailable": true,
      "credentialsValidated": true
    },
    "chassisSerialNumber": "111930011231",
    "chassisSlot": "D",
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",
    "model": "H410C",
```

5. Ejecute la actualización de firmware del nodo de computación:

- a. Abra la interfaz de usuario de API DE REST del servicio de hardware en el nodo de gestión:

```
https://<ManagementNodeIP>/hardware/2/
```

- b. Seleccione **autorizar** y complete lo siguiente:
 - i. Introduzca el nombre de usuario y la contraseña del clúster.
 - ii. Introduzca el ID de cliente as `mnode-client`.
 - iii. Seleccione **autorizar** para iniciar una sesión.
 - iv. Cierre la ventana de autorización.
- c. Seleccione **POST /Nodes/{hardware_id}/upgrades**.
- d. Seleccione **probar**.
- e. Introduzca el identificador de activo del host de hardware ("`hardwareId`" guardado de un paso anterior) en el campo parámetro.
- f. Haga lo siguiente con los valores de carga útil:
 - i. Conserve los valores "`force`": `false` y "`maintenanceMode`": `true`" De modo que las comprobaciones de estado se realizan en el nodo y el host ESXi se establece en modo de mantenimiento.
 - ii. Introduzca el ID de controladora del clúster ("`controllerId`" guardado de un paso anterior).
 - iii. Introduzca el nombre y la versión de paquete de firmware de computación que guardó en el paso anterior.

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

- g. Seleccione **Ejecutar** para iniciar la actualización.



La actualización no se puede pausar una vez que se inicia. El firmware se actualizará secuencialmente en el siguiente orden: NIC, BIOS y BMC. No inicie sesión en la interfaz de usuario del BMC durante la actualización. Al iniciar sesión en el BMC se finaliza la sesión de control de nube híbrida en serie en LAN (sol) que supervisa el proceso de actualización.

- h. Copie el ID de tarea de actualización que forma parte del enlace de recurso ("`resourceLink`") URL en la respuesta.
6. Verifique el progreso y los resultados de la actualización:
 - a. Seleccione **GET /task/{task_id}/logs**.
 - b. Seleccione **probar**.
 - c. Introduzca el ID de tarea desde el paso anterior en **Task_ID**.
 - d. Seleccione **Ejecutar**.

- e. Realice una de las siguientes acciones si existen problemas o requisitos especiales durante la actualización:

Opción	Pasos
Debe corregir los problemas de estado del clúster debido a <code>failedHealthChecks</code> mensaje en el cuerpo de respuesta.	<ul style="list-style-type: none"> i. Vaya al artículo de la base de conocimientos específico indicado para cada problema o realice la solución especificada. ii. Si se especifica un KB, complete el proceso descrito en el artículo de la base de conocimientos correspondiente. iii. Después de resolver los problemas del clúster, vuelva a autenticarse si es necesario y seleccione POST /Nodes/{hardware_id}/upgrades. iv. Repita los pasos descritos anteriormente en el paso de actualización.
Error en la actualización. Los pasos de mitigación no se enumeran en el registro de actualización.	<ul style="list-style-type: none"> i. Vea esto "Artículo de base de conocimientos" (se requiere inicio de sesión).

- f. Ejecute la API **GET /Task/{task_id}/logs** varias veces, según sea necesario, hasta que el proceso se complete.

Durante la actualización, el `status` lo que indica `running` si no se encuentra ningún error. A medida que se termina cada paso, el `status` el valor cambia a `completed`.

La actualización ha finalizado correctamente cuando el estado de cada paso es `completed` y la `percentageCompleted` el valor es 100.

7. (Opcional) confirme las versiones de firmware actualizadas para cada componente:

- a. Abra la interfaz de usuario de API DE REST del servicio de hardware en el nodo de gestión:

```
https://<ManagementNodeIP>/hardware/2/
```

- b. Seleccione **autorizar** y complete lo siguiente:

- i. Introduzca el nombre de usuario y la contraseña del clúster.
- ii. Introduzca el ID de cliente as `mnode-client`.
- iii. Seleccione **autorizar** para iniciar una sesión.
- iv. Cierre la ventana de autorización.

- c. En la interfaz de usuario de LA API DE REST, seleccione **GET /nodes/{hardware_id}/upgrades**.

- d. (Opcional) Introduzca los parámetros de fecha y estado para filtrar los resultados.

- e. Introduzca el identificador de activo del host de hardware ("`hardwareId`" guardado de un paso anterior) en el campo parámetro.

- f. Seleccione **probar**.

- g. Seleccione **Ejecutar**.
- h. Verifique en la respuesta que el firmware de todos los componentes se ha actualizado correctamente de la versión anterior al firmware más reciente.

Utilice una unidad USB expuesta con el paquete de firmware de computación más reciente

Puede insertar una unidad USB con el paquete de firmware de computación más reciente descargado en un puerto USB del nodo de computación. Como alternativa al uso del método de unidad de memoria USB descrito en este procedimiento, puede montar el paquete de firmware de computación en el nodo de computación utilizando la opción **CD/DVD** virtual en la consola virtual en la interfaz del controlador de administración de la placa base (BMC). El método BMC tarda considerablemente más que el método USB de la unidad de memoria USB. Asegúrese de que su estación de trabajo o servidor tiene el ancho de banda de red necesario y de que la sesión del explorador con el BMC no agota el tiempo de espera.

Lo que necesitará

- Si el nodo de gestión no está conectado a Internet, se descargó el paquete de firmware de computación del "[Sitio de soporte de NetApp](#)".



Debe extraer el TAR.GZ archivo a TAR y, a continuación, extraiga el TAR archivo al bundle de firmware de computación.

Pasos

1. Utilice la utilidad etcher para actualizar el paquete de firmware de computación a una unidad USB.
2. Coloque el nodo de computación en modo de mantenimiento mediante VMware vCenter y evacue todas las máquinas virtuales del host.



Si está habilitado el programador de recursos distribuidos de VMware (DRS) en el clúster (este es el valor predeterminado en las instalaciones de NetApp HCI), las máquinas virtuales se migrarán automáticamente a otros nodos del clúster.

3. Inserte la unidad de almacenamiento USB en un puerto USB del nodo de computación y reinicie el nodo de computación mediante VMware vCenter.
4. Durante EL CICLO POSTERIOR del nodo de computación, pulse **F11** para abrir Boot Manager. Es posible que tenga que pulsar **F11** varias veces en sucesión rápida. Puede realizar esta operación conectando un vídeo/teclado o utilizando la consola de BMC.
5. Seleccione **One Shot > USB Flash Drive** en el menú que aparece. Si la unidad USB en miniatura no aparece en el menú, compruebe que la unidad flash USB forma parte del orden de inicio anterior del BIOS del sistema.
6. Pulse **Intro** para iniciar el sistema desde la unidad de memoria USB. Comienza el proceso de flash del firmware.

Una vez que se completa la actualización del firmware y el nodo se reinicia, es posible que ESXi demore unos minutos en iniciarse.

7. Una vez completado el reinicio, salga del modo de mantenimiento en el nodo de computación actualizado mediante vCenter.
8. Extraiga la unidad flash USB del nodo de computación actualizado.
9. Repita esta tarea para otros nodos de computación del clúster ESXi hasta que se actualicen todos los nodos de computación.

Usar la interfaz de usuario (UI) de la controladora de gestión de placa base (BMC)

Debe realizar los pasos secuenciales para cargar el paquete de firmware de computación y reiniciar el nodo en el bundle de firmware de computación a fin de garantizar que la actualización se realice correctamente. El paquete de firmware de computación debe estar ubicado en el sistema o la máquina virtual (VM) donde se aloja el explorador web. Verifique que se haya descargado el bundle de firmware de computación antes de iniciar el proceso.



Se recomienda tener el sistema o la máquina virtual y el nodo en la misma red.



La actualización a través de la interfaz de usuario de BMC tarda entre 25 y 30 minutos aproximadamente.

- [Actualice el firmware en los nodos H410C y H300E/H500E/H700E](#)
- [Actualice el firmware en los nodos H610C/H615C](#)

Actualice el firmware en los nodos H410C y H300E/H500E/H700E

Si su nodo forma parte de un clúster, debe colocar el nodo en modo de mantenimiento antes de la actualización y sacarlo del modo de mantenimiento después de la actualización.



Ignore el siguiente mensaje informativo que se muestra durante el proceso: `Untrusty Debug Firmware Key is used, SecureFlash is currently in Debug Mode`

Pasos

1. Si su nodo forma parte de un clúster, colóquelo en el modo de mantenimiento de la manera siguiente. Si no es así, vaya al paso 2.
 - a. Inicie sesión en el cliente web de VMware vCenter.
 - b. Haga clic con el botón derecho del ratón en el nombre del host (nodo de computación) y seleccione **modo de mantenimiento > Entrar en modo de mantenimiento**.
 - c. Seleccione **OK**. Las máquinas virtuales del host se migrarán a otro host disponible. La migración de equipos virtuales puede llevar tiempo, en función del número de equipos virtuales que se deban migrar.



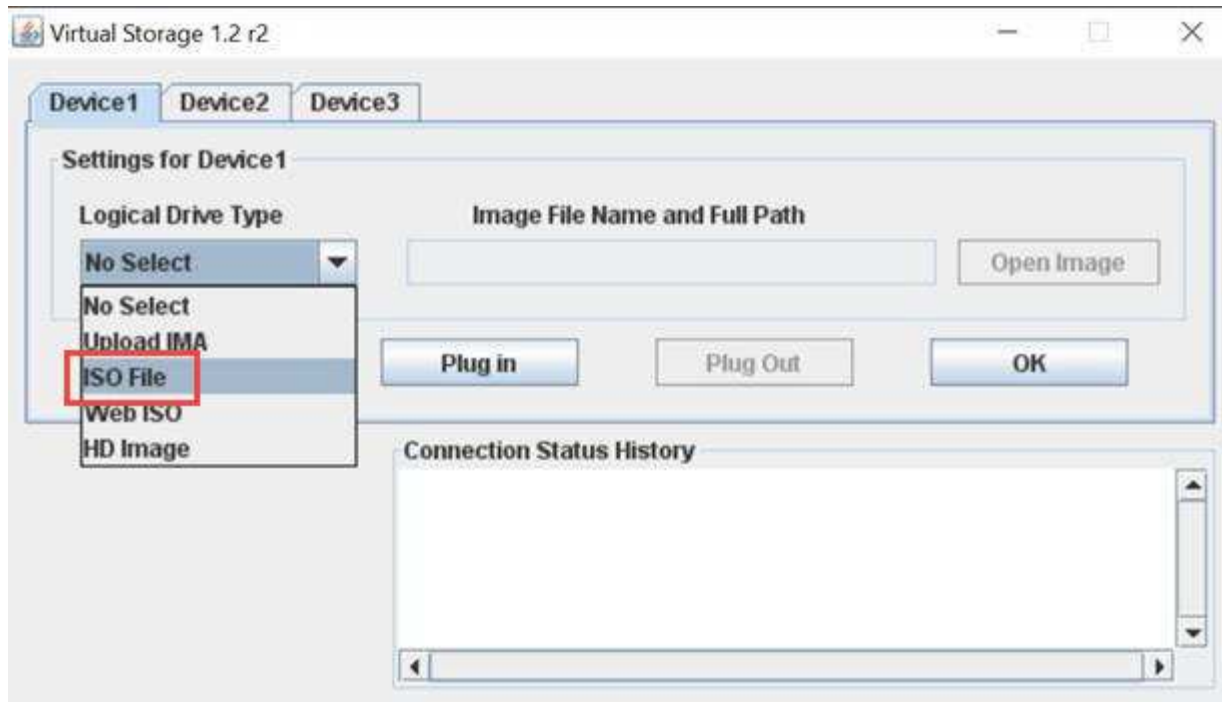
Asegúrese de que todas las máquinas virtuales del host estén migradas antes de continuar.

2. Vaya a la interfaz de usuario del BMC, <https://BMCIP/#login>, Donde BMCIP es la dirección IP del BMC.
3. Inicie sesión con sus credenciales.
4. Seleccione **Control remoto > Redirección de consola**.
5. Seleccione **Iniciar consola**.



Es posible que tenga que instalar Java o actualizarlo.

6. Cuando se abra la consola, seleccione **Medios virtuales > almacenamiento virtual**.
7. En la pantalla **almacenamiento virtual**, seleccione **Tipo de unidad lógica** y seleccione **Archivo ISO**.



8. Seleccione **Abrir imagen** para buscar la carpeta donde descargó el archivo del paquete de firmware de computación y seleccionar el archivo del paquete de firmware de computación.
9. Seleccione **Plug in**.
10. Cuando se muestra el estado de la conexión Device#: VM Plug-in OK!!, Seleccione **Aceptar**.
11. Reinicie el nodo pulsando **F12** y seleccionando **Reiniciar** o seleccionando **Control de energía > Configurar reinicio de energía**.
12. Durante el reinicio, pulse **F11** para seleccionar las opciones de inicio y cargar el paquete de firmware de computación. Es posible que tenga que pulsar F11 varias veces antes de que aparezca el menú de inicio.

Verá la siguiente pantalla:

```
ISOLINUX 6.84 6.84-pre1 ETCD Copyright (C) 1994-2015 H.
Ender Linux Installation LiveCD

Enter to boot: F1 for kernels F2 for options.
Booting ender
boot:
```

13. En la pantalla anterior, pulse **Intro**. Dependiendo de la red, puede que tarde unos minutos después de pulsar **Intro** para que comience la actualización.



Algunas de las actualizaciones del firmware podrían provocar que la consola se desconectara y/o provocarán la desconexión de la sesión en el BMC. Puede volver a iniciar sesión en el BMC, sin embargo, es posible que algunos servicios, como la consola, no estén disponibles debido a las actualizaciones del firmware. Una vez que hayan completado las actualizaciones, el nodo realizará un reinicio en frío, que puede tardar aproximadamente cinco minutos.

14. Vuelva a iniciar sesión en la interfaz de usuario del BMC y seleccione **sistema** para verificar la versión del BIOS y el tiempo de compilación después de iniciar el sistema operativo. Si la actualización se completó

correctamente, verá las nuevas versiones de BIOS y BMC.



La versión del BIOS no mostrará la versión actualizada hasta que el nodo haya terminado de arrancarse por completo.

15. Si el nodo forma parte de un clúster, complete los pasos a continuación. Si se trata de un nodo independiente, no se necesita realizar ninguna otra acción.
 - a. Inicie sesión en el cliente web de VMware vCenter.
 - b. Saque el host del modo de mantenimiento. Esto podría mostrar un indicador rojo desconectado. Espere a que se borren todos los Estados.
 - c. Encienda cualquiera de las máquinas virtuales restantes que se hayan apagado.

Actualice el firmware en los nodos H610C/H615C

Los pasos varían en función de si el nodo es independiente o forma parte de un clúster. El procedimiento puede tardar aproximadamente 25 minutos e incluye apagar el nodo, cargar el bundle de firmware de computación, actualizar los dispositivos y volver a encender el nodo después de la actualización.

Pasos

1. Si su nodo forma parte de un clúster, colóquelo en el modo de mantenimiento de la manera siguiente. Si no es así, vaya al paso 2.
 - a. Inicie sesión en el cliente web de VMware vCenter.
 - b. Haga clic con el botón derecho del ratón en el nombre del host (nodo de computación) y seleccione **modo de mantenimiento > Entrar en modo de mantenimiento**.
 - c. Seleccione **OK**. Las máquinas virtuales del host se migrarán a otro host disponible. La migración de equipos virtuales puede llevar tiempo, en función del número de equipos virtuales que se deban migrar.



Asegúrese de que todas las máquinas virtuales del host estén migradas antes de continuar.

2. Vaya a la interfaz de usuario del BMC, <https://BMCIP/#login>, Donde BMC IP es la dirección IP del BMC.
3. Inicie sesión con sus credenciales.
4. Seleccione **Control remoto > Iniciar KVM (Java)**.
5. En la ventana de la consola, seleccione **Media > Virtual Media Wizard**.



6. Seleccione **Browse** y seleccione el firmware de computación .iso archivo.
7. Seleccione **conectar**. Se muestra una ventana emergente que indica que se ha realizado correctamente, junto con la ruta y el dispositivo que se muestra en la parte inferior. Puede cerrar la ventana **Medios virtuales**.



8. Reinicie el nodo pulsando **F12** y seleccionando **Reiniciar** o seleccionando **Control de energía > Configurar reinicio de energía**.
9. Durante el reinicio, pulse **F11** para seleccionar las opciones de inicio y cargar el paquete de firmware de computación.
10. Seleccione **AMI Virtual CDROM** de la lista que se muestra y seleccione **Intro**. Si no ve el CDROM virtual de AMI en la lista, vaya al BIOS y active el CDROM en la lista de inicio. El nodo se reiniciará después de guardar. Durante el reinicio, pulse **F11**.



11. En la pantalla que aparece, seleccione **Intro**.



Algunas de las actualizaciones del firmware podrían provocar que la consola se desconectara y/o provocarán la desconexión de la sesión en el BMC. Puede volver a iniciar sesión en el BMC, sin embargo, es posible que algunos servicios, como la consola, no estén disponibles debido a las actualizaciones del firmware. Una vez que hayan completado las actualizaciones, el nodo realizará un reinicio en frío, que puede tardar aproximadamente cinco minutos.

12. Si se desconecta de la consola, seleccione **Control remoto** y seleccione **Iniciar KVM** o **Iniciar KVM (Java)** para volver a conectarse y verificar cuando el nodo haya terminado de arrancar de nuevo. Es posible que necesite volver a conectar varios para verificar que el nodo se haya iniciado correctamente.



Durante el proceso de encendido, durante aproximadamente cinco minutos, la consola KVM muestra **sin señal**.

13. Después de encender el nodo, seleccione **Panel > Información del dispositivo > más información** para verificar las versiones del BIOS y del BMC. Se muestran las versiones actualizadas de BIOS y BMC. No se mostrará la versión actualizada del BIOS hasta que el nodo se haya iniciado completamente.
14. Si colocó el nodo en modo de mantenimiento, después de que el nodo arranca en ESXi, haga clic con el botón derecho en el nombre del host (nodo de computación) y seleccione **modo de mantenimiento > salir del modo de mantenimiento** y migre las máquinas virtuales de nuevo al host.
15. En vCenter, con el nombre de host seleccionado, configure y verifique la versión de BIOS.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Automatice las actualizaciones de firmware de los nodos de computación con Ansible

Puede actualizar el firmware del sistema en los nodos de computación NetApp HCI, incluido el firmware para componentes como el BMC, el BIOS y la NIC mediante los flujos de trabajo del control de cloud híbrido de NetApp. Para instalaciones con clústeres informáticos de gran tamaño, puede automatizar los flujos de trabajo con Ansible para realizar una actualización gradual de todo el clúster.



Mientras que NetApp pone a disposición el rol de Ansible para automatizar las actualizaciones del firmware de los nodos de computación, la automatización es un componente auxiliar que requiere una configuración adicional y componentes de software para ejecutar. La modificación de la automatización de Ansible solo se admite cuando se realiza el mejor esfuerzo.



El rol de Ansible para las actualizaciones solo funciona en los nodos de computación de NetApp HCI H-Series. No se puede usar este rol para actualizar nodos de computación de terceros.

Lo que necesitará

- **Preparación y requisitos previos para las actualizaciones de firmware:** La instalación de NetApp HCI debe estar lista para la actualización del firmware, tal y como se indica en las instrucciones para ["realizando actualizaciones de firmware"](#).
- **Disponibilidad para ejecutar la automatización en el nodo de control de Ansible:** Un servidor físico o virtual para ejecutar la automatización de actualizaciones de firmware en Ansible.

Acerca de esta tarea

En un entorno de producción, debe actualizar los nodos de computación de un clúster en una instalación de NetApp HCI en forma gradual; un nodo después del otro, un nodo por vez. Las API que se encuentran en el control de cloud híbrido de NetApp organizan el proceso de actualización del firmware general de los nodos de computación para un único nodo de computación, incluida la ejecución de comprobaciones de estado, la colocación de ESXi en los nodos de computación en el mantenimiento y reiniciar el nodo de computación para aplicar las actualizaciones de firmware. El rol de Ansible proporciona la opción de orquestar la actualización del firmware para un grupo de nodos de computación o clústeres enteros.

Comience a utilizar la automatización de la actualización del firmware

Para comenzar, navegue hasta la ["Repositorio de Ansible de NetApp en GitHub"](#) y descargue el `nar_compute_nodes_firmware_upgrades` papel y documentación.

Obtenga más información

- ["Página de recursos de NetApp HCI"](#)

Actualice los componentes de vSphere para un sistema NetApp HCI con el plugin de Element para vCenter Server

Al actualizar los componentes de VMware vSphere de la instalación de NetApp HCI, tendrá que realizar algunos pasos adicionales al plugin de Element para vCenter Server.

Pasos

1. Para actualizaciones de vcsa, ["claro"](#) Configuración de QoSSIOC en el plugin (**Configuración de NetApp Element > Configuración de QoSSIOC**). Aparece el campo **Estado de QoSSIOC** `Not Configured` una vez completado el proceso.
2. Para actualizaciones de vcsa y Windows, ["cancele el registro"](#) El plugin desde la instancia de vCenter Server a la que se asocia mediante la utilidad de registro.
3. ["Actualice vSphere, incluidos vCenter Server, ESXi, VMs y otros componentes de VMware"](#).



Debe actualizar al plugin de NetApp Element para vCenter Server 5.0 o una versión posterior para otorgar la capacidad de implementar el plugin con VMware vCenter 7.0 Update 3 sin tener que aplicar una solución alternativa.

Con el plugin de Element para vCenter Server 4.x, cuando se actualiza a VMware vCenter Server 7.0 Update 3, el plugin 4.x no puede implementar. Para resolver este problema con Spring Framework 4, consulte ["Este artículo de la base de conocimientos"](#).



Al actualizar ESXi para nodos de computación para un ["clúster de dos nodos"](#), actualice sólo un nodo de computación a la vez para que solo un nodo testigo no esté disponible temporalmente y se pueda mantener el quórum del clúster.

4. ["Regístrese"](#) El plugin de Element para vCenter Server nuevamente con vCenter.
5. ["Añadir clústeres"](#) con el plugin.
6. ["Configure los ajustes de QoSSIOC"](#) con el plugin.
7. ["Habilite QoSSIOC"](#) para todos los almacenes de datos controlados por el plugin.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)
- ["Informe técnico de dos nodos de clúster de almacenamiento de NetApp HCI"](#)

Amplíe su sistema NetApp HCI

Visión general de la ampliación

Puede ampliar su sistema de NetApp HCI mediante el control de cloud híbrido de NetApp. Puede ampliar los recursos de almacenamiento o de computación por separado o ampliarlos al mismo tiempo.



Los nodos de almacenamiento H610S nuevos y de repuesto pueden tener requisitos de instalación adicionales según la versión existente del software Element del clúster de almacenamiento. Póngase en contacto con el soporte de NetApp si desea obtener más información.

Después de instalar el nodo en el chasis de NetApp HCI, utilice el control de cloud híbrido de NetApp para configurar NetApp HCI con el fin de utilizar los recursos nuevos. NetApp HCI detecta la configuración de red existente y ofrece opciones de configuración dentro de las redes y VLAN existentes, si las hubiera.



Si ha ampliado recientemente su instalación y los nuevos activos no se han añadido automáticamente a la configuración, es posible que deba agregar los activos manualmente. Consulte ["Información general sobre los nodos de gestión"](#).

NetApp HCI utiliza VMware Enhanced vMotion Compatibility (EVC) para garantizar la funcionalidad vMotion cuando hay nodos de computación con generaciones de CPU diferentes en el clúster de vSphere. Cuando se necesita EVC para la ampliación, NetApp HCI lo habilita automáticamente siempre que sea posible.

En las siguientes situaciones, es posible que deba cambiar manualmente la configuración de EVC en el cliente de vSphere para completar la ampliación:

- Los nodos de computación existentes tienen una generación de CPU más nueva que los nodos de computación que intenta añadir.
- La instancia de vCenter de control no admite el nivel de EVC requerido.
- Los nodos de computación que intenta añadir tienen una generación de CPU más antigua que la configuración de EVC de la instancia de vCenter de control.



Al ampliar los recursos de computación o almacenamiento de NetApp HCI en el motor de implementación de NetApp, debe conectarse a la instancia de vCenter que gestione los nodos de computación de NetApp HCI existentes.

Obtenga más información

- ["Amplíe los recursos de computación de NetApp HCI"](#)
- ["Amplíe los recursos de almacenamiento de NetApp HCI"](#)
- ["Amplíe los recursos informáticos y de almacenamiento de NetApp HCI al mismo tiempo"](#)
- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Amplíe los recursos de almacenamiento de NetApp HCI

Después de terminar la implementación de NetApp HCI, puede ampliar y configurar recursos de almacenamiento NetApp HCI mediante el control de cloud híbrido de NetApp.

Antes de empezar

- Asegúrese de tener direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (cada nodo nuevo debe instalarse en la misma red que los nodos existentes de su tipo).
- Asegúrese de tener uno de los siguientes tipos de cuentas de clúster de almacenamiento de SolidFire:
 - La cuenta de administrador nativa que se creó durante la implementación inicial
 - Una cuenta de usuario personalizada con permisos de administración de dominios, unidades, volúmenes y nodos
- Asegúrese de haber realizado las siguientes acciones con cada nodo nuevo:
 - Instaló el nodo nuevo en el chasis NetApp HCI siguiendo el "[instrucciones de instalación](#)".
 - Cableó y encendió el nodo nuevo
- Asegúrese de tener la dirección IPv4 de gestión de un nodo de almacenamiento ya instalado. Puede encontrar la dirección IP en la pestaña **Administración de NetApp Element > clúster > nodos** del plugin de NetApp Element para vCenter Server.
- Asegúrese de que cada nodo nuevo utilice la misma topología y el mismo cableado de red que los clústeres de computación o almacenamiento existentes.



Al ampliar los recursos de almacenamiento, la capacidad de almacenamiento debe dividirse de manera uniforme en todo el chasis para una mayor fiabilidad.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. Haga clic en **expandir** en la esquina superior derecha de la interfaz.

El explorador abre el motor de implementación de NetApp.

4. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

5. En la página **Bienvenido**, haga clic en **no** y haga clic en **continuar**.
6. En la página **Inventario disponible**, seleccione los nodos de almacenamiento que desea agregar y haga clic en **continuar**.
7. En la página **Configuración de red**, se ha detectado parte de la información de red desde la

implementación inicial. Cada nodo de almacenamiento nuevo se enumera por número de serie, y es necesario asignarle la información de red nueva. Complete los siguientes pasos para cada nodo de almacenamiento nuevo:

- a. **Nombre de host:** Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo prefijo de nomenclatura detectado e insértelo como prefijo para el nuevo nombre de host único que agregue en el campo Nombre de host.
- b. **Dirección de administración:** Introduzca una dirección IP de administración para el nuevo nodo de almacenamiento que se encuentra dentro de la subred de la red de administración.
- c. **Dirección IP de almacenamiento (iSCSI):** Introduzca una dirección IP iSCSI para el nuevo nodo de almacenamiento que se encuentra en la subred de la red iSCSI.
- d. Haga clic en **continuar**.



La NetApp HCI puede tardar algún tiempo en validar las direcciones IP especificadas. El botón continuar estará disponible cuando finalice la validación de la dirección IP.

8. En la página **Review** de la sección Network Settings (Configuración de red), los nodos nuevos se muestran en el texto en negrita. Para hacer cambios en cualquier sección, haga lo siguiente:
 - a. Haga clic en **Editar** para esa sección.
 - b. Después de terminar, haga clic en **continuar** en cualquier página posterior para volver a la página Revisión.
9. **Opcional:** Si no desea enviar estadísticas del clúster ni información de soporte a los servidores Active IQ alojados de NetApp, desactive la casilla de comprobación final.

Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.

10. Haga clic en **Agregar nodos**.

Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.

11. **Opcional:** Verifique que haya nodos de almacenamiento nuevos visibles en el plugin de Element para vCenter Server.



Si expandió un clúster de almacenamiento de dos nodos a cuatro nodos o más, la pareja de nodos testigo que anteriormente utilizaba el clúster de almacenamiento seguirá visible como máquinas virtuales en espera en vSphere. El clúster de almacenamiento recién ampliado no los utiliza; si desea recuperar recursos de equipos virtuales, puede hacerlo ["quitar manualmente"](#) Las máquinas virtuales del nodo de testigo.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Amplíe los recursos de computación de NetApp HCI

Después de terminar la implementación de NetApp HCI, puede ampliar y configurar

recursos de computación de NetApp HCI mediante el control de cloud híbrido de NetApp.

Antes de empezar

- Compruebe que la instancia de vSphere de NetApp HCI utilice licencia vSphere Enterprise Plus si se va a ampliar una implementación con switches virtuales distribuidos.
- Compruebe que ninguna de las instancias de vCenter o vSphere que se utilizan con NetApp HCI tenga licencias caducadas.
- Asegúrese de tener direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (cada nodo nuevo debe instalarse en la misma red que los nodos existentes de su tipo).
- Compruebe que dispone de las credenciales de cuenta de administrador de vCenter preparadas.
- Asegúrese de haber realizado las siguientes acciones con cada nodo nuevo:
 - Instaló el nodo nuevo en el chasis NetApp HCI siguiendo el "[instrucciones de instalación](#)".
 - Cableó y encendió el nodo nuevo
- Asegúrese de que cada nodo nuevo utilice la misma topología y el mismo cableado de red que los clústeres de computación o almacenamiento existentes.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. Haga clic en **expandir** en la esquina superior derecha de la interfaz.

El explorador abre el motor de implementación de NetApp.

4. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

5. En la página **Bienvenido**, haga clic en **Sí** y haga clic en **continuar**.
6. En la página **Licencia de usuario final**, lea el Contrato de licencia de usuario final de VMware y haga clic en **Acepto** para aceptar los términos y haga clic en **continuar**.
7. En la página **vCenter**, complete los siguientes pasos:
 - a. Introduzca un FQDN o una dirección IP y credenciales de administrador para la instancia de vCenter asociada con la instalación de NetApp HCI.
 - b. Haga clic en **continuar**.
 - c. Seleccione un centro de datos de vSphere en el que desea añadir los nodos de computación o haga clic en **Create New Datacenter** para añadir los nodos de computación a un centro de datos nuevo.



Si hace clic en Create New Datacenter, el campo Cluster se completa automáticamente.

- d. Si seleccionó un centro de datos existente, seleccione un clúster de vSphere con el que se deben

asociar los nodos de computación nuevos.



Si NetApp HCI no reconoce la configuración de red del clúster seleccionado para la ampliación, asegúrese de que la asignación vmkernel y vmnic para las redes de gestión, almacenamiento y vMotion estén establecidas con los valores predeterminados de puesta en marcha. Consulte "[cambios de red admitidos](#)" si quiere más información.

e. Haga clic en **continuar**.

8. En la página **ESXi Credentials**, introduzca la contraseña raíz de ESXi para los nodos de computación que va a añadir.

Debe usar la misma contraseña que se creó durante la implementación inicial de NetApp HCI.

9. Haga clic en **continuar**.

10. Si creó un nuevo clúster de centro de datos de vSphere, en la página **Network Topology**, seleccione una topología de red para que coincida con los nodos de computación nuevos que va a añadir.



Solo debe seleccionar la opción de dos cables si los nodos de computación utilizan la topología de dos cables y la implementación de NetApp HCI existente se configura con identificadores de VLAN.

11. En la página **Inventario disponible**, seleccione los nodos que desea agregar a la instalación existente de NetApp HCI.



En algunos nodos de computación, es posible que deba habilitar EV en el nivel más alto compatible con la versión de vCenter antes de poder añadirlos a la instalación. Debe utilizar el cliente de vSphere a fin de habilitar EVC para estos nodos de computación. Después de habilitar dicha función, actualice la página Inventory e intente añadir nuevamente los nodos de computación.

12. Haga clic en **continuar**.

13. **Opcional:** Si creó un nuevo clúster de centro de datos de vSphere, en la página **Configuración de red**, importe la información de la red desde una implementación de NetApp HCI existente seleccionando la casilla de verificación **Copiar configuración desde un clúster existente**.

Esto rellena la información de la pasarela y de la subred predeterminadas para cada red.

14. En la página **Configuración de red**, se ha detectado parte de la información de red desde la implementación inicial. Cada nodo de computación nuevo se enumera por número de serie, y es necesario asignarle información de red nueva. Para cada nodo de computación nuevo, complete los siguientes pasos:

- a. **Nombre de host:** Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo **prefijo de nomenclatura detectado** e insértelo como prefijo para el nuevo nombre de host.
- b. **Dirección IP de administración:** Introduzca una dirección IP de administración para el nuevo nodo informático que se encuentra en la subred de la red de administración.
- c. **IP Address** de vMotion: Introduzca una dirección IP de vMotion para el nuevo nodo de computación que se encuentra en la subred de la red de vMotion.
- d. **iSCSI A - IP Address:** Introduzca una dirección IP para el primer puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.

- e. **ISCSI B - Dirección IP:** Introduzca una dirección IP para el segundo puerto iSCSI del nodo de computación que está en la subred de la red iSCSI
 - f. Haga clic en **continuar**.
15. En la página **Review** de la sección Network Settings (Configuración de red), los nodos nuevos se muestran en el texto en negrita. Para hacer cambios en cualquier sección, haga lo siguiente:
- a. Haga clic en **Editar** para esa sección.
 - b. Después de terminar, haga clic en **continuar** en cualquiera de las páginas siguientes para volver a la página **revisar**.
16. **Opcional:** Si no desea enviar estadísticas del clúster ni información de soporte a los servidores SolidFire Active IQ alojados de NetApp, desactive la casilla de comprobación final.

Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.

17. Haga clic en **Agregar nodos**.

Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.

18. **Opcional:** Verifique que los nodos de computación nuevos estén visibles en VMware vSphere Web Client.

Obtenga más información

- ["Página de recursos de NetApp HCI"](#)
- ["Instrucciones de instalación y configuración para nodos de almacenamiento y de computación de NetApp HCI"](#)
- ["VMware Knowledge base: Soporte de procesador de Enhanced vMotion Compatibility \(EVC\)"](#)

Amplíe los recursos informáticos y de almacenamiento de NetApp HCI al mismo tiempo

Después de terminar la implementación de NetApp HCI, puede ampliar y configurar recursos de almacenamiento y computación de NetApp HCI al mismo tiempo utilizando Cloud Control de NetApp.

Antes de empezar

- Compruebe que la instancia de vSphere de NetApp HCI utilice licencia vSphere Enterprise Plus si se va a ampliar una implementación con switches virtuales distribuidos.
- Compruebe que ninguna de las instancias de vCenter o vSphere que se utilizan con NetApp HCI tenga licencias caducadas.
- Compruebe que dispone de las credenciales de cuenta de administrador de vCenter preparadas.
- Asegúrese de tener direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (cada nodo nuevo debe instalarse en la misma red que los nodos existentes de su tipo).
- Asegúrese de tener uno de los siguientes tipos de cuentas de clúster de almacenamiento de SolidFire:
 - La cuenta de administrador nativa que se creó durante la implementación inicial
 - Una cuenta de usuario personalizada con permisos de administración de dominios, unidades,

volúmenes y nodos

- Asegúrese de haber realizado las siguientes acciones con cada nodo nuevo:
 - Instaló el nodo nuevo en el chasis NetApp HCI siguiendo el "[instrucciones de instalación](#)".
 - Cableó y encendió el nodo nuevo
- Asegúrese de tener la dirección IPv4 de gestión de un nodo de almacenamiento ya instalado. Puede encontrar la dirección IP en la pestaña **Administración de NetApp Element > clúster > nodos** del plugin de NetApp Element para vCenter Server.
- Asegúrese de que cada nodo nuevo utilice la misma topología y el mismo cableado de red que los clústeres de computación o almacenamiento existentes.

Acerca de esta tarea

- Es posible combinar el nodo de computación H410C con los nodos existentes de computación y de almacenamiento de NetApp HCI en el mismo chasis y clúster.
- No es posible combinar nodos de computación con nodos de computación habilitados para BPU en el mismo clúster. Si selecciona un nodo de computación habilitado para GPU, los nodos de computación solo para CPU pasan a ser inseleccionables y viceversa.
- Debe habilitar EVC antes de continuar si va a añadir nodos de computación con generaciones de CPU que son diferentes a la generación de CPU de los nodos de computación existentes, y la función Enhanced vMotion Compatibility (EVC) está deshabilitada en la instancia de vCenter de control. Esto garantiza que se complete la funcionalidad vMotion después de la ampliación.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. Haga clic en **expandir** en la esquina superior derecha de la interfaz.

El explorador abre el motor de implementación de NetApp.

4. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

5. En la página **Bienvenido**, haga clic en **Sí** y haga clic en **continuar**.
6. En la página **Licencia de usuario final**, lea el Contrato de licencia de usuario final de VMware y haga clic en **Acepto** para aceptar los términos y haga clic en **continuar**.
7. En la página **vCenter**, complete los siguientes pasos:
 - a. Introduzca un FQDN o una dirección IP y credenciales de administrador para la instancia de vCenter asociada con la instalación de NetApp HCI.
 - b. Haga clic en **continuar**.
 - c. Seleccione un centro de datos de vSphere en el que desea añadir los nodos de computación o haga clic en **Create New Datacenter** para añadir los nodos de computación a un centro de datos nuevo.



Si hace clic en Create New Datacenter, el campo Cluster se completa automáticamente.

- d. Si seleccionó un centro de datos existente, seleccione un clúster de vSphere con el que se deben asociar los nodos de computación nuevos.



Si NetApp HCI no reconoce la configuración de red del clúster seleccionado para la ampliación, asegúrese de que la asignación vmkernel y vmnic para las redes de gestión, almacenamiento y vMotion estén establecidas con los valores predeterminados de puesta en marcha. Consulte ["cambios de red admitidos"](#) si quiere más información.

e. Haga clic en **continuar**.

8. En la página **ESXi Credentials**, introduzca la contraseña raíz de ESXi para los nodos de computación que va a añadir.

Debe usar la misma contraseña que se creó durante la implementación inicial de NetApp HCI.

9. Haga clic en **continuar**.

10. Si creó un nuevo clúster de centro de datos de vSphere, en la página **Network Topology**, seleccione una topología de red para que coincida con los nodos de computación nuevos que va a añadir.



Solo debe seleccionar la opción de dos cables si los nodos de computación utilizan la topología de dos cables y la implementación de NetApp HCI existente se configura con identificadores de VLAN.

11. En la página **Inventario disponible**, seleccione los nodos de almacenamiento y computación que desea agregar y haga clic en **continuar**.



En algunos nodos de computación, es posible que deba habilitar EV en el nivel más alto compatible con la versión de vCenter antes de poder añadirlos a la instalación. Debe utilizar el cliente de vSphere a fin de habilitar EVC para estos nodos de computación. Después de habilitar dicha función, actualice la página Inventory e intente añadir nuevamente los nodos de computación.

12. Haga clic en **continuar**.

13. **Opcional:** Si creó un nuevo clúster de centro de datos de vSphere, en la página **Configuración de red**, importe la información de la red desde una implementación de NetApp HCI existente seleccionando la casilla de verificación **Copiar configuración desde un clúster existente**.

Esto rellena la información de la pasarela y de la subred predeterminadas para cada red.

14. En la página **Configuración de red**, se ha detectado parte de la información de red desde la implementación inicial. Cada nodo de almacenamiento nuevo se enumera por número de serie, y es necesario asignarle la información de red nueva. Complete los siguientes pasos para cada nodo de almacenamiento nuevo:

- a. **Nombre de host:** Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo prefijo de nomenclatura detectado e insértelo como prefijo para el nuevo nombre de host único que agregue en el campo Nombre de host.
- b. **Dirección de administración:** Introduzca una dirección IP de administración para el nuevo nodo de almacenamiento que se encuentra dentro de la subred de la red de administración.
- c. **Dirección IP de almacenamiento (iSCSI):** Introduzca una dirección IP iSCSI para el nuevo nodo de

almacenamiento que se encuentra en la subred de la red iSCSI.

d. Haga clic en **continuar**.



La NetApp HCI puede tardar algún tiempo en validar las direcciones IP especificadas. El botón continuar estará disponible cuando finalice la validación de la dirección IP.

15. En la página **Review** de la sección Network Settings (Configuración de red), los nodos nuevos se muestran en el texto en negrita. Para hacer cambios en cualquier sección, haga lo siguiente:
 - a. Haga clic en **Editar** para esa sección.
 - b. Después de terminar, haga clic en **continuar** en cualquier página posterior para volver a la página Revisión.
16. **Opcional:** Si no desea enviar estadísticas del clúster ni información de soporte a los servidores Active IQ alojados de NetApp, desactive la casilla de comprobación final.

Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.

17. Haga clic en **Agregar nodos**.

Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.

18. **Opcional:** Verifique que los nodos nuevos estén visibles en VMware vSphere Web Client (para nodos de computación) o en el plugin de Element para vCenter Server (para nodos de almacenamiento).



Si expandió un clúster de almacenamiento de dos nodos a cuatro nodos o más, la pareja de nodos testigo que anteriormente utilizaba el clúster de almacenamiento seguirá visible como máquinas virtuales en espera en vSphere. El clúster de almacenamiento recién ampliado no los utiliza; si desea recuperar recursos de equipos virtuales, puede hacerlo "[quitar manualmente](#)". Las máquinas virtuales del nodo de testigo.

Obtenga más información

- ["Página de recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Instrucciones de instalación y configuración para nodos de almacenamiento y de computación de NetApp HCI"](#)
- ["VMware Knowledge base: Soporte de procesador de Enhanced vMotion Compatibility \(EVC\)"](#)

Quite nodos de testigos después de expandir el clúster

Después de expandir un clúster de almacenamiento de dos nodos a cuatro o más nodos, puede eliminar el par de nodos de testigo para liberar recursos de computación en la instalación de NetApp HCI. Los nodos de testimonio utilizados anteriormente en el clúster de almacenamiento siguen visibles como máquinas virtuales en espera (VM) en vSphere Web Client.

Acerca de esta tarea

No se necesitan nodos de testigos en clústeres con más de cuatro nodos de almacenamiento. Este es un procedimiento opcional si desea liberar la CPU y la memoria después de expandir el clúster de dos nodos a cuatro o más nodos.



Compruebe que no se ha notificado ningún error o fallo del clúster. Para encontrar información sobre las alertas del sistema, haga clic en **informar > Alertas** en el punto de extensión NetApp Element Management de vSphere.

Pasos

1. Desde vSphere, acceda al punto de extensión NetApp Element Management desde la pestaña **Accesos directos** o el panel lateral.
2. Seleccione **Administración de NetApp Element > clúster > nodos**.

NetApp Element Management

Cluster: SFPS-... CLUSTER | MVIP: 10... 146 | SVIP: 10... B4 | vCenter: 10... 140

Getting Started | Reporting | Management | Protection | **Cluster** | VVoIs

<input type="checkbox"/>	Node ID	Node Name	Node State	Available 4k IOPS	Node Role	Node Type	Active Drives	Management IP	Storage IP	Management VLAN ID	Storage VLAN
<input type="checkbox"/>	1	sfps-...-stg-01	Active	50000	Ensemble Node	H410S-0	6	10...147	10...85	0	101
<input type="checkbox"/>	2	sfps-...-stg-02	Active	50000	Ensemble Node, Cluster Master	H410S-0	6	10...148	10...86	0	101
<input checked="" type="checkbox"/>	3	sfps-...-witness-01	Active	0		SFVIRT	0	10...42	10...90		
<input checked="" type="checkbox"/>	4	sfps-...-witness-02	Active	0		SFVIRT	0	10...43	10...91		
<input type="checkbox"/>	5	sfps-...-stg-03	Active	50000	Ensemble Node	H410S-0	6	10...149	10...87	0	101
<input type="checkbox"/>	6	sfps-...-stg-04	Active	50000		H410S-0	6	10...150	10...88	0	101

3. Seleccione la casilla de verificación para el nodo testigo que desea eliminar y haga clic en **acciones > Quitar**.
4. Confirme la acción en el símbolo del sistema.
5. Haga clic en **hosts y clústeres**.
6. Desplácese hasta la máquina virtual del nodo de testigo que haya quitado anteriormente.
7. Haga clic con el botón derecho en la máquina virtual y apáguela.
8. Haga clic con el botón derecho del ratón en la máquina virtual que ha apagado y haga clic en **Eliminar del disco**.
9. Confirme la acción en el símbolo del sistema.

Obtenga más información

- ["Clúster de almacenamiento de dos nodos NetApp HCI | TR-4823"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

- "Centro de documentación de SolidFire y el software Element"

Use Rancher en NetApp HCI

Descripción general de rancher on NetApp HCI

Rancher es una completa pila de software para equipos que adoptan contenedores. Rancher responde a los retos operativos y de seguridad que plantea la gestión de varios clústeres de Kubernetes en distintas infraestructuras, y proporciona a los equipos de DevOps herramientas integradas para ejecutar cargas de trabajo en contenedores.

Al implementar Rancher en NetApp HCI, se pone en marcha el plano de control Rancher, también conocido como *Rancher Server* y se pueden crear clústeres de Kubernetes en las instalaciones. Puede poner en marcha el plano de control Rancher mediante Cloud Control de NetApp híbrido.

Después de la puesta en marcha, con el plano de control de Rancher, puede aprovisionar, gestionar y supervisar clústeres de Kubernetes que utilizan los equipos de desarrollo y operaciones. Los equipos de desarrollo y operaciones pueden usar Rancher para realizar actividades en clústeres de usuarios que residen en la propia NetApp HCI, un proveedor de cloud público o cualquier otra infraestructura que permita Rancher.

Ventajas de Rancher en NetApp HCI

- **Facilidad de instalación:** No necesita aprender a instalar y configurar Rancher. Puede implementar una implementación basada en plantillas, desarrollada conjuntamente por NetApp HCI y Rancher.
- **Gestión del ciclo de vida:** En una implementación manual de Rancher, las actualizaciones para la aplicación del servidor Rancher o el clúster RKE (RKE) no están automatizadas. Rancher en NetApp HCI proporciona la capacidad de realizar actualizaciones en el clúster de administración, que incluye el servidor Rancher y el RKE.

Lo que puede hacer con Rancher en NetApp HCI

Con Rancher en NetApp HCI, podrá:

- Ponga en marcha servicios entre proveedores de cloud y su cloud privado.
- Puertos de las aplicaciones y los datos en una arquitectura de cloud híbrido independientemente de la ubicación del cloud sin comprometer los acuerdos de nivel de servicio.
- Aumente la velocidad de las aplicaciones nativas del cloud.
- Centralice la gestión de varios clústeres (nuevos y existentes).
- Realice la orquestación de las aplicaciones basadas en Kubernetes del cloud híbrido.

Opción de soporte técnico

El uso de Rancher en NetApp HCI y el software de código abierto Kubernetes incluye la puesta en marcha y el uso gratuitos. Las claves de licencia no son necesarias.

Puede elegir una opción de soporte para Rancher de NetApp para obtener soporte empresarial basado en los núcleos.

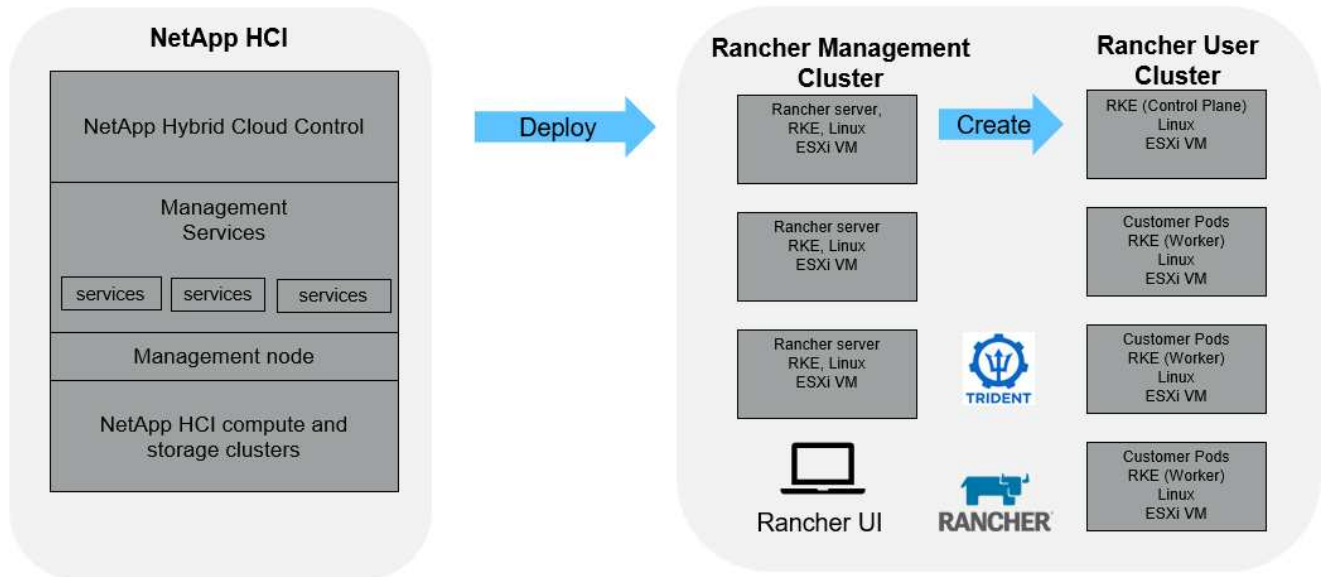


No se incluye el soporte de rancher en su acuerdo Support Edge de NetApp. Póngase en contacto con el departamento de ventas de NetApp o con su distribuidor para obtener más información sobre Si adquiere Rancher Support de NetApp, recibirá un correo electrónico con las instrucciones.

Ranchero sobre la arquitectura y los componentes de NetApp HCI

A continuación se ofrece una descripción general de los distintos componentes de Rancher en NetApp HCI:

Rancher on NetApp HCI



- **Control de cloud híbrido de NetApp:** Esta interfaz le permite implementar Rancher en el software NetApp HCI y NetApp Element, necesario para Rancher en NetApp HCI.



Puede usar el control de cloud híbrido de NetApp también para actualizar los servicios de gestión, ampliar el sistema, recopilar registros y supervisar la instalación.

- **Servicios de gestión:** Los servicios de gestión se ejecutan en el nodo de gestión y le permiten implementar Rancher en NetApp HCI mediante el control de cloud híbrido de NetApp.
- **Clúster de gestión:** Rancher en NetApp HCI implementa tres máquinas virtuales en el clúster de gestión de Rancher, que puede ver mediante el control de cloud híbrido de NetApp, vCenter Server o la interfaz de usuario de Rancher. Las máquinas virtuales del clúster de gestión alojan el servidor Rancher, el motor Rancher Kubernetes Engine (RKE) y el sistema operativo Linux.



Para obtener el mejor rendimiento y una mayor seguridad, considere la posibilidad de usar un clúster de Kubernetes dedicado para el servidor de gestión Rancher. No debe ejecutar las cargas de trabajo de usuario en el clúster de gestión.

- **Clústeres de usuario:** Los clústeres de usuarios de Kubernetes que están en proceso de flujo descendente ejecutan sus aplicaciones y servicios. Cualquier clúster que implemente desde Rancher o importe en Rancher es un clúster de usuarios.

- **Trident:** Hay un catálogo de Trident disponible para Rancher en NetApp HCI y se ejecuta en los clústeres de usuarios. La inclusión de este catálogo simplifica la puesta en marcha de Trident en los clústeres de usuarios.

Obtenga más información

- ["Documentación de rancher sobre arquitectura"](#)
- ["Recursos de NetApp HCI"](#)

Francher en conceptos de NetApp HCI

Conozca los conceptos básicos relacionados con Rancher en NetApp HCI.

- **Rancher Server** o **plano de control:** El plano de control Rancher, a veces llamado el *Rancher Server*, aprovisiona, administra y supervisa clústeres Kubernetes utilizados por los equipos de Desarrollo y Operaciones.
- **Catálogos:** Los catálogos son repositorios de GitHub o repositorios de Helm Chart llenos de aplicaciones listas para su implementación. Rancher proporciona la capacidad de utilizar un catálogo de gráficos Helm que facilitan la implementación de aplicaciones repetidas veces. Rancher incluye dos tipos de catálogos: Catálogos globales incorporados y catálogos personalizados. Trident se pone en marcha como catálogo. Consulte ["Documentación de rancher sobre catálogos"](#).
- **Clúster de gestión:** Rancher en NetApp HCI implementa tres máquinas virtuales en el clúster de gestión de Rancher, que puede ver mediante Rancher, Control de cloud híbrido y el complemento vCenter. Las máquinas virtuales del clúster de gestión alojan el servidor Rancher, el motor Rancher Kubernetes Engine (RKE) y el sistema operativo Linux.
- **Clústeres de usuario:** Estos clústeres de Kubernetes de flujo descendente ejecutan sus aplicaciones y servicios. En las instalaciones de Kubernetes de Rancher, el clúster de gestión debe estar separado de los clústeres de usuarios. Cualquier clúster que un usuario de Rancher implemente desde Rancher, o que importe a Rancher, se considera un clúster de usuarios.
- **Plantilla de nodo de Rancher:** Hybrid Cloud Control utiliza una plantilla de nodo de Rancher para simplificar la implementación.

Consulte ["Documentación de rancher sobre las plantillas de nodos"](#).

El software Trident y los conceptos de almacenamiento persistente

Trident, en sí misma una aplicación nativa de Kubernetes, se ejecuta directamente en un clúster de Kubernetes. Con Trident, los usuarios de Kubernetes (como desarrolladores, científicos de datos y administradores de Kubernetes) pueden crear, gestionar e interactuar con volúmenes de almacenamiento persistentes en el formato Kubernetes estándar, con el que ya están familiarizados. Con Trident, las soluciones de NetApp pueden satisfacer las demandas de volumen persistente que realizan los clústeres de Kubernetes.

Con Rancher, puede usar un volumen persistente, un volumen que existe independientemente de un pod específico y, por tanto, durante su propia vida útil. El uso de Trident para gestionar reclamaciones de volúmenes persistentes (RVP) aísla a los desarrolladores con pods a partir de los detalles de implementación de nivel inferior del almacenamiento al que acceden.

Cuando una aplicación en contenedor emite una solicitud de reclamación de volumen persistente (RVP), Trident aprovisiona de forma dinámica el almacenamiento según los parámetros solicitados desde la capa de almacenamiento del software NetApp Element en NetApp HCI.

Hay un catálogo de Trident disponible para Rancher en NetApp HCI y se ejecuta en los clústeres de usuarios. Como parte de la implementación de Rancher en NetApp HCI, hay un instalador de Trident disponible en el catálogo Rancher de forma predeterminada. La inclusión de este catálogo simplifica la puesta en marcha de Trident en los clústeres de usuarios.

Consulte ["Instale Trident con Rancher en NetApp HCI"](#).

Si desea obtener más información, visite la ["Documentación de Trident"](#).

Obtenga más información

- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Recursos de NetApp HCI"](#)

Requisitos para Rancher en NetApp HCI

Antes de instalar Rancher en NetApp HCI, asegúrese de que su entorno y su sistema NetApp HCI cumplan estos requisitos.



Si se implementa accidentalmente Rancher en NetApp HCI con información incorrecta (como un FQDN de servidor Rancher incorrecto), no hay forma de corregir la implementación sin eliminarla ni volver a implementarla. Deberá quitar el Rancher en la instancia de NetApp HCI y, a continuación, volver a poner en marcha Rancher en NetApp HCI desde la IU de control de cloud híbrido de NetApp. Consulte ["Retire una instalación de Rancher en NetApp HCI"](#) si quiere más información.

Requisitos de nodo

- Compruebe que su sistema NetApp HCI tenga al menos tres nodos de computación; esto es necesario para obtener una resiliencia completa. Rancher en NetApp HCI no es compatible con configuraciones de solo almacenamiento.
- Compruebe que el almacén de datos que pretende utilizar para la implementación de Rancher en NetApp HCI tenga al menos 60 GB de espacio libre.
- Asegúrese de que el clúster de NetApp HCI ejecute servicios de gestión versión 2.17 o posterior.

Detalles del nodo

Rancher en NetApp HCI pone en marcha un clúster de gestión de tres nodos.

Todos los nodos tienen las siguientes características:

VCPU	RAM (GB)	Disco (GB)
2	8	20

Requisitos de red

- Compruebe que la red que pretende implementar el Rancher en el clúster de gestión de NetApp HCI tiene una ruta hacia la red de gestión de nodos de gestión.

- Rancher en NetApp HCI admite direcciones DHCP para el plano de control (servidor Rancher) y los clústeres de usuarios, pero recomendamos direcciones IP estáticas para entornos de producción. Asegúrese de haber asignado las direcciones IP estáticas necesarias si se va a implementar en un entorno de producción.
 - El servidor de rancher requiere tres direcciones IP estáticas.
 - Cada clúster de usuarios requiere tantas direcciones IP estáticas como nodos en el clúster. Por ejemplo, un clúster de usuarios con cuatro nodos requiere cuatro direcciones IP estáticas.
 - Si piensa utilizar direcciones DHCP para el plano de control Rancher o los clústeres de usuarios, asegúrese de que la duración de la concesión DHCP sea de al menos 24 horas.
- Si necesita utilizar un proxy HTTP para habilitar el acceso a Internet para Rancher en NetApp HCI, debe realizar un cambio previo a la implementación del nodo de gestión. Inicie sesión en su nodo de gestión mediante SSH y siga el ["instrucciones"](#) En la documentación de Docker para actualizar manualmente la configuración de proxy para Docker.
- Si activa y configura un servidor proxy durante la implementación, los siguientes rangos de direcciones IP y dominios se agregan automáticamente a la configuración de noProxy del servidor Rancher:

```
127.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, .svc,
.cluster.local
```

- Asegúrese de que el nodo de gestión pueda usar DNS para resolver el nombre de host `<any IP address>.nip.io` a una dirección IP. Este es el proveedor DNS que se utiliza durante la implementación; si el nodo de gestión no puede resolver esta URL, se producirá un error en la implementación.
- Asegúrese de que ha configurado registros DNS para cada dirección IP estática que necesite.

Requisitos de vSphere de VMware

- Compruebe que la instancia de VMware vSphere que utiliza sea la versión 6.5, 6.7 o 7.0.
- Puede usar una configuración de red de vSphere Standard Switch (VSS), pero si lo hace, asegúrese de que los switches virtuales y los hosts físicos utilizados para los equipos virtuales Rancher puedan acceder a todos los mismos grupos de puertos, del mismo modo que se asegurará de que lo hagan con las máquinas virtuales normales.

Consideraciones sobre la implementación

Quizás desee revisar las siguientes consideraciones:

- Tipos de implementaciones
 - Puestas en marcha de demostraciones
 - Instalaciones de producción
- Rancher FQDN



Rancher en NetApp HCI no es resiliente a los fallos de nodo a menos que configure algún tipo de balanceo de carga de red. Como solución sencilla, cree una entrada DNS por turnos para las tres direcciones IP estáticas reservadas para el servidor Rancher. Estas entradas DNS deben resolverse en el FQDN del servidor Rancher que utilizará para acceder al host del servidor Rancher, que sirve a la interfaz de usuario web de Rancher una vez completada la implementación.

Tipos de implementaciones

Puede implementar Rancher en NetApp HCI de las siguientes formas:

- **Implementaciones de demostración:** Si DHCP está disponible en el entorno de implementación dirigido y desea realizar una demostración de la capacidad de Rancher en NetApp HCI, entonces la implementación de DHCP es la más conveniente.

En este modelo de implementación, se puede acceder a la interfaz de usuario de Rancher desde cada uno de los tres nodos del clúster de gestión.

Si su organización no utiliza DHCP, también puede probarlo utilizando cuatro direcciones IP estáticas asignadas antes de la implementación, de modo similar a lo que se haría para una implementación de producción.

- **Implementaciones de producción:** Para implementaciones de producción o cuando DHCP no está disponible en el entorno de implementación dirigido, se requiere un poco más de trabajo previo a la implementación. El primer paso es obtener tres direcciones IP consecutivas. Introduzca el primero durante la implementación.

Se recomienda utilizar el equilibrio de carga L4 o la configuración DNS round-robin para entornos de producción. Esto requiere una cuarta dirección IP y una entrada independiente en la configuración de DNS.

- *** Equilibrio de carga L4*:** Esta es una técnica donde una máquina virtual o contenedor que aloja una aplicación como nginx está configurado para distribuir solicitudes entre los tres nodos del cluster de administración.
- **Round-robin DNS:** Es una técnica en la que se configura un único nombre de host en el sistema DNS que rota las solicitudes entre los tres hosts que forman el clúster de administración.

Rancher FQDN

La instalación requiere la asignación de una dirección URL de Rancher, que incluye el nombre de dominio completo (FQDN) del host donde se servirá la interfaz de usuario de Rancher una vez finalizada la instalación.

En todos los casos, se puede acceder a la interfaz de usuario de Rancher en el navegador mediante el protocolo https (puerto 443).

Las puestas en marcha de producción requieren un FQDN configurado que equilibra la carga entre los nodos del clúster de gestión. Sin usar un FQDN y el equilibrio de carga, el entorno no es flexible y solo es adecuado para entornos de demostración.

Puertos necesarios

Asegúrese de que la lista de puertos de la sección "puertos para nodos de servidor de RKE" de la sección **nodos de Rancher** del funcionario "[Documentación del rancher](#)" Están abiertos en la configuración del firewall hacia y desde los nodos que ejecutan el servidor Rancher.

URL requeridas

Debe accederse a las siguientes direcciones URL desde los hosts en los que reside el plano de control Rancher:

URL	Descripción
https://charts.jetstack.io/	Integración con Kubernetes
https://releases.rancher.com/server-charts/stable	Descargas de software de rancher
https://entropy.ubuntu.com/	Servicio de entropía de Ubuntu para la generación aleatoria de números
https://raw.githubusercontent.com/vmware/cloud-init-vmware-guestinfo/v1.3.1/install.sh	Adiciones de VMware
https://download.docker.com/linux/ubuntu/gpg	Clave pública de Docker Ubuntu GPG
https://download.docker.com/linux/ubuntu	Enlace de descarga de Docker
https://hub.docker.com/	Docker Hub para NetApp Hybrid Cloud Control

Ponga en marcha Rancher en NetApp HCI

Para utilizar Rancher en su entorno de NetApp HCI, primero debe implementar Rancher en NetApp HCI.



Antes de iniciar la implementación, asegúrese de comprobar el espacio libre y el otro del almacén de datos "[Requisitos para Rancher en NetApp HCI](#)".



No se incluye el soporte de rancher en su acuerdo Support Edge de NetApp. Póngase en contacto con el departamento de ventas de NetApp o con su distribuidor para obtener más información sobre Si adquiere Rancher Support de NetApp, recibirá un correo electrónico con las instrucciones.

¿Qué ocurre cuando implementan Rancher en NetApp HCI?

La implementación implica los siguientes pasos, cada uno descrito con más detalle:

- Utilice el control de cloud híbrido de NetApp para iniciar la puesta en marcha.
- La implementación de Rancher crea un clúster de gestión, que incluye tres máquinas virtuales.

A cada máquina virtual se le asignan todos los roles de Kubernetes tanto para el plano de control como para el trabajador. Esto significa que la IU de Rancher está disponible en cada nodo.

- También se instala el plano de control de Rancher (o *Rancher Server*), utilizando la plantilla de nodos NetApp HCI en Rancher para una implementación más sencilla. El plano de control de Rancher funciona automáticamente con la configuración utilizada en el motor de puesta en marcha de NetApp, que se utilizó para crear la infraestructura de NetApp HCI.
- Después de la implementación, recibirá un correo electrónico de NetApp donde le ofrecerá la opción de registrarse en las implementaciones de soporte de NetApp en Rancher en NetApp HCI.
- Después de la implementación, los equipos de Dev y OPS pueden poner en marcha sus clústeres de

usuarios, de forma similar a cualquier implementación de Rancher.

Pasos para implementar Rancher en NetApp HCI

- [Acceda al control del cloud híbrido de NetApp](#)
- [Ponga en marcha Rancher en NetApp HCI](#)
- [Compruebe la puesta en marcha mediante vCenter Server](#)

Acceda al control del cloud híbrido de NetApp

Para comenzar la puesta en marcha, acceda a Hybrid Cloud Control de NetApp.

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

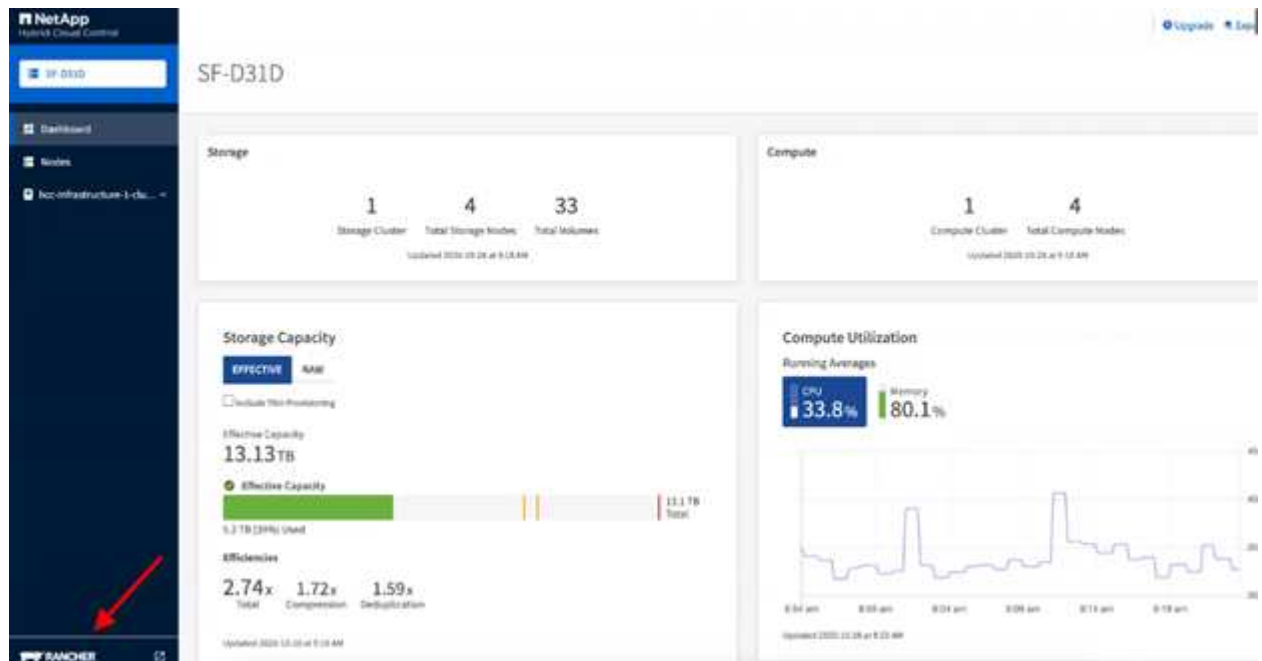
```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.

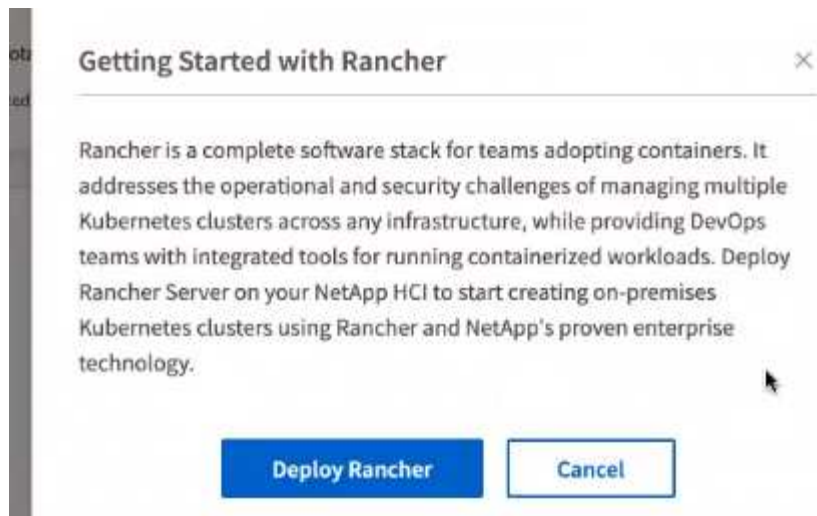
Aparece la interfaz de control del cloud híbrido de NetApp.

Ponga en marcha Rancher en NetApp HCI

1. En Hybrid Cloud Control, haga clic en el icono **Rancher** en la parte inferior izquierda de la barra de navegación.

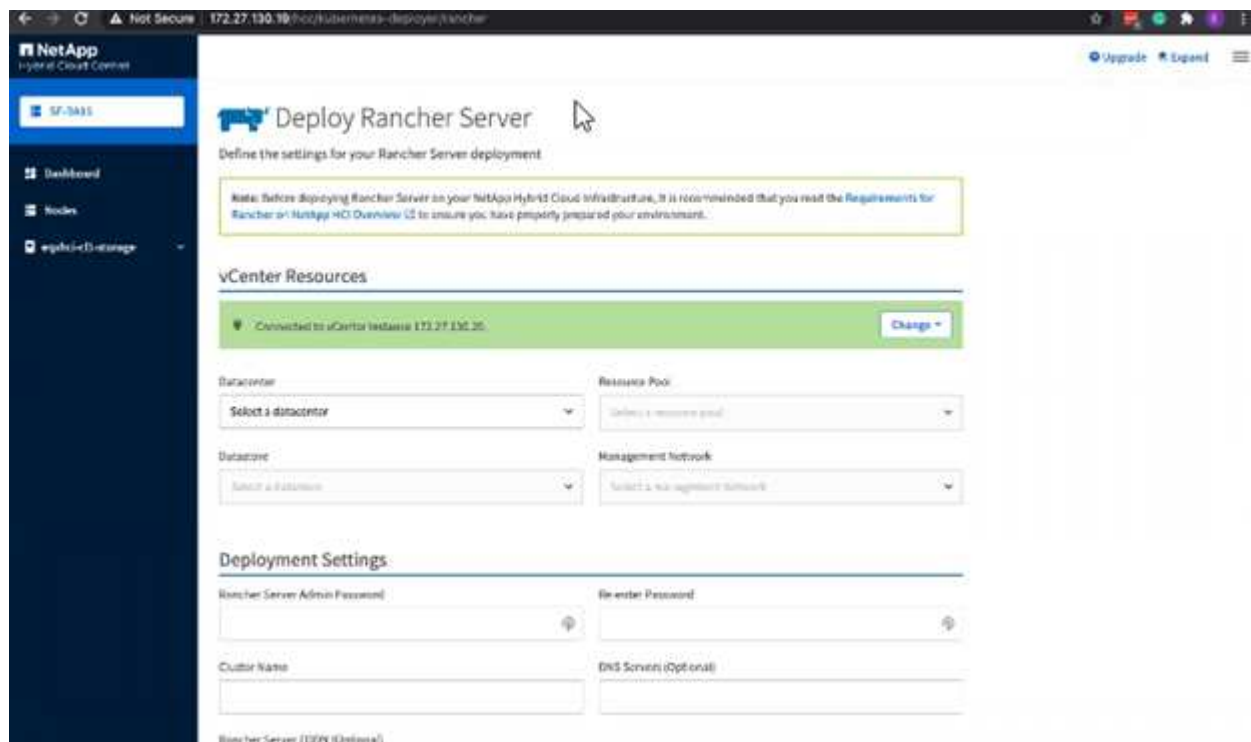


Una ventana emergente muestra un mensaje sobre cómo empezar a usar Rancher.



2. Haga clic en **desplegar Rancher**.

Aparece la IU de Rancher.



Sus credenciales de vCenter se recogen en la instalación del motor de puesta en marcha de NetApp.

3. Introduzca la información * vCenter Resources*. A continuación se describen algunos campos.

- **Datacenter:** Seleccione un centro de datos. Después de seleccionar el centro de datos, todos los demás campos se rellenan automáticamente, aunque pueda cambiarlos.
- **Datastore:** Seleccione un almacén de datos en los nodos de almacenamiento de NetApp HCI. Este almacén de datos debe ser flexible y estar accesible para todos los hosts de VMware. No seleccione un almacén de datos local al que solo pueda acceder uno de los hosts.
- **Red de administración:** Debería ser accesible desde las estaciones de administración y desde la red de máquinas virtuales donde se alojarán los clusters de usuarios.

4. Introduzca **Información sobre los ajustes de implementación:**

- **Servidores DNS:** Opcional. Si utiliza el equilibrio de carga, introduzca la información del servidor DNS interno.
- **Rancher Server FQDN:** Para asegurarse de que el servidor Rancher permanece disponible durante los errores de nodo, proporcione un nombre de dominio (FQDN) completamente cualificado que el servidor DNS puede resolver en cualquiera de las direcciones IP asignadas a los nodos del clúster Rancher Server. Este FQDN con el prefijo "https" se convierte en la URL de Rancher que utilizará para acceder a la implementación de Rancher.

Si no se proporciona ningún nombre de dominio, se utilizará DNS comodín y podrá acceder al servidor de Rancher utilizando una de las direcciones URL presentadas una vez completada la implementación.

5. Introduzca la información de **Configuración avanzada:**

- **Asignar direcciones IP estáticas:** Si activa direcciones IP estáticas, proporcione direcciones IP de inicio para tres direcciones IPv4 en secuencia, una para cada máquina virtual del clúster de administración. Rancher en NetApp HCI pone en marcha tres máquinas virtuales de clústeres de gestión.
- **Configurar servidor proxy:**

6. Revise y seleccione la casilla del Contrato de licencia para el usuario final de Rancher.

7. Revise y seleccione la casilla de verificación para confirmar la información sobre el software Rancher.

8. Haga clic en **desplegar**.

Una barra indica el progreso de la implementación.



La puesta en marcha de Rancher podría llevar unos 15 minutos.

Una vez finalizada la implementación, Rancher muestra un mensaje acerca de la finalización y proporciona una URL de Rancher.



9. Registre que Rancher URL que muestra al final de la implementación. Utilizará esta URL para acceder a la interfaz de usuario de Rancher.

Compruebe la puesta en marcha mediante vCenter Server

En su cliente vSphere, puede ver el clúster de gestión de Rancher, que incluye las tres máquinas virtuales.



Una vez finalizada la implementación, no modifique la configuración del clúster de máquinas virtuales del servidor Rancher ni quite las máquinas virtuales. Rancher en NetApp HCI se basa en la configuración de clúster de gestión de RKE implementada para funcionar normalmente.

El futuro

Después de la implementación, puede realizar lo siguiente:

- ["Complete las tareas posteriores a la implementación"](#)
- ["Instale Trident con Rancher en NetApp HCI"](#)
- ["Poner en marcha aplicaciones y clústeres de usuarios"](#)
- ["Administrar Rancher en NetApp HCI"](#)
- ["Monitor Rancher en NetApp HCI"](#)

Obtenga más información

- ["Solución de problemas de implementación de rancher"](#)
- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Recursos de NetApp HCI"](#)

Tareas posteriores a la implementación

Información general de las tareas posteriores a la implementación

Después de implementar Rancher en NetApp HCI, debe continuar con las actividades posteriores a la implementación.

- ["Asegúrese de que la paridad sea compatible con Rancher"](#)
- ["Mejore la resiliencia de los equipos virtuales Rancher"](#)
- ["Configurar la supervisión"](#)
- ["Instale Trident"](#)
- ["Habilite la compatibilidad de Trident para clústeres de usuarios"](#)

Obtenga más información

- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Asegúrese de que la paridad sea compatible con Rancher

Después de implementar Rancher en NetApp HCI, debe asegurarse de que el número de núcleos de Rancher Support que ha adquirido coincida con el número de núcleos de CPU que está utilizando para las máquinas virtuales de gestión de Rancher y los clústeres de usuarios.

Si ha comprado Rancher Support para solo parte de los recursos informáticos de NetApp HCI, debe tomar

medidas en VMware vSphere para garantizar que Rancher en NetApp HCI y sus clústeres de usuarios gestionados solo se ejecuten en hosts para los que ha adquirido Rancher Support. Consulte la documentación de VMware vSphere para obtener información sobre cómo ayudar a garantizar esto mediante el confinamiento de cargas de trabajo de computación en hosts específicos.

Obtenga más información

- ["Reglas de afinidad de vSphere ha y DRS"](#)
- ["Crear reglas de antiafinidad de VM"](#)
- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Mejore la resiliencia de los equipos virtuales Rancher

Después de implementar Rancher en NetApp HCI, su entorno vSphere contendrá tres nodos nuevos como máquinas virtuales para alojar el entorno Rancher. La interfaz de usuario web de Rancher está disponible en cada uno de estos nodos. Para lograr una resiliencia completa, cada una de las tres máquinas virtuales junto con los discos virtuales correspondientes debería residir en un host físico diferente, después de eventos como ciclos de alimentación y recuperación tras fallos.

Para garantizar que cada equipo virtual y sus recursos permanezcan en un host físico diferente, puede crear reglas de afinidad para el programador de recursos distribuidos (DRS) de VMware vSphere. Esto no está automatizado como parte de Rancher en la implementación de NetApp HCI.

Para obtener instrucciones sobre cómo configurar las reglas de anti-afinidad de DRS, consulte los siguientes recursos de documentación de VMware:

["Crear reglas de antiafinidad de VM"](#)

["Reglas de afinidad de vSphere ha y DRS"](#)

Obtenga más información

- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Habilite la supervisión

Después de implementar Rancher en NetApp HCI, puede habilitar la supervisión del almacenamiento de Active IQ (para almacenamiento all-flash de SolidFire y NetApp HCI) y la supervisión de computación de NetApp HCI (solo para NetApp HCI) si no lo hizo todavía durante la instalación o la actualización.

Para obtener instrucciones sobre cómo activar la supervisión, consulte ["Habilite la supervisión de Active IQ y NetApp HCI"](#).

Obtenga más información

- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Instale Trident

Obtenga más información sobre cómo instalar Trident después de instalar Rancher en NetApp HCI. Trident es un orquestador de almacenamiento, que se integra con Docker y Kubernetes, así como plataformas basadas en estas tecnologías, como Red Hat OpenShift, Rancher e IBM Cloud Private. El objetivo de Trident es hacer que el aprovisionamiento, la conexión y el consumo del almacenamiento sea transparente y sin fricciones para las aplicaciones. Trident es un proyecto de código abierto totalmente compatible y mantenido por NetApp. Trident le permite crear, gestionar e interactuar con volúmenes de almacenamiento persistentes en el formato Kubernetes estándar que esté familiarizado.



Si desea obtener más información sobre Trident, consulte ["Documentación de Trident"](#).

Lo que necesitará

- Ha instalado Rancher en NetApp HCI.
- Implementó los clústeres de usuarios.
- Configuró las redes de clúster de usuarios para Trident. Consulte ["Habilite la compatibilidad de Trident para clústeres de usuarios"](#) si desea obtener instrucciones.
- Ha completado los pasos de requisitos previos necesarios para la preparación del nodo de trabajo para Trident. Consulte ["Documentación de Trident"](#).

Acerca de esta tarea

El catálogo de instalación de Trident se instala como parte de la instalación de Rancher mediante NetApp Hybrid Cloud Control. En esta tarea, se debe usar el catálogo de instalación para instalar y configurar Trident. Como parte de la instalación de Rancher, NetApp proporciona una plantilla de nodo. Si no tiene pensado utilizar la plantilla de nodo que proporciona NetApp y desea aprovisionar en RHEL o CentOS, puede haber requisitos adicionales. Si cambia el nodo de trabajo a RHEL o CentOS, se deberán cumplir varios requisitos previos. Consulte ["Documentación de Trident"](#).

Pasos

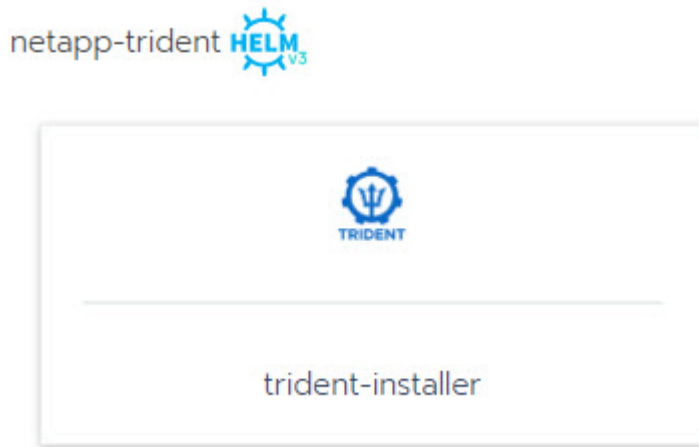
1. En la IU de Rancher, seleccione un proyecto para el clúster de usuarios.



Para obtener información sobre proyectos y espacios de nombres, consulte ["Documentación del rancher"](#).

2. Seleccione **aplicaciones** y seleccione **Iniciar**.

3. En la página **Catálogo**, seleccione el instalador de Trident.



En la página que se abre, puede seleccionar la flecha **descripciones detalladas** para obtener más información sobre la aplicación Trident y también encontrar el enlace a la "[Documentación de Trident](#)".

4. Seleccione la flecha **Opciones de configuraciones** e introduzca las credenciales y la información de configuración de almacenamiento.

STORAGECONFIGURATION

<p>Storage Tenant *</p> <input type="text" value="NetApp-HCI"/> <p><small>The name of the tenant that is already present on the SolidFire AFA.</small></p>	<p>SVIP *</p> <input type="text" value=""/> <p><small>The virtual/cluster IP address for data (I/O).</small></p>
<p>MVIP *</p> <input type="text" value=""/> <p><small>The virtual/cluster IP address for management.</small></p>	<p>Trident Backend Name *</p> <input type="text" value="solidfire"/> <p><small>The name of this Trident backend configuration.</small></p>
<p>Trident Storage Driver *</p> <input type="text" value="solidfire-san"/> <p><small>The name of the Trident storage driver.</small></p>	







El inquilino de almacenamiento predeterminado es NetApp HCI. Puede cambiar este valor. También puede cambiar el nombre del backend. Sin embargo, no cambie el valor predeterminado del controlador de almacenamiento, que es **solidfire-san**.

5. Seleccione **Iniciar**.

De este modo se instala la carga de trabajo de Trident en el espacio de nombres **trident**.

6. Seleccione **Recursos > cargas de trabajo** y compruebe que el espacio de nombres **trident** incluye los siguientes componentes:

Namespace: trident		
<input type="checkbox"/>	▶ Active	trident-csi 
<input type="checkbox"/>	▶ Active	trident-csi 
<input type="checkbox"/>	▶ Active	trident-installer 
<input type="checkbox"/>	▶ Active	trident-operator 

7. (Opcional) Seleccione **almacenamiento** para el clúster de usuarios a fin de ver las clases de almacenamiento que puede utilizar para los volúmenes persistentes.



Las tres clases de almacenamiento son: Solidfire-gold*, solidfire-silver* y solidfire-bronze*. Puede hacer que una de estas clases de almacenamiento sea la predeterminada seleccionando el icono en la columna **predeterminado**.

Obtenga más información

- ["Habilite la compatibilidad de Trident para clústeres de usuarios"](#)
- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Habilite la compatibilidad de Trident para clústeres de usuarios

Si el entorno de NetApp HCI no tiene una ruta entre las redes de gestión y almacenamiento, y se implementan los clústeres de usuario que necesitan compatibilidad con Trident, se debe seguir configurando las redes de clúster de usuarios después de instalar Trident. Para cada clúster de usuario, debe habilitar la comunicación entre las redes de gestión y almacenamiento. Para ello, puede modificar la configuración de red de cada nodo del clúster de usuarios.

Acerca de esta tarea

Siga estos pasos generales para modificar la configuración de red de cada nodo del clúster de usuarios. En estos pasos se asume que ha creado el clúster de usuario con la plantilla de nodo predeterminada que se instala con Rancher en NetApp HCI.



Puede realizar estos cambios como parte de una plantilla de nodo personalizada para usarlos en futuros clústeres de usuarios.

Pasos

1. Implemente un clúster de usuarios con una plantilla predeterminada existente.
2. Conecte la red de almacenamiento al clúster de usuarios.
 - a. Abra VMware vSphere Web Client para la instancia de vCenter conectada.
 - b. En el árbol de inventario hosts and Clusters, seleccione un nodo en el clúster de usuario recién implementado.
 - c. Edite la configuración del nodo.
 - d. En el cuadro de diálogo de configuración, agregue un nuevo adaptador de red.
 - e. En la lista desplegable **Nueva red**, busque una red y seleccione **HCI_Internal_Storage_Data_Network**.
 - f. Expanda la sección del adaptador de red y registre la dirección MAC del nuevo adaptador de red.
 - g. Haga clic en **Aceptar**.
3. En Rancher, descargue el archivo de claves privadas SSH para cada nodo del clúster de usuarios.
4. Conéctese mediante SSH a un nodo del clúster de usuarios, mediante el archivo de claves privadas que descargó para ese nodo:

```
ssh -i <private key filename> <ip address>
```

5. Como superusuario, edite y guarde el `/etc/netplan/50-cloud-init.yaml` de modo que incluya la `ens224` de forma similar al ejemplo siguiente. Sustituya `<MAC address>` Con la dirección MAC registrada anteriormente:

```
network:
  ethernets:
    ens192:
      dhcp4: true
      match:
        macaddress: 00:50:56:91:1d:41
      set-name: ens192
    ens224:
      dhcp4: true
      match:
        macaddress: <MAC address>
      set-name: ens224
  version: 2
```

6. Utilice el siguiente comando para reconfigurar la red:

```
`netplan try`
```

7. Repita los pasos 4 a 6 para cada nodo restante del clúster de usuarios.
8. Cuando haya reconfigurado la red para cada nodo del clúster de usuarios, puede implementar aplicaciones en el clúster de usuarios que utilicen Trident.

Poner en marcha aplicaciones y clústeres de usuarios

Después de implementar Rancher en NetApp HCI, puede configurar clústeres de usuarios y agregar aplicaciones a dichos clústeres.

Ponga en marcha clústeres de usuario

Después de la implementación, los equipos de Dev y OPS pueden poner en marcha sus clústeres de usuarios de Kubernetes, de forma similar a cualquier puesta en marcha de Rancher en la que puedan poner en marcha aplicaciones.

1. Acceda a la interfaz de usuario de Rancher utilizando la dirección URL que se le proporcionó al final de la implementación de Rancher.
2. Cree clústeres de usuarios. Consulte la documentación de Rancher acerca de "[poner en marcha cargas de trabajo](#)".
3. Aprovisionar los clústeres de usuarios en Rancher en NetApp HCI. Consulte la documentación de Rancher acerca de "[Configuración de clústeres de Kubernetes en Rancher](#)".

Poner en marcha aplicaciones en clústeres de usuarios

Al igual que cualquier puesta en marcha de Rancher, se añaden aplicaciones en los clústeres de Kubernetes.

Consulte la documentación de Rancher acerca de "[implementar aplicaciones en los clústeres](#)".

Obtenga más información

- "[Documentación de rancher sobre arquitectura](#)"
- "[Terminología de Kubernetes para Rancher](#)"
- "[Recursos de NetApp HCI](#)"

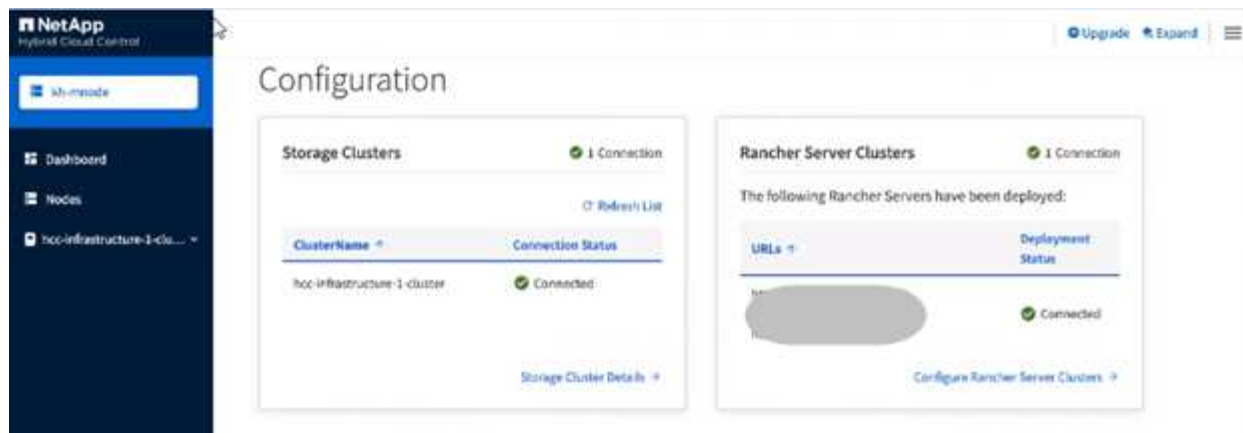
Administrar Rancher en NetApp HCI

Después de implementar Rancher en NetApp HCI, puede ver las direcciones URL y el estado del clúster del servidor Rancher. También puede eliminar el servidor Rancher.

Identificar las direcciones URL y el estado del clúster del servidor Rancher

Puede identificar las direcciones URL del clúster del servidor de Rancher y determinar el estado del servidor.

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI o Element.
2. En el panel de control, seleccione el icono de opciones de la parte superior derecha y seleccione **Configurar**.



La página Rancher Server Clusters muestra una lista de clústeres de servidores Rancher que se han implementado, la dirección URL asociada y el estado.

Obtenga más información

- ["Retire el Ranchor"](#)
- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Recursos de NetApp HCI"](#)

Supervisar un Ranchor en la implementación de NetApp HCI

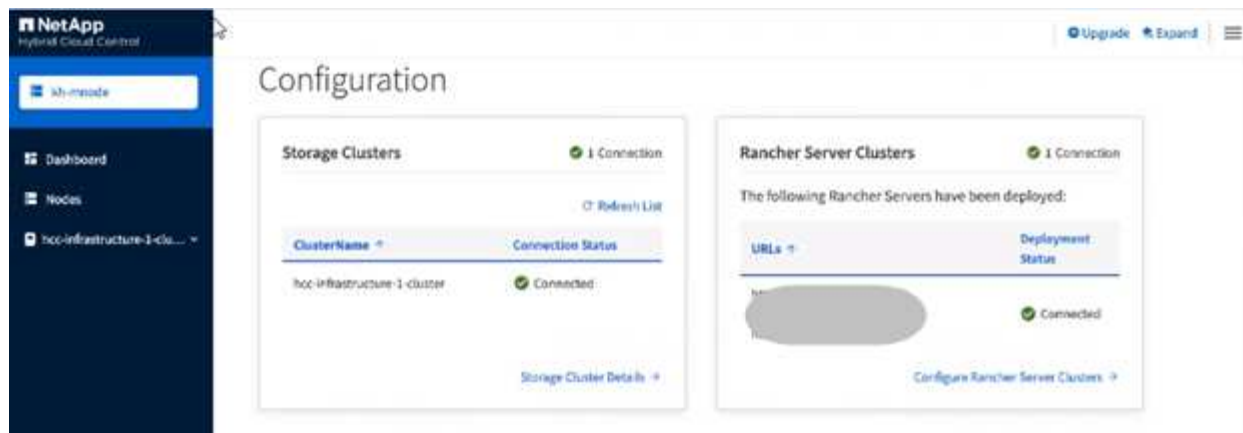
Existen varias formas de supervisar el servidor Rancher, los clústeres de administración y otros detalles.

- Control del cloud híbrido de NetApp
- IU del rancher
- Active IQ de NetApp
- VCenter Server

Supervise el rancher mediante el Control para el cloud híbrido de NetApp

Con el control de cloud híbrido de NetApp, puede ver la URL del Rancher y el estado de los clústeres del servidor Rancher. También puede supervisar los nodos en los que se está ejecutando Rancher.

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. En el Panel de control, haga clic en el icono de opciones superior derecho y seleccione **Configurar**.



3. Para ver la información de los nodos, en Hybrid Cloud Control Dashboard, expanda el nombre de su clúster de almacenamiento y haga clic en **Nodes**.

Supervise Rancher mediante la IU de Rancher

Con la interfaz de usuario de Rancher, puede ver información sobre Rancher en los clústeres de gestión y usuarios de NetApp HCI.



En la IU de Rancher, los clústeres de gestión se denominan "clústeres locales".

1. Acceda a la interfaz de usuario de Rancher utilizando la dirección URL que se le proporcionó al final de la implementación de Rancher.
2. Consulte ["Supervisión en Rancher v2.5"](#).

Supervisión de Rancher mediante Active IQ de NetApp

Mediante Active IQ de NetApp, puede ver la telemetría de Rancher, como información de instalación, nodos, clústeres, estado, información de espacio de nombres, y sigue.

1. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento Element.
2. En el menú superior derecho, seleccione **Active IQ** de NetApp.

Supervise Rancher mediante vCenter Server

Con vCenter Server, puede supervisar las máquinas virtuales Rancher.

Obtenga más información

- ["Documentación de rancher sobre arquitectura"](#)
- ["Terminología de Kubernetes para Rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Recursos de NetApp HCI"](#)

Actualice Rancher en NetApp HCI

Para actualizar el software Rancher, puede usar la interfaz de usuario de Cloud Control (HCC) híbrido de NetApp o la API DE REST. HCC proporciona un proceso sencillo con solo pulsar un botón para actualizar los componentes de la implementación de Rancher, incluidos el servidor Rancher, Rancher Kubernetes Engine (RKE) y el sistema operativo del nodo del clúster de gestión (para actualizaciones de seguridad). También puede usar la API para ayudar a automatizar las actualizaciones.

Las actualizaciones están disponibles por componentes en lugar de un paquete acumulativo. De este modo, algunas actualizaciones de componentes, como el sistema operativo Ubuntu, están disponibles con una cadencia más rápida. Las actualizaciones sólo afectan a la instancia del servidor Rancher y al clúster de administración en el que se implementa Rancher Server. Las actualizaciones al sistema operativo Ubuntu del nodo del clúster de gestión se aplican únicamente a revisiones de seguridad críticas y no se actualiza el sistema operativo. Los clústeres de usuario no pueden actualizarse desde NetApp Hybrid Cloud Control.

Lo que necesitará

- **Privilegios de administrador:** Dispone de permisos de administrador del clúster de almacenamiento para realizar la actualización.
- **Servicios de administración:** Ha actualizado su paquete de servicios de administración a la última versión.



Debe actualizar al paquete de servicios de administración más reciente 2.17 o posterior para obtener la funcionalidad Rancher.

- **Puertos del sistema:** Si utiliza NetApp Hybrid Cloud Control para actualizaciones, se ha asegurado de que los puertos necesarios están abiertos. Consulte "[Puertos de red](#)" si quiere más información.
- **Contrato de licencia para el usuario final (CLUF):** A partir de los servicios de administración 2.20.69, debe aceptar y guardar el CLUF antes de utilizar la API o la IU de control de cloud híbrido de NetApp para actualizar una implementación de Rancher:
 - a. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

- b. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
- c. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
- d. Aparece el EULA. Desplácese hacia abajo, seleccione **Acepto para actualizaciones actuales y futuras** y seleccione **Guardar**.

Opciones de actualización

Elija uno de los siguientes procesos de actualización:

- [Utilice la interfaz de usuario de control del cloud híbrido de NetApp para actualizar la puesta en marcha de un Rancher](#)
- [Utilice la API de control de cloud híbrido de NetApp para actualizar la implementación de Rancher](#)

Utilice la interfaz de usuario de control del cloud híbrido de NetApp para actualizar la puesta en marcha de un Rancher

Con la IU de control de cloud híbrido de NetApp, puede actualizar cualquiera de estos componentes en la implementación de Rancher:

- Servidor de rancher
- Motor Kubernetes de rancher (RKE)
- Actualizaciones de seguridad del sistema operativo de los nodos

Lo que necesitará

- Una buena conexión a internet. Las actualizaciones de sitios oscuros (actualizaciones en un sitio sin conectividad externa) no están disponibles.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. Seleccione **Actualizar** cerca de la parte superior derecha de la interfaz.
4. En la página **actualizaciones**, seleccione **Rancher**.
5. Seleccione el menú **acciones** del software que desea actualizar.
 - Servidor de rancher
 - Motor Kubernetes de rancher (RKE)
 - Actualizaciones de seguridad del sistema operativo de los nodos
6. Seleccione **Actualizar** para las actualizaciones de RKE o de servidor RKE o **aplicar actualización** para las actualizaciones de seguridad del sistema operativo del nodo.



Para el sistema operativo del nodo, las actualizaciones sin supervisión de las revisiones de seguridad se ejecutan diariamente, pero el nodo no se reinicia automáticamente. Al aplicar las actualizaciones, reinicia cada nodo para que las actualizaciones de seguridad surtan efecto.

Aparece un banner para indicar que la actualización del componente se ha realizado correctamente. Es posible que haya un retraso de hasta 2 minutos antes de que la interfaz de usuario de control de cloud híbrido de NetApp muestre el número de versión actualizado.

Utilice la API de control de cloud híbrido de NetApp para actualizar la implementación de Rancher

Puede utilizar las API para actualizar cualquiera de estos componentes en la implementación de Rancher:

- Servidor de rancher
- Motor Kubernetes de rancher (RKE)

- Sistema operativo nodo (para actualizaciones de seguridad)

Puede utilizar una herramienta de automatización de su elección para ejecutar las API o la interfaz de usuario de API DE REST disponibles en el nodo de gestión.

Opciones

- [Actualice Rancher Server](#)
- [Actualizar RKE](#)
- [Aplique las actualizaciones de seguridad del sistema operativo del nodo](#)



Para el sistema operativo del nodo, las actualizaciones sin supervisión de las revisiones de seguridad se ejecutan diariamente, pero el nodo no se reinicia automáticamente. Al aplicar las actualizaciones, reinicia cada nodo para que las actualizaciones de seguridad surtan efecto.

Actualice Rancher Server

Comandos API

1. Inicie la solicitud de actualización de la lista de versiones:

```
curl -X POST "https://<managementNodeIP>/k8sdeployer/1/upgrade/rancher-versions" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza "autorizar". El portador `${TOKEN}` está en la respuesta curl.

2. Obtener el estado de la tarea mediante el ID de tarea del comando anterior y copiar el número de la última versión de la respuesta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Inicie la solicitud de actualización del servidor Rancher:

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rancher/<version number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. Obtener el estado de la tarea mediante el ID de tarea de la respuesta del comando de actualización:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. Seleccione **autorizar** y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Seleccione **autorizar** para iniciar una sesión.
 - d. Cierre la ventana de autorización.
3. Compruebe el último paquete de actualización:
 - a. Desde la interfaz de usuario DE LA API DE REST, ejecute **POST /upgrade/rancher-Versions**.
 - b. Desde la respuesta, copie el ID de tarea.
 - c. Ejecute **GET /task/{taskID}** con el ID de tarea del paso anterior.
4. En la respuesta **/task/{taskID}**, copie el último número de versión que desea utilizar para la actualización.
5. Ejecute la actualización de Rancher Server:
 - a. Desde la interfaz de usuario DE LA API DE REST, ejecute **PUT /upgrade/rancher/{version}** con el último número de versión del paso anterior.
 - b. Desde la respuesta, copie el ID de tarea.
 - c. Ejecute **GET /task/{taskID}** con el ID de tarea del paso anterior.

La actualización se completó correctamente cuando el `PercentComplete` lo que indica 100 y.. `results` indica el número de versión actualizada.

Actualizar RKE

Comandos API

1. Inicie la solicitud de actualización de la lista de versiones:

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/rke-versions" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza **"autorizar"**. El portador `${TOKEN}` está en la respuesta curl.

2. Obtener el estado de la tarea mediante el ID de tarea del comando anterior y copiar el número de la última versión de la respuesta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Inicie la solicitud de actualización de RKE

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rke/<version number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. Obtener el estado de la tarea mediante el ID de tarea de la respuesta del comando de actualización:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. Seleccione **autorizar** y complete lo siguiente:

- Introduzca el nombre de usuario y la contraseña del clúster.
- Introduzca el ID de cliente as `mnode-client`.
- Seleccione **autorizar** para iniciar una sesión.
- Cierre la ventana de autorización.

3. Compruebe el último paquete de actualización:

- Desde LA interfaz de usuario DE LA API DE REST, ejecute **POST /upgrade/rke-Versions**.
- Desde la respuesta, copie el ID de tarea.
- Ejecute **GET /task/{taskID}** con el ID de tarea del paso anterior.

4. En la respuesta **/task/{taskID}**, copie el último número de versión que desea utilizar para la actualización.

5. Ejecute la actualización RKE:

- Desde la interfaz de usuario DE LA API DE REST, ejecute **PUT /upgrade/rke/{version}** con el último número de versión del paso anterior.
- Copie el ID de tarea de la respuesta.
- Ejecute **GET /task/{taskID}** con el ID de tarea del paso anterior.

La actualización se completó correctamente cuando el `PercentComplete` lo que indica 100 y.. `results` indica el número de versión actualizada.

Aplique las actualizaciones de seguridad del sistema operativo del nodo

Comandos API

1. Inicie la solicitud de comprobación de actualizaciones:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/upgrade/checkNodeUpdates"  
-H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Usted puede encontrar al portador `${TOKEN}` Lo utiliza el comando API cuando lo utiliza "autorizar". El portador `${TOKEN}` está en la respuesta curl.

2. Obtener el estado de la tarea mediante el Id. De tarea desde el comando anterior y verificar que hay disponible un número de versión más reciente en la respuesta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:  
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Aplique las actualizaciones del nodo:

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/applyNodeUpdates"  
-H "accept: application/json" -H "Authorization: Bearer"
```



Para el sistema operativo del nodo, las actualizaciones sin supervisión de las revisiones de seguridad se ejecutan diariamente, pero el nodo no se reinicia automáticamente. Al aplicar las actualizaciones, reinicia cada nodo secuencialmente para que las actualizaciones de seguridad surtan efecto.

4. Obtener el estado de la tarea mediante el ID de tarea de la actualización `applyNodeUpdates` respuesta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:  
application/json" -H "Authorization: Bearer ${TOKEN}"
```

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Abra la interfaz de usuario de LA API DE REST del nodo de gestión en el nodo de gestión:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. Seleccione **autorizar** y complete lo siguiente:
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Introduzca el ID de cliente as `mnode-client`.
 - c. Seleccione **autorizar** para iniciar una sesión.
 - d. Cierre la ventana de autorización.
3. Compruebe si hay un paquete de actualización disponible:
 - a. Desde la interfaz de usuario DE LA API DE REST, ejecute **GET /upgrade/checkNodeUpdates**.

- b. Desde la respuesta, copie el ID de tarea.
 - c. Ejecute **GET /task/{taskID}** con el ID de tarea del paso anterior.
 - d. En la respuesta **/task/{taskID}**, compruebe que hay un número de versión más reciente que el que se aplica actualmente a los nodos.
4. Aplique las actualizaciones del sistema operativo del nodo:



Para el sistema operativo del nodo, las actualizaciones sin supervisión de las revisiones de seguridad se ejecutan diariamente, pero el nodo no se reinicia automáticamente. Al aplicar las actualizaciones, reinicia cada nodo secuencialmente para que las actualizaciones de seguridad surtan efecto.

- a. Desde la interfaz de usuario DE LA API DE REST, ejecute **POST /upgrade/appleyNodeUpdates**.
- b. Desde la respuesta, copie el ID de tarea.
- c. Ejecute **GET /task/{taskID}** con el ID de tarea del paso anterior.
- d. En la respuesta **/task/{taskID}**, compruebe que se ha aplicado la actualización.

La actualización se completó correctamente cuando el `PercentComplete` lo que indica 100 y.. `results` indica el número de versión actualizada.

Obtenga más información

- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Retire una instalación de Rancher en NetApp HCI

Si ha implementado por accidente Rancher en NetApp HCI con información incorrecta (como un FQDN de Rancher de servidor incorrecto), debe eliminar la instalación y volver a ponerlos en marcha. Siga estos pasos para quitar la instalación de Rancher en la instancia de NetApp HCI.

Esta acción no elimina los clústeres de usuarios.



Puede ser conveniente conservar los clústeres de usuario. Si los conserva, posteriormente puede migrarlos a otra implementación de Rancher. Si desea eliminar los clústeres de usuario, debe hacerlo primero antes de eliminar el servidor Rancher; de lo contrario, es más difícil eliminar los clústeres de usuario después de eliminar el servidor Rancher.

Opciones

- [Elimine el Rancher en NetApp HCI usando el control del cloud híbrido de NetApp](#) (Recomendado)
- [Quite Rancher en NetApp HCI usando la API DE REST](#)

Elimine el Rancher en NetApp HCI usando el control del cloud híbrido de NetApp

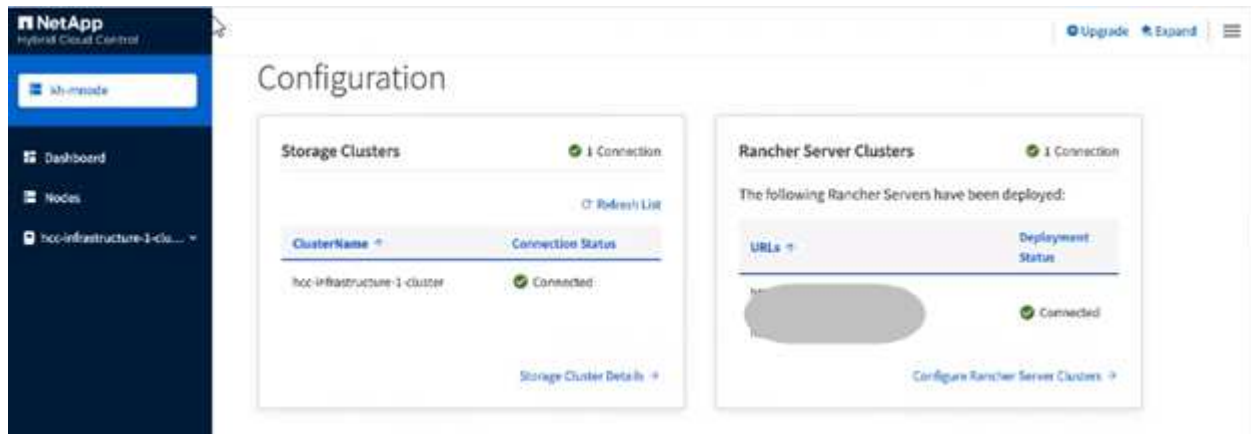
Puede usar la interfaz de usuario web de NetApp Hybrid Cloud Control para quitar las tres máquinas virtuales que se configuraron durante la implementación para alojar el servidor Rancher.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en Hybrid Cloud Control de NetApp proporcionando las credenciales de administrador del clúster de almacenamiento.
3. En el panel de control, haga clic en el menú de la parte superior derecha.
4. Seleccione **Configurar**.



5. En el panel **Rancher Server Clusters**, haga clic en **Configurar clústeres de servidor Rancher**.
6. Seleccione el menú **acciones** para la instalación de Rancher que necesita quitar.



Al hacer clic en **Eliminar** se elimina inmediatamente el Rancher del clúster de administración de NetApp HCI.

7. Seleccione **Eliminar**.

Quite Rancher en NetApp HCI usando la API DE REST

Puede utilizar la API DE REST de NetApp Hybrid Cloud Control para quitar las tres máquinas virtuales que se configuraron durante la implementación para alojar el servidor Rancher.

Pasos

1. Introduzca la dirección IP del nodo de gestión seguida de `/k8sdeployer/api/`:

```
https://[IP address]/k8sdeployer/api/
```

2. Haga clic en **autorizar** o en cualquier icono de bloqueo e introduzca las credenciales de administración del clúster para los permisos de uso de las API.
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Seleccione **solicitar cuerpo** en la lista desplegable Tipo si el valor no está seleccionado.
 - c. Introduzca el ID de cliente as `mnode-client` si el valor no se ha rellenado todavía.
 - d. No introduzca un valor para el secreto de cliente.

- e. Haga clic en **autorizar** para iniciar una sesión.
- f. Cierre la ventana.
3. Cierre el cuadro de diálogo **autorizaciones disponibles**.
4. Haga clic en **POST/destruir**.
5. Haga clic en **probar**.
6. En el cuadro de texto cuerpo de la solicitud, introduzca el FQDN del servidor Rancher como `serverURL` valor.
7. Haga clic en **Ejecutar**.

Después de varios minutos, las máquinas virtuales del servidor Rancher ya no deben verse en la lista hosts and Clusters de vSphere Client. Después de quitarlo, puede usar el control del cloud híbrido de NetApp para volver a poner en marcha Rancher en NetApp HCI.

Obtenga más información

- ["Solución de problemas de implementación de rancher"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["Página de recursos de NetApp HCI"](#)

Mantenimiento de hardware H-Series

Descripción general del mantenimiento de hardware H-Series

Debe realizar tareas de mantenimiento de hardware, como sustituir nodos defectuosos, sustituir unidades defectuosas en los nodos de almacenamiento, y así sucesivamente para garantizar que el sistema funcione de forma óptima.

Estos son los enlaces a las tareas de mantenimiento del hardware:

- ["Sustituya el chasis 2U de la serie H"](#)
- ["Sustituya las unidades de alimentación CC en los nodos H615C y H610S"](#)
- ["Reemplace los DIMM en los nodos de computación"](#)
- ["Sustituya las unidades para los nodos de almacenamiento"](#)
- ["Sustituya los nodos H410C"](#)
- ["Sustituya los nodos H410S"](#)
- ["Reemplace los nodos H610C y H615C"](#)
- ["Sustituya los nodos H610S"](#)
- ["Sustituya las unidades de alimentación"](#)
- ["Sustituir los interruptores SN2010, SN2100 y SN2700"](#)
- ["Sustituya el nodo de almacenamiento en un clúster de dos nodos"](#)

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)
- ["TR-4820: Guía de planificación rápida de redes de NetApp HCI"](#)
- ["Asesor de configuración de NetApp" 5.8.1 o posterior herramienta de validación de red](#)

Sustituya el chasis 2U de la serie H

Si su chasis tiene un fallo de ventilador o un problema de alimentación, debe reemplazarlo lo antes posible. Los pasos del procedimiento de sustitución del chasis dependen de la configuración de NetApp HCI y la capacidad del clúster, lo que requiere considerar y planificar cuidadosamente. Debe ponerse en contacto con el soporte de NetApp para obtener instrucciones y solicitar un chasis de reemplazo.

Acerca de esta tarea

Debe tener en cuenta lo siguiente antes de sustituir el chasis:

- ¿Su rack tiene espacio adicional para un nuevo chasis?
- ¿Alguno de los chasis de la implementación tiene ranuras de nodo sin utilizar?

- Si el rack tiene espacio adicional, ¿puede mover cada uno de los nodos del chasis que ha fallado al nuevo chasis, uno por vez? Debe tener en cuenta que este proceso puede llevar tiempo.
- ¿El clúster de almacenamiento puede permanecer en línea cuando quita los nodos que forman parte del chasis con errores?
- ¿Sus máquinas virtuales (VM) y el clúster ESXi pueden manejar la carga de trabajo cuando quita los nodos de computación que forman parte del chasis con errores?

Opciones de sustitución

Elija una de las siguientes opciones: [Reemplace el chasis cuando haya espacio adicional sin utilizar disponible en el rack](#)

[Sustituya el chasis cuando no se encuentre espacio adicional sin utilizar disponible en el rack](#)

Reemplace el chasis cuando haya espacio adicional sin utilizar disponible en el rack

Si su rack tiene espacio adicional, puede instalar el nuevo chasis y mover los nodos de uno en uno al nuevo chasis. Si alguno de los chasis instalados tiene ranuras para nodos no utilizadas, puede mover los nodos del chasis con errores a las ranuras no utilizadas de uno en uno y, a continuación, quite el chasis con errores. Antes de ser el procedimiento, asegúrese de que las longitudes de los cables sean suficientes y de que los puertos del switch estén disponibles.



Los pasos para mover nodos de computación son diferentes de los pasos para mover nodos de almacenamiento. Debe asegurarse de que los nodos estén apagados correctamente antes de moverlos. Después de mover todos los nodos del chasis con errores, debe quitar el chasis del rack y devolverlo a NetApp.

Instale el chasis nuevo

Puede instalar el nuevo chasis en el espacio de rack disponible y mover los nodos hacia él.

Lo que necesitará

- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.
- Tiene el chasis de reemplazo.
- Tiene un ascensor o dos o más personas para realizar los pasos.
- Tiene un destornillador Phillips del número 1.

Pasos

1. Póngase protección antiestática.
2. Desembale el chasis de repuesto. Conserve el embalaje para cuando devuelva el chasis fallido a NetApp.
3. Inserte los rieles que se le enviaron junto con el chasis.
4. Deslice el chasis de repuesto en el rack.



Utilice siempre mano de obra suficiente o un elevador mientras instala el chasis.

5. Fije el chasis al rack con los tornillos de fijación delanteros y apriete los tornillos con el destornillador.

Mover un nodo de computación

Antes de mover un nodo de computación al nuevo chasis o a un chasis existente que tiene ranuras adicionales sin utilizar, debe migrar las máquinas virtuales (VM), apagar el nodo correctamente y etiquetar los cables insertados en el nodo.



Asegúrese de tener protección antiestática al mover el nodo.

Pasos

1. Tome nota del número de serie del nodo en la etiqueta adhesiva que aparece en la parte posterior del nodo.
2. En VMware vSphere Web Client, seleccione **hosts and Clusters**, seleccione un nodo (host) y, a continuación, seleccione **Monitor > hardware Status > Sensors**.
3. En la sección **Sensores**, busque el número de serie que anotó en la pegatina situada en la parte posterior del nodo.
4. Después de encontrar el número de serie coincidente, migre las máquinas virtuales a otro host disponible.



Consulte la documentación de VMware para conocer los pasos de migración.

5. Haga clic con el botón derecho del ratón en el nodo y seleccione **Alimentación > Apagar**. Ahora está listo para quitar físicamente el nodo del chasis.
6. Etiquete el nodo y todos los cables que hay en la parte posterior del nodo.
7. Retire el nodo del chasis tirando del tirador de leva situado en el lado derecho de cada nodo y tirando del nodo hacia fuera con las dos asas de leva.
8. Reinstale el nodo en el nuevo chasis presionando el nodo hasta que oiga un clic. Las etiquetas que había conectado al nodo antes de quitar le guía de ayuda. El nodo se enciende automáticamente cuando lo instala correctamente.



Asegúrese de que admite el nodo en cuando lo instale. No use una fuerza excesiva mientras presiona el nodo hacia el chasis.



Si se instala en el chasis nuevo, asegúrese de instalar el nodo en su ranura original en el chasis.

9. Vuelva a conectar los cables a los mismos puertos en la parte posterior del nodo. Las etiquetas que tenía en los cables cuando los desconectó le ayudan a guiar.



Asegúrese de no forzar los cables en los puertos; podría dañar los cables, los puertos o ambos.

10. Confirme que el nodo de computación (host) figura en el clúster ESXi de VMware vSphere Web Client.
11. Ejecute estos pasos para todos los nodos de computación en el chasis con errores.

Mover un nodo de almacenamiento

Antes de mover los nodos de almacenamiento al nuevo chasis, debe quitar las unidades, apagar los nodos correctamente y etiquetar todos los componentes.

Pasos

1. Identifique el nodo que se va a quitar del siguiente modo:
 - a. Tenga en cuenta el número de serie del nodo en la etiqueta adhesiva de la parte posterior del nodo.
 - b. En VMware vSphere Web Client, seleccione **NetApp Element Management** y copie la dirección IP de MVIP.
 - c. Utilice la dirección IP de MVIP en un explorador web para iniciar sesión en la interfaz de usuario del software de NetApp Element con el nombre de usuario y la contraseña que se configuraron en el motor de implementación de NetApp.
 - d. Seleccione **Cluster > Nodes**.
 - e. Haga coincidir el número de serie anotado con el número de serie (etiqueta de servicio) que aparece en la lista.
 - f. Tome nota del ID de nodo del nodo.
2. Una vez que identifique el nodo, mueva las sesiones iSCSI fuera del nodo mediante la siguiente llamada API:


```
`wget --no-check-certificate -q --user=<USER> --password=<PASS> -O - --post-data '{
"method":"MovePrimariesAwayFromNode", "params":{"nodeID":<NODEID>}' https://<MVIP>/json-rpc/
8.0`MVIP
```

 es la dirección IP de MVIP, NODEID es el ID del nodo, EL USUARIO es el nombre de usuario que configuró en el motor de puesta en marcha de NetApp cuando se configura NetApp HCI y PASS es la contraseña que configuró en el motor de implementación de NetApp cuando se configura NetApp HCI.
3. Seleccione **Cluster > Drives** para eliminar las unidades asociadas al nodo.



Debe esperar a que las unidades que quitó para mostrarse como disponibles antes de quitar el nodo.

4. Seleccione **Cluster > Nodes > Actions > Remove** para eliminar el nodo.
5. Utilice la siguiente llamada API para apagar el nodo:


```
`wget --no-check-certificate -q --user=<USER> --password=<PASS> -O - --post-data '{
"method":"Shutdown", "params":{"option":"halt", "nodes":[ <NODEID>]}' https://<MVIP>/json-rpc/8.0`MVIP
```

 es la dirección IP de MVIP, NODEID es el ID del nodo, EL USUARIO es el nombre de usuario que configuró en el motor de puesta en marcha de NetApp cuando se configura NetApp HCI y PASS es la contraseña que configuró en el motor de implementación de NetApp cuando se configura NetApp HCI. Después de apagar el nodo, estará listo para quitarlo físicamente del chasis.
6. Quite las unidades del nodo en el chasis de la siguiente manera:
 - a. Retire el bisel.
 - b. Etiquete las unidades.
 - c. Abra la palanca de leva y deslice con cuidado cada unidad con ambas manos.
 - d. Coloque las unidades en una superficie nivelada y antiestática.
7. Quite el nodo del chasis de la siguiente manera:
 - a. Etiquete el nodo y los cables conectados.
 - b. Tire hacia abajo del asa de leva en el lado derecho de cada nodo y tire del nodo para sacarlo con las dos asas de leva.
8. Vuelva a instalar el nodo en el chasis empujando el nodo hacia dentro hasta que oiga un clic. Las etiquetas que había conectado al nodo antes de quitar le guía de ayuda.



Asegúrese de que admite el nodo en cuando lo instale. No use una fuerza excesiva mientras presiona el nodo hacia el chasis.



Si se instala en el chasis nuevo, asegúrese de instalar el nodo en su ranura original en el chasis.

9. Instale las unidades en sus ranuras respectivas del nodo presionando el asa de leva en cada unidad hasta que haga clic.
10. Vuelva a conectar los cables a los mismos puertos en la parte posterior del nodo. Las etiquetas que había conectado a los cables cuando los desconectó le ayudarán a guiar.



Asegúrese de no forzar los cables en los puertos; podría dañar los cables, los puertos o ambos.

11. Después de que el nodo se encienda, añada el nodo al clúster.



Puede que el nodo tarde hasta 2 minutos en agregarse y se muestre en **nodos > activo**.

12. Añada las unidades.
13. Ejecute estos pasos para todos los nodos de almacenamiento del chasis.

Sustituya el chasis cuando no se encuentre espacio adicional sin utilizar disponible en el rack

Si el rack no dispone de espacio adicional y si ninguno de los chasis de la implementación tiene ranuras de nodo sin usar, debe determinar qué puede permanecer en línea, de ser necesario, antes de realizar el procedimiento de reemplazo.

Acerca de esta tarea

Debe tener en cuenta los siguientes puntos antes de sustituir el chasis:

- ¿Su clúster de almacenamiento puede permanecer en línea sin los nodos de almacenamiento en el chasis con errores? Si la respuesta es no, debe apagar todos los nodos (tanto de computación como de almacenamiento) en la implementación de NetApp HCI. Si la respuesta es sí, solo puede apagar los nodos de almacenamiento en el chasis con errores.
- ¿Sus máquinas virtuales y el clúster ESXi pueden permanecer en línea sin los nodos de computación del chasis con errores? Si la respuesta es no, debe apagar o migrar las máquinas virtuales adecuadas para poder apagar los nodos de computación en el chasis con errores. Si la respuesta es sí, solo puede apagar los nodos de computación del chasis con errores.

Apague un nodo de computación

Antes de mover el nodo de computación al nuevo chasis, debe migrar las máquinas virtuales, apagarlo correctamente y etiquetar los cables insertados en el nodo.

Pasos

1. Tome nota del número de serie del nodo en la etiqueta adhesiva que aparece en la parte posterior del nodo.
2. En VMware vSphere Web Client, seleccione **hosts and Clusters**, seleccione un nodo (host) y, a continuación, seleccione **Monitor > hardware Status > Sensors**.
3. En la sección **Sensores**, busque el número de serie que anotó en la pegatina situada en la parte posterior del nodo.

4. Después de encontrar el número de serie coincidente, migre las máquinas virtuales a otro host disponible.



Consulte la documentación de VMware para conocer los pasos de migración.

5. Haga clic con el botón derecho del ratón en el nodo y seleccione **Alimentación > Apagar**. Ahora está listo para quitar físicamente el nodo del chasis.

Apague un nodo de almacenamiento

Consulte los pasos [aquí](#).

Quite el nodo

Debe asegurarse de quitar el nodo con cuidado del chasis y de etiquetar todos los componentes. Los pasos para quitar físicamente el nodo son los mismos para los nodos de computación y de almacenamiento. Para un nodo de almacenamiento de, quite la unidad antes de quitar el nodo.

Pasos

1. Para un nodo de almacenamiento de, quite las unidades del nodo en el chasis de la siguiente manera:
 - a. Retire el bisel.
 - b. Etiquete las unidades.
 - c. Abra la palanca de leva y deslice con cuidado cada unidad con ambas manos.
 - d. Coloque las unidades en una superficie nivelada y antiestática.
2. Quite el nodo del chasis de la siguiente manera:
 - a. Etiquete el nodo y los cables conectados.
 - b. Tire hacia abajo del asa de leva en el lado derecho de cada nodo y tire del nodo para sacarlo con las dos asas de leva.
3. Ejecute estos pasos en todos los nodos que desee quitar. Ahora está listo para quitar el chasis con errores.

Sustituya el chasis

Si el rack no dispone de espacio adicional, debe desinstalar el chasis con errores y reemplazarlo por el nuevo chasis.

Pasos

1. Póngase protección antiestática.
2. Desembale el chasis de repuesto y manténgalo en una superficie nivelada. Conserve el embalaje para cuando devuelva la unidad con error a NetApp.
3. Retire el chasis que ha fallado del bastidor y colóquelo en una superficie nivelada.



Utilice mano de obra suficiente o un elevador mientras mueve un chasis.

4. Retire los rieles.
5. Instale los nuevos rieles que se le enviaron con el chasis de reemplazo.
6. Deslice el chasis de repuesto en el rack.
7. Fije el chasis al rack con los tornillos de fijación delanteros y apriete los tornillos con el destornillador.

8. Instale los nodos en el nuevo chasis de la siguiente manera:

- a. Vuelva a instalar el nodo en su ranura original del chasis. Para ello, empuje el nodo hasta que oiga un clic. Las etiquetas que ha conectado al nodo antes de haberlo quitado como guía de ayuda.




Asegúrese de que admite el nodo en cuando lo instale. No use una fuerza excesiva mientras presiona el nodo hacia el chasis.

- b. Para los nodos de almacenamiento, instale las unidades en sus ranuras respectivas del nodo presionando el asa de leva de cada unidad hasta que haga clic.
- c. Vuelva a conectar los cables a los mismos puertos en la parte posterior del nodo. Las etiquetas que está conectado a los cables cuando los ha desconectado le ayudan a guiar.



Asegúrese de no forzar los cables en los puertos; podría dañar los cables, los puertos o ambos.

9. Asegúrese de que los nodos estén en línea de la siguiente manera:

Opción	Pasos
Si reinstaló todos los nodos (tanto de almacenamiento como de computación) en la implementación de NetApp HCI	<ul style="list-style-type: none">a. En VMware vSphere Web Client, confirme que los nodos de computación (hosts) figuran en el clúster ESXi.b. En el plugin de Element para vCenter Server, confirme que los nodos de almacenamiento se enumeran como activos.
Si solo reinstaló los nodos en el chasis con errores	<ul style="list-style-type: none">a. En VMware vSphere Web Client, confirme que los nodos de computación (hosts) figuran en el clúster ESXi.b. En el plugin de Element para vCenter Server, seleccione Cluster > Nodes > Pending.c. Seleccione el nodo y seleccione Agregar.  Puede que el nodo tarde hasta 2 minutos en agregarse y se muestre en nodos > activo.d. Seleccione unidades.e. En la lista Available, añada las unidades.f. Realice estos pasos en todos los nodos de almacenamiento que reinstaló.

10. Verifique que los volúmenes y los almacenes de datos estén actualizados y accesibles.

Obtenga más información

- ["Recursos de NetApp HCI"](#)

Sustituya las unidades de alimentación CC en los nodos H615C y H610S

Los nodos H615C y H610S admiten dos unidades de fuente de alimentación de -48 V a -60 V CC . Estas unidades están disponibles como complementos opcionales cuando se solicitan los nodos H615C o H610S. Puede utilizar estas instrucciones para extraer las unidades de alimentación de CA del chasis y sustituirlas por unidades de alimentación de CC, o bien sustituir una unidad de alimentación de CC defectuosa por una nueva fuente de alimentación de CC.

Lo que necesitará

- Si va a sustituir una unidad de fuente de alimentación de CC defectuosa, ha adquirido una unidad de alimentación de CC de repuesto.
- Si va a intercambiar las unidades de suministro de alimentación de CA en el chasis por unidades de CC, ha tenido en cuenta el tiempo de inactividad para el procedimiento.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.
- Se aseguró de que se cumplan los requisitos del suministro de alimentación:
 - Tensión de alimentación: $-(48-60)\text{ V CC}$
 - Consumo de corriente: 37A (máximo)
 - Requisitos del disyuntor: Disyuntor 40A
- Se ha asegurado de que los materiales de su entorno cumplen las especificaciones RoHS.
- Debe asegurarse de que se cumplan los requisitos de cable:
 - Un cable negro máximo (trenzado) de 2 m UL 10 AWG [$-(48-60)\text{ V CC}$]
 - Un cable rojo UL 10 AWG, máximo de 2 m (trenzado) [retorno de CC V]
 - Un cable UL 10 AWG, máximo de 2 m verde/amarillo, verde con banda amarilla, cable trenzado (tierra de seguridad)

Acerca de esta tarea

El procedimiento se aplica a los siguientes modelos de nodo:

- Una unidad de rack (1U) chasis de computación H615C
- Chasis de almacenamiento H610S de 1U



En el caso H615C y H610S, los términos "nodo" y "chasis" se utilizan indistintamente porque los componentes de nodo y chasis no son separados, a diferencia del caso del chasis de 2U de cuatro nodos.



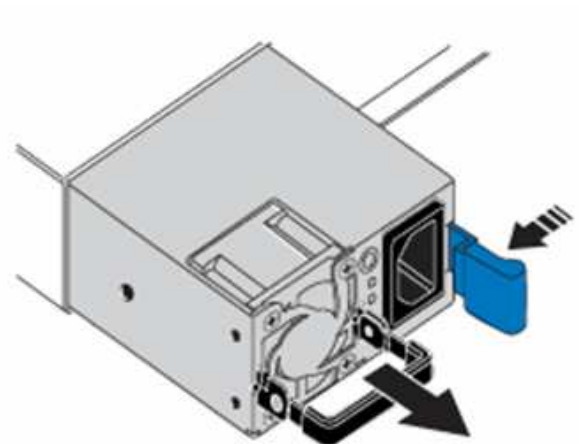
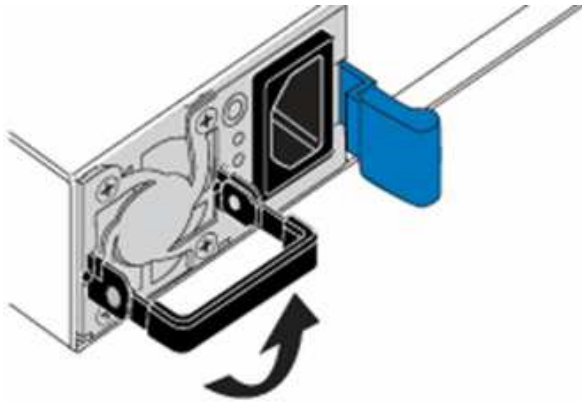
No puede mezclar unidades de fuente de alimentación de CA y CC en su instalación.

Pasos

1. Apague las unidades de alimentación y desenchufe los cables de alimentación. Si va a sustituir una

unidad de fuente de alimentación de CC defectuosa, apague la fuente de alimentación y retire todos los cables insertados en el conector azul.

2. Levante el asa de la leva y presione el pestillo azul para sacar la unidad de alimentación.

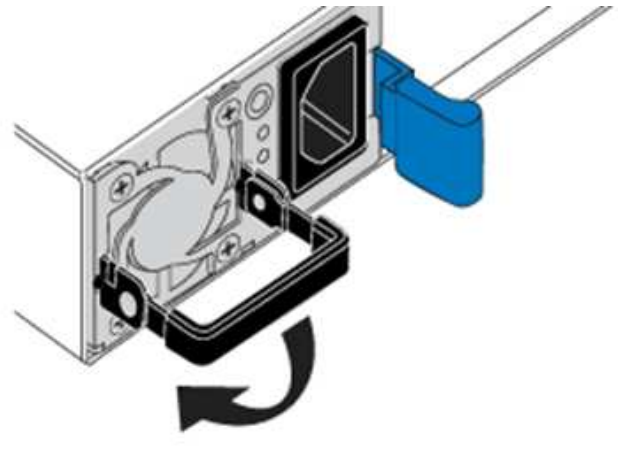
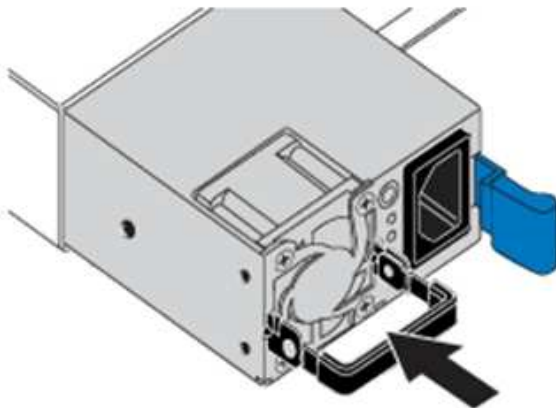


La ilustración es un ejemplo. La ubicación de la fuente de alimentación en el chasis y el color del botón de liberación varían según el tipo de chasis que tenga.



Asegúrese de utilizar ambas manos para soportar el peso de la unidad de alimentación.

3. Con ambas manos, alinee los bordes de la unidad de alimentación con la abertura del chasis, empuje suavemente la unidad hacia el chasis con el asa de leva hasta que encaje en su sitio y vuelva a colocar el mango de leva en la posición vertical.



4. Conecte el cable de las unidades de alimentación de CC. Asegúrese de que la fuente de alimentación está apagada mientras realiza el cableado de la unidad de alimentación de CC y de la fuente de alimentación.
 - a. Inserte los cables negro, rojo y verde/amarillo en los conectores azules.
 - b. Inserte el conector azul en las unidades de fuente de alimentación de CC y en la fuente de alimentación.



5. Encienda las unidades de fuente de alimentación de CC.



Los LED de la fuente de alimentación se encienden cuando la unidad de fuente de alimentación de CC se conecta. Las luces LED verdes indican que las unidades de la fuente de alimentación funcionan correctamente.

6. Devuelva la unidad defectuosa a NetApp siguiendo las instrucciones de la caja que le ha enviado.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Reemplace los DIMM en los nodos de computación

Puede sustituir un módulo de memoria en línea doble (DIMM) defectuoso en los nodos de computación NetApp HCI en lugar de sustituir el nodo completo.

Lo que necesitará

- Antes de iniciar este procedimiento, debe haberse puesto en contacto con el servicio de soporte de NetApp y haber recibido una pieza de repuesto. Durante la instalación de la sustitución, el soporte estará implicado. Si aún no lo ha hecho, póngase en contacto con ["Soporte técnico"](#).
- Ha planificado experimentar tiempos de inactividad del sistema, ya que necesita desconectar o apagar el nodo y arrancar el nodo en el modo a prueba de fallos de NetApp para acceder a la interfaz de usuario del terminal (TUI).

Acerca de esta tarea

Este procedimiento se aplica a los siguientes modelos de nodo de computación:

- Nodos H410C. Un nodo H410C se inserta en un chasis 2U NetApp HCI.
- Nodo H610C. Se integra un nodo H610C en el chasis.
- Nodo H615C. Existe un nodo H615C integrado en el chasis.



Los nodos H410C y H615C incluyen DIMM de diferentes proveedores. Asegúrese de no mezclar DIMM de diferentes proveedores en un chasis.



Los términos "chasis" y "nodo" se utilizan indistintamente en el caso de H610C y H615C, ya que el nodo y el chasis no son componentes separados.

Estos son los pasos para sustituir DIMM en los nodos de computación:

- [Prepárese para sustituir el DIMM](#)
- [Sustituya el DIMM del chasis](#)

Prepárese para sustituir el DIMM

Cuando se producen problemas con el DIMM, VMware ESXi muestra alertas como Memory Configuration Error, Memory Uncorrectable ECC, Memory Transition to Critical, y Memory Critical Overtemperature. Incluso si las alertas desaparecen al cabo de un tiempo, el problema del hardware puede persistir. Debe diagnosticar y tratar el DIMM defectuoso. Puede obtener información sobre el DIMM defectuoso desde vCenter Server. Si necesita más información de la que está disponible en vCenter Server, debe ejecutar la comprobación del hardware en la TUI.

Pasos

1. Identifique la ranura que registró el error de la siguiente manera:
 - a. Para H615C, haga lo siguiente:
 - i. Inicie sesión en la interfaz de usuario de BMC.
 - ii. Seleccione **registros e informes > Registro de sucesos de IPMI**.
 - iii. En el registro de eventos, busque el error de memoria e identifique la ranura en la que se registró el error.



- b. Para H410C, haga lo siguiente:
 - i. Inicie sesión en la interfaz de usuario de BMC.
 - ii. Seleccione **Estado del servidor > Registro de sucesos de mantenimiento**.
 - iii. En el registro de eventos, busque el error de memoria e identifique la ranura en la que se registró el error.

Severity	Time Stamp	Sensor	Description
!		BIOS OEM(Memory Error)	DIMM Receive Enable training is failed. (P2-DIMMF1) - Assertion

2. Siga los pasos para identificar el número de referencia del fabricante del DIMM.



Los nodos H410C y H615C incluyen DIMM de diferentes fabricantes. No debe combinar distintos tipos de DIMM en el mismo chasis. Debe identificar el fabricante del DIMM defectuoso y solicitar una sustitución del mismo tipo.

- a. Inicie sesión en el BMC para iniciar la consola en el nodo.

b. Pulse **F2** en el teclado para acceder al menú **Personalizar el sistema/Ver registros**.

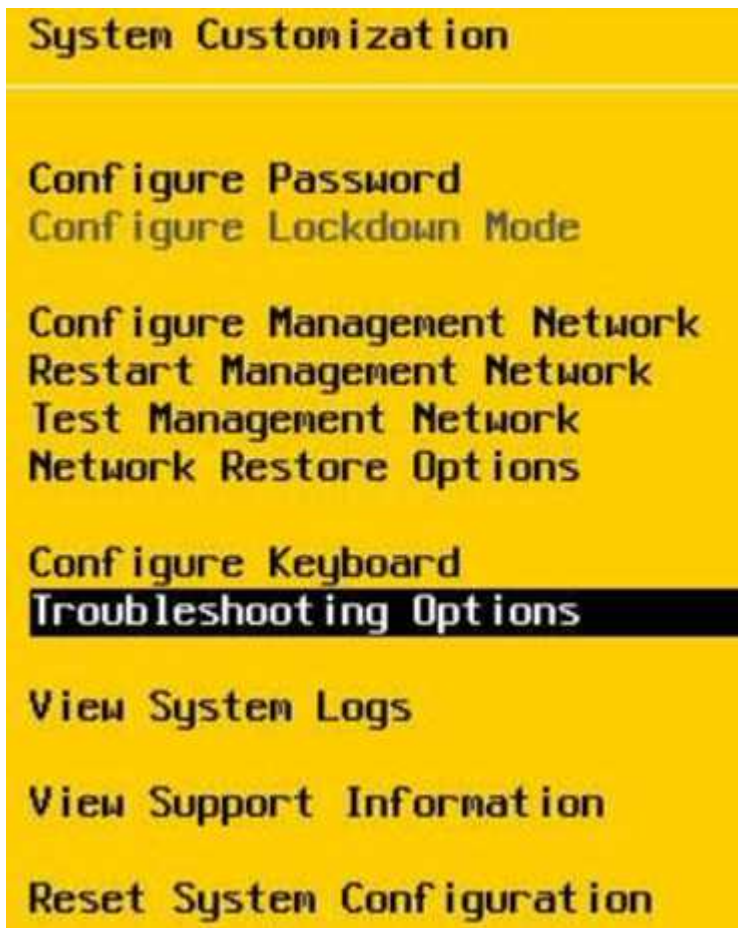
c. Introduzca la contraseña cuando se le solicite.



La contraseña debe coincidir con la configuración en el motor de implementación de NetApp al configurar NetApp HCI.



a. En el menú Personalización del sistema, pulse la flecha hacia abajo para ir a Opciones de solución de problemas y pulse **Intro**.



- b. En el menú Troubleshooting Mode Options, utilice la flecha hacia arriba o hacia abajo para habilitar el shell ESXi y SSH, que están deshabilitados de forma predeterminada.
- c. Pulse la tecla <Esc> dos veces para salir de Opciones de solución de problemas.
- d. Ejecute el `smbiosDump` comando mediante una de las siguientes opciones:

Opción	Pasos
Opción A	<ol style="list-style-type: none"> i. Conéctese al host ESXi (nodo de computación) mediante la dirección IP del host y las credenciales raíz que haya definido. ii. Ejecute el <code>smbiosDump</code> comando. Consulte la siguiente salida de ejemplo: <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> `Memory Device:#30 Location: "P1-DIMMA1" Bank: "P0_Node0_Channel0_Dimm0" Manufacturer:"Samsung" Serial: "38EB8380" Asset Tag: "P1-DIMMA1_AssetTag (date:18/15) " Part Number: "M393A4K40CB2-CTD" Memory Array: #29 Form Factor: 0x09 (DIMM) Type: 0x1a (DDR4) Type Detail: 0x0080 (Synchronous) Data Width: 64 bits (+8 ECC bits) Size: 32 GB` </pre> </div>
Opción B	<ol style="list-style-type: none"> i. Pulse Alt + F1 para introducir shell e iniciar sesión en el nodo para ejecutar el comando.

3. Póngase en contacto con el soporte de NetApp para obtener ayuda sobre los siguientes pasos. El soporte de NetApp requiere la siguiente información para procesar la sustitución de una pieza:
 - Número de serie del nodo
 - Nombre del clúster
 - Detalles del registro de eventos del sistema desde la interfaz de usuario de BMC
 - Salida de `smbiosDump` comando

Sustituya el DIMM del chasis

Antes de quitar y sustituir físicamente el DIMM defectuoso en el chasis, asegúrese de haber realizado todo el ["pasos preparatorios"](#).



Los DIMM deben sustituirse en las mismas ranuras de las que se han retirado.

Pasos

1. Para acceder al nodo, inicie sesión en vCenter Server.
2. Haga clic con el botón derecho en el nodo que notifica el error y seleccione la opción para colocar el nodo en modo de mantenimiento.
3. Migrar las máquinas virtuales (VM) a otro host disponible.



Consulte la documentación de VMware para conocer los pasos de migración.

4. Apague el chasis o el nodo.



En los chasis H610C o H615C, apague el chasis. Para los nodos H410C en un chasis 2U de cuatro nodos, apague solo el nodo con el DIMM defectuoso.

5. Retire los cables de alimentación y los cables de red, deslice con cuidado el nodo o el chasis hacia fuera del rack y colóquelo en una superficie plana y antiestática.



Considere la posibilidad de utilizar bridas de torsión para cables.

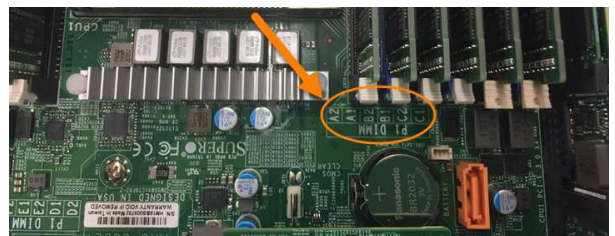
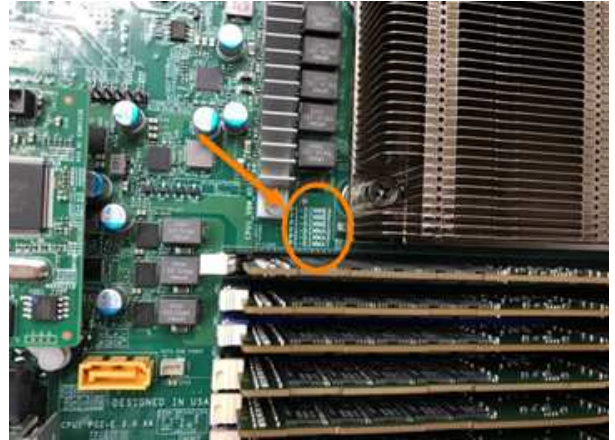
6. Coloque protección antiestática antes de abrir la cubierta del chasis para sustituir el DIMM.
7. Realice los pasos relevantes para su modelo de nodo:

Modelo de nodo

H410C

Pasos

- a. Encuentre el DIMM con errores haciendo coincidir el número de ranura/ID que anotó anteriormente con la numeración en la placa base. A continuación se muestran imágenes de ejemplo que muestran los números de ranura del DIMM en la placa base:



- b. Presione los dos clips de retención hacia afuera y tire con cuidado del DIMM hacia arriba. A continuación se muestra una imagen de ejemplo que muestra los clips de retención:



- c. Instale el módulo DIMM de repuesto correctamente. Cuando inserte el DIMM correctamente en la ranura, los dos clips se bloquean en su lugar.



Asegúrese de tocar únicamente los extremos traseros del módulo DIMM. Si presiona otras partes del módulo DIMM, se podrían producir daños en el hardware.

Modelo de nodo

H610C

Pasos

- a. Levante la cubierta como se muestra en la siguiente imagen:



- b. Afloje los cuatro tornillos de bloqueo azules situados en la parte posterior del nodo. A continuación se muestra una imagen de ejemplo que muestra la ubicación de dos tornillos de bloqueo; los otros dos se encuentran en el otro lado del nodo:



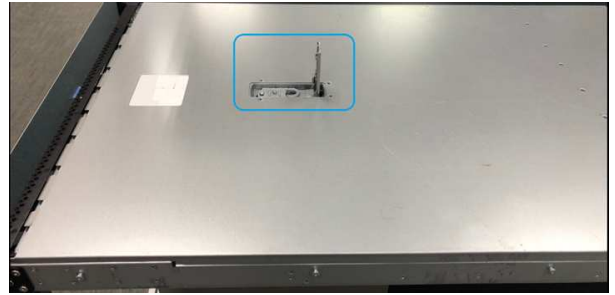
- c. Retire los espacios en blanco de ambas tarjetas PCI.
- d. Retire la GPU y la cubierta de flujo de aire.
- e. Encuentre el DIMM con errores haciendo coincidir el número de ranura/ID que anotó anteriormente con la numeración en la placa base. Aquí hay una imagen de ejemplo que muestra la ubicación de los números de ranura DIMM en la placa base:

Modelo de nodo

H615C

Pasos

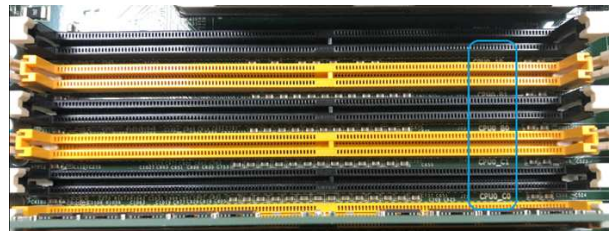
- a. Levante la cubierta como se muestra en la siguiente imagen:



- b. Quite la GPU (si el nodo H615C tiene la GPU instalada) y la cubierta de flujo de aire.



- c. Encuentre el DIMM con errores haciendo coincidir el número de ranura/ID que anotó anteriormente con la numeración en la placa base. Aquí hay una imagen de ejemplo que muestra la ubicación de los números de ranura DIMM en la placa base:



- d. Presione los dos clips de retención hacia afuera y tire con cuidado del DIMM hacia arriba.
- e. Instale el módulo DIMM de repuesto correctamente. Cuando inserte el DIMM correctamente en la ranura, los dos clips se bloquean en su lugar.



Asegúrese de tocar únicamente los extremos traseros del módulo DIMM. Si presiona otras partes del módulo DIMM, se podrían producir daños en el hardware.

Vuelva a colocar la cubierta de flujo de aire.

Vuelva a colocar la cubierta en el nodo.

8. Inserte los cables de alimentación y los cables de red. **Asegúrese de que todas las luces de puerto se encienden.**
9. Pulse el botón de encendido en la parte frontal del nodo **si no se enciende automáticamente cuando lo instala.**
 - h. Instale el chasis H610C en el rack, **asegurándose de que el chasis haga clic cuando lo deslice en su lugar.**
10. Después de que se muestre el nodo en vSphere, haga clic con el botón derecho en el nombre y saque el nodo del modo de mantenimiento.
11. Verifique la información de hardware de la siguiente manera:
 - a. Inicie sesión en la interfaz de usuario del controlador de administración de la placa base (BMC).
 - b. Seleccione **sistema > Información de hardware** y compruebe los módulos DIMM enumerados.

El futuro

Una vez que el nodo vuelve a su funcionamiento normal, en vCenter, compruebe la pestaña Summary para garantizar que la capacidad de memoria sea lo esperado.



Si DIMM no se ha instalado correctamente, el nodo funcionará con normalidad pero con una capacidad de memoria inferior a la esperada.



Después del procedimiento de reemplazo de DIMM, puede borrar las advertencias y errores en la pestaña hardware Status de vCenter. Puede hacer esto si desea borrar el historial de errores relacionados con el hardware que ha sustituido. ["Leer más"](#).

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Sustituya las unidades para los nodos de almacenamiento

Si una unidad está defectuosa o si el nivel de deterioro de la unidad está por debajo de un umbral, debe reemplazarla. Las alarmas en la interfaz de usuario del software Element y VMware vSphere Web Client se notifican cuando se produce un error en una unidad o se produce un fallo. Es posible cambiar en caliente una unidad con error.

Acerca de esta tarea

Este procedimiento permite reemplazar unidades en nodos de almacenamiento H610S y H410S. Al quitar una unidad, esta se desconecta. Los datos en la unidad se extraen y se migran a otras unidades del clúster. La migración de datos a otras unidades activas del sistema puede demorar desde algunos minutos hasta una hora según el uso de la capacidad y las operaciones de I/O activas en el clúster.

Prácticas recomendadas para gestionar unidades

Se deben seguir las siguientes prácticas recomendadas para gestionar las unidades:

- Mantenga la unidad en la bolsa ESD hasta que esté listo para instalarla.
- Abra la bolsa ESD a mano o corte la parte superior con unas tijeras.
- Utilice siempre una muñequera ESD conectada a una superficie sin pintar en su chasis.

- Utilice siempre ambas manos cuando quite, instale o lleve una unidad.
- No fuerce nunca una unidad en el chasis.
- Utilice siempre paquetes aprobados cuando los lleve.
- No coloque las unidades entre sí.

Prácticas recomendadas para agregar y quitar unidades


Debe seguir estas prácticas recomendadas para añadir unidades al clúster y quitar unidades del clúster:

- Añada todas las unidades de bloques y asegúrese de que la sincronización de bloques se complete antes de añadir las unidades de segmentos.
- Para el software Element 10.x y versiones posteriores, añada todas las unidades de bloques a la vez. Asegúrese de no hacerlo para más de tres nodos a la vez.
- Para el software Element 9.x y versiones anteriores, añada tres unidades a la vez que le permitan sincronizarse completamente antes de añadir el siguiente grupo de tres.
- Quite la unidad de segmentos y asegúrese de que la sincronización de segmentos se complete antes de quitar las unidades de bloques.
- Quite todas las unidades de bloques de un único nodo a la vez. Asegúrese de que toda la sincronización de bloques esté completa antes de moverse al siguiente nodo.

Pasos

1. Quite la unidad del clúster mediante la interfaz de usuario del software NetApp Element o el punto de extensión NetApp Element Management del plugin de Element para vCenter Server.

Opción	Pasos
Usar la interfaz de usuario de Element	<ol style="list-style-type: none"> a. En la interfaz de usuario de Element, seleccione Cluster > Drives. b. Haga clic en error para ver la lista de unidades con errores. c. Anote el número de ranura de la unidad con error. Esta información se necesita para localizar la unidad con error en el chasis. d. Haga clic en acciones para la unidad que desea quitar. e. Haga clic en Quitar. <p>Ahora puede quitar físicamente la unidad del chasis.</p>

Opción	Pasos
Usar el plugin de Element para la interfaz de usuario de vCenter Server	<p>a. En el punto de extensión NetApp Element Management de vSphere Web Client, seleccione Gestión de NetApp Element > clúster.</p> <p>b. Si se añaden dos o más clústeres, el clúster que se planea utilizar para la tarea debe estar seleccionado en la barra de navegación.</p> <p>c. Seleccione todo en la lista desplegable para ver la lista completa de unidades.</p> <p>d. Seleccione la casilla de comprobación de cada unidad que desea quitar.</p> <p>e. Seleccione Quitar unidades.</p> <p>f. Confirme la acción.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 20px;"> <p> Si no hay suficiente capacidad para quitar las unidades activas antes de quitar un nodo, se muestra un mensaje de error al confirmar la eliminación de la unidad. Después de resolver el error, ahora puede quitar físicamente la unidad del chasis.</p> </div>

2. Sustituya la unidad del chasis:

- a. Desembale la unidad de repuesto y colóquela en una superficie plana y sin estática cerca del bastidor. Guarde los materiales de embalaje para cuando devuelva la unidad con error a NetApp. Aquí tiene la vista frontal de los nodos de almacenamiento H610S y H410S con las unidades:

H610S storage node



H410S storage nodes in a four-node chassis



- b. Realice los pasos según el modelo de nodo:

Modelo de nodo

H410S

Pasos

- i. Identifique el nodo haciendo coincidir el número de serie (etiqueta de servicio) con el número que anotó abajo en la interfaz de usuario de Element. El número de serie está en una pegatina situada en la parte posterior de cada nodo. Después de identificar el nodo, se puede usar la información de ranura para identificar la ranura en la que está ubicada la unidad con error. Las unidades se ordenan alfabéticamente de La A a la D y del 0 al 5.
- ii. Retire el bisel.
- iii. Pulse el botón de liberación de la unidad con error:

**Release button**

Al pulsar el botón de liberación, la palanca de leva de los resortes de accionamiento se abre parcialmente y la unidad se libera del plano medio.

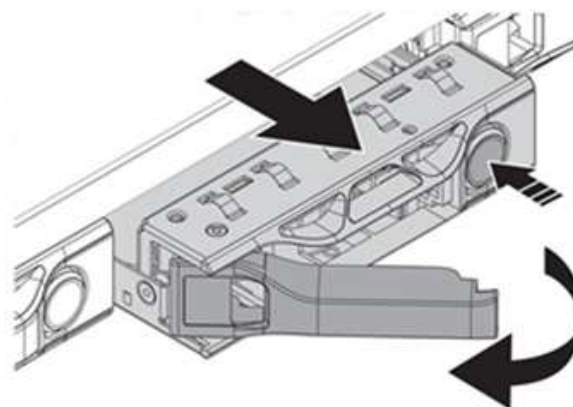
- iv. Abra el mango de la leva y deslice la unidad con cuidado con ambas manos.
- v. Coloque la unidad sobre una superficie nivelada y antiestática.
- vi. Inserte la unidad de sustitución en la ranura completamente en el chasis con ambas manos.
- vii. Presione el asa de la leva hasta que haga clic.
- viii. Vuelva a instalar el bisel.
- ix. Notifique al soporte de NetApp sobre el reemplazo de la unidad. El soporte de NetApp proporcionará instrucciones para la devolución de la unidad con error.

Modelo de nodo

H610S

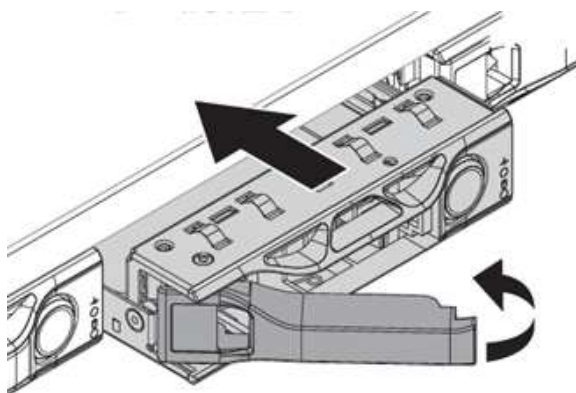
Pasos

- i. Coincida el número de ranura de la unidad con error desde la interfaz de usuario de Element con el número en el chasis. El LED de la unidad con error se ilumina en ámbar.
- ii. Retire el bisel.
- iii. Pulse el botón de liberación y quite la unidad con error como se muestra en la siguiente ilustración:



Asegúrese de que el asa de la bandeja está completamente abierto antes de intentar sacar la unidad del chasis.

- iv. Deslice la unidad hacia fuera y colóquela sobre una superficie nivelada y sin estática.
- v. Pulse el botón de liberación de la unidad de repuesto antes de insertarla en el compartimiento para unidades. Los muelles del mango de la bandeja de unidades se abren.



- vi. Inserte la transmisión de sustitución sin aplicar demasiada fuerza. Cuando la unidad se inserta por completo, se oye un clic.

Cierre Tratar con cuidado. del soporte de unidades

Vuelva a instalar el bisel.

3. Vuelva a añadir la unidad al clúster mediante la interfaz de usuario de Element o el punto de extensión NetApp Element Management del plugin de Element para vCenter Server.

ix. Notifique al soporte de NetApp sobre el reemplazo de la unidad. El soporte de NetApp proporcionará instrucciones para la devolución de la unidad con error.



Al instalar una unidad nueva en un nodo existente, la unidad se registra automáticamente como **disponible** en la interfaz de usuario de Element. La unidad se debe añadir al clúster antes de que esta pueda participar en el clúster.

Opción	Pasos
Usar la interfaz de usuario de Element	<ol style="list-style-type: none"> En la interfaz de usuario de Element, seleccione Cluster > Drives. Seleccione Available para ver la lista de unidades disponibles. Seleccione el icono acciones de la unidad que desea agregar y seleccione Agregar.
Usar el plugin de Element para la interfaz de usuario de vCenter Server	<ol style="list-style-type: none"> En el punto de extensión NetApp Element Management de vSphere Web Client, seleccione Gestión de NetApp Element > clúster > unidades. En la lista desplegable disponible, seleccione la unidad y seleccione Agregar. Confirme la acción.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Sustituya los nodos H410C

Debe sustituir un nodo de computación en caso de que se produzca un fallo de CPU, otros problemas de la placa base o si no se enciende. Las instrucciones se aplican a los nodos H410C. Si tiene un nodo de computación H410C que ejecuta la versión 1.6P1 de Bootstrap OS de NetApp HCI o posterior, no tiene que sustituir el nodo si falla el DIMM de memoria; debe sustituir solo el DIMM con errores. Si los DIMM del nodo no han dado error, puede usarlos en el nodo de reemplazo.



El nodo de reemplazo debe tener la misma versión de NetApp HCI Bootstrap OS que el resto de los nodos de computación de la instalación de NetApp HCI.

NetApp recomienda el uso del motor de implementación de NetApp para añadir un nodo de computación de reemplazo. Si no puede continuar con la instalación del motor de puesta en marcha de NetApp para ESXi, consulte el artículo de la base de conocimientos de NetApp ["Cómo instalar ESXi en el nodo de computación NetApp HCI manualmente"](#).

Lo que necesitará

- Determinó que el nodo de computación debe sustituirse.
- Tiene un nodo de computación de reemplazo. Para solicitar un nodo de sustitución, debe comunicarse con el soporte de NetApp. El nodo de computación se le envía con el Bootstrap OS instalado. Los nodos se envían de fábrica con la última versión de Bootstrap OS. Es posible que necesite realizar el proceso de retorno a la imagen de fábrica (RTFI) en el nodo en las siguientes situaciones:
 - La instalación actual de NetApp HCI está ejecutando una versión de Bootstrap OS anterior a la última versión. En este caso, el proceso de RTFI degradará el nodo nuevo a la versión del SO que se está ejecutando la instalación de NetApp HCI.
 - El nodo de reemplazo enviado ejecuta una versión de bootstrap OS anterior a la última versión, y la instalación de NetApp HCI donde se va a reemplazar el nodo ya está ejecutando la última versión. En este caso, el proceso RTFI actualizará la versión del SO del nuevo nodo a la última. Consulte "[Cómo usar RTFI con una llave USB \(se requiere inicio de sesión\)](#)" y.. "[Cómo usar RTFI \(requiere inicio de sesión\)](#)".
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.
- Ha etiquetado cada cable conectado al nodo de computación.

Acerca de esta tarea

Las alarmas en VMware vSphere Web Client alertan de un nodo cuando se produce un fallo. Debe coincidir con el número de serie del nodo que ha fallado en VMware vSphere Web Client con el número de serie de la etiqueta adhesiva que aparece en la parte posterior del nodo.

Cuando se reemplaza un nodo de computación H410C, se debe tener en cuenta lo siguiente:

- Es posible combinar el nodo de computación H410C con los nodos existentes de computación y de almacenamiento de NetApp HCI en el mismo chasis y clúster.
- El nodo de computación H410C solo funciona con tensión de línea alta (200-240 V CA). Debe asegurarse de que se cumplan los requisitos de alimentación cuando añada nodos H410C a un sistema NetApp HCI existente.

Descripción general de los pasos

A continuación se ofrece una descripción general de los pasos de este procedimiento:

[Paso 1: Prepárese para reemplazar el nodo de computación](#)

[Paso 2: Reemplace el nodo de computación en el chasis](#)

[7 y versiones posteriores](#)

[Paso 4: Añada el nodo de computación al clúster](#)

[Paso 5: Vuelva a poner en marcha nodos testigos para clústeres de almacenamiento de dos y tres nodos](#)

A continuación se indican algunas tareas adicionales que puede que deba realizar si su sistema tiene las condiciones específicas a las que se aplican:

- ["Quite nodos de testigos para liberar recursos informáticos"](#)
- [Cambie la contraseña si ha recibido un nodo de repuesto con una contraseña BMC no estándar](#)
- [Actualice el firmware del BMC en el nodo](#)

Paso 1: Prepárese para reemplazar el nodo de computación

Debe migrar las máquinas virtuales (VM) alojadas en el nodo a un host disponible, y quitar el nodo con errores del clúster. Debería obtener detalles sobre el nodo con errores, como el número de serie y la información de red.

Pasos

1. En VMware vSphere Web Client, realice los pasos necesarios para migrar las máquinas virtuales a otro host disponible.



Consulte la documentación de VMware para conocer los pasos de migración.

2. Realice los pasos necesarios para quitar el nodo del inventario. Los pasos dependen de la versión de NetApp HCI en su instalación actual:

Número de versión de NetApp HCI	Pasos
NetApp HCI 1.3 y posteriores	<ol style="list-style-type: none">a. Seleccione el nodo que ha fallado y seleccione Monitor > Estado del hardware > Sensores.b. Tenga en cuenta el número de serie del nodo con errores. Esto le ayuda a identificar el nodo del chasis haciendo que coincida con el número de serie de la pegatina que hay en la parte posterior del nodo con el número de serie que ha indicado.c. Haga clic con el botón derecho del ratón en el nodo que ha fallado y seleccione Conexión > desconectar.d. Seleccione Sí para confirmar la acción.e. Haga clic con el botón derecho del ratón en el nodo con errores y seleccione Quitar del inventario.f. Seleccione Sí para confirmar la acción.
Versiones de NetApp HCI anteriores a 1.3	<ol style="list-style-type: none">a. Haga clic con el botón derecho del ratón en el nodo y seleccione Quitar del inventario.b. Seleccione el nodo que ha fallado y seleccione Monitor > Estado del hardware > Sensores.c. Tenga en cuenta el número de serie del nodo 0, que es el número de serie del nodo con errores. Esto le ayuda a identificar el nodo del chasis haciendo que coincida con el número de serie de la pegatina que hay en la parte posterior del nodo con el número de serie que ha indicado.d. Con el nodo que ha fallado seleccionado, seleccione Administrar > redes > adaptadores de VMkernel y copie las cuatro direcciones IP que aparecen en la lista. Esta información se puede reutilizar cuando se realizan los pasos de configuración de red inicial en VMware ESXi.

Paso 2: Reemplace el nodo de computación en el chasis

Después de quitar el nodo con errores del clúster, puede quitar el nodo del chasis e instalar el nodo de reemplazo.



Asegúrese de tener protección antiestática antes de realizar los pasos aquí.

Pasos

1. Póngase protección antiestática.
2. Desembale el nuevo nodo y configúrelo en una superficie nivelada cerca del chasis. Mantenga el material de empaque durante el momento en que devuelve el nodo de error a NetApp.
3. Etiquete cada cable que esté insertado en la parte posterior del nodo que desea quitar. Después de instalar el nodo nuevo, debe insertar los cables nuevamente en los puertos originales.
4. Desconecte todos los cables del nodo.
5. Si desea reutilizar los módulos DIMM, extráigalos.
6. Tire hacia abajo del asa de leva en el lado derecho del nodo y tire del nodo para sacarlo con las dos asas de leva. El asa de leva que debe tirar hacia abajo tiene una flecha sobre ella para indicar la dirección en la que se mueve. El otro controlador de leva no se mueve y está allí para ayudarle a sacar el nodo.



Dé soporte al nodo con las dos manos cuando lo tire del chasis.

7. Coloque el nodo en una superficie nivelada. Debe empaquetar el nodo y devolverlo a NetApp.
8. Instale el nodo de reemplazo.
9. Empuje el nodo hasta que oiga un clic.



Asegúrese de no utilizar una fuerza excesiva al deslizar el nodo en el chasis.



Asegúrese de que el nodo se encienda. Si no se enciende automáticamente, pulse el botón de alimentación situado en la parte frontal del nodo.

10. Si ha quitado DIMM del nodo con errores anteriormente, insértelos en el nodo de reemplazo.



Debe sustituir DIMM en las mismas ranuras desde las que se quitaron en el nodo con errores.

11. Vuelva a conectar los cables a los puertos desde los que se desconectaron originalmente. Las etiquetas que había conectado a los cables cuando los desconectó le ayudarán a guiar.



Si la apertura de flujo de aire de la parte trasera del chasis está bloqueada con cables o etiquetas, puede provocar fallos prematuros en los componentes debido al sobrecalentamiento. No fuerce los cables hacia los puertos, podría dañar los cables, los puertos o ambos.



Asegúrese de que el nodo de reemplazo esté cableado de la misma manera que los otros nodos del chasis.

Paso 3: Quite el activo de nodo de computación en NetApp HCI 1,7 y versiones posteriores

En NetApp HCI 1.7 y versiones posteriores, después de reemplazar físicamente el nodo, debe quitar el activo del nodo de computación mediante las API del nodo de gestión. Para utilizar API DE REST, su clúster de almacenamiento debe ejecutar el software NetApp Element 11.5 o una versión posterior y debe haber implementado un nodo de gestión que ejecute la versión 11.5 o posterior.

Pasos

1. Introduzca la dirección IP del nodo de gestión seguida de /mnode:
`https://[IP address]/mnode`
2. Seleccione **autorizar** o cualquier icono de bloqueo e introduzca las credenciales de administración del clúster para los permisos de uso de las API.
 - a. Introduzca el nombre de usuario y la contraseña del clúster.
 - b. Seleccione solicitar cuerpo en la lista desplegable Tipo si el valor no está seleccionado.
 - c. Introduzca el ID de cliente como mnode-client si el valor no está ya rellenado. No introduzca un valor para el secreto de cliente.
 - d. Seleccione **autorizar** para iniciar una sesión.



Si usted consigue el `Auth Error TypeError: Failed to fetch Mensaje de error` después de intentar autorizar, es posible que deba aceptar el certificado SSL para la MVIP del clúster. Copie la dirección IP en la URL de token, pegue la dirección IP en otra ficha del navegador y vuelva a autorizar. Si intenta ejecutar un comando después de que caduque el token, obtendrá un `Error: UNAUTHORIZED error`. Si recibe esta respuesta, vuelva a autorizar.

3. Cierre el cuadro de diálogo autorizaciones disponibles.
4. Seleccione **GET/assets**.
5. Seleccione **probar**.
6. Seleccione **Ejecutar**. Desplácese hacia abajo en el cuerpo de respuesta a la sección Compute y copie los valores primario e ID para el nodo de computación fallido.
7. Seleccione **DELETE/assets/{Asset_id}/Compute-Nodes/{Compute_id}**.
8. Seleccione **probar**. Introduzca los valores padre e id que obtuvo en el paso 7.
9. Seleccione **Ejecutar**.

Paso 4: Añada el nodo de computación al clúster

Debe volver a añadir el nodo de computación al clúster. Los pasos varían en función de la versión de NetApp HCI que esté ejecutando.

NetApp HCI 1.6P1 y posteriores

Puede utilizar el control del cloud híbrido de NetApp solo si se ejecuta su instalación de NetApp HCI en la versión 1.6P1 o posterior.

Lo que necesitará

- Compruebe que la instancia de vSphere que utiliza NetApp HCI tenga licencia vSphere Enterprise Plus si se va a ampliar una implementación con switches virtuales distribuidos.

- Compruebe que ninguna de las instancias de vCenter o vSphere que se utilizan con NetApp HCI tenga licencias caducadas.
- Asegúrese de tener direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (cada nodo nuevo debe instalarse en la misma red que los nodos existentes de su tipo).
- Compruebe que dispone de las credenciales de cuenta de administrador de vCenter preparadas.
- Asegúrese de que cada nodo nuevo utilice la misma topología y el mismo cableado de red que los clústeres de computación o almacenamiento existentes.
- "[Permite gestionar los iniciadores y los grupos de acceso de volúmenes](#)" para el nodo de computación nuevo.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. En el panel expandir instalación, seleccione **expandir**.
4. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

5. En la página de bienvenida, seleccione **Sí**.
6. En la página End User License, realice las siguientes acciones:
 - a. Lea el contrato de licencia para usuario final de VMware.
 - b. Si acepta los términos, seleccione **Acepto** al final del texto del acuerdo.
7. Seleccione **continuar**.
8. En la página vCenter, realice los pasos siguientes:
 - a. Introduzca un FQDN o una dirección IP y credenciales de administrador para la instancia de vCenter asociada con la instalación de NetApp HCI.
 - b. Seleccione **continuar**.
 - c. Seleccione un centro de datos de vSphere existente al que añadir el nodo de computación nuevo o seleccione **Crear nuevo centro de datos** para añadir los nodos de computación nuevos a un centro de datos nuevo.



Si selecciona Create New Datacenter, el campo Cluster se completa automáticamente.

- d. Si seleccionó un centro de datos existente, seleccione un clúster de vSphere con el que se deben asociar los nodos de computación nuevos.



Si NetApp HCI no puede reconocer la configuración de red del clúster seleccionado, asegúrese de que la asignación vmkernel y vmnic para las redes de gestión, almacenamiento y vMotion estén establecidos con los valores predeterminados de puesta en marcha.

e. Seleccione **continuar**.

9. En la página ESXi Credentials, introduzca una contraseña raíz ESXi para los nodos de computación que va a añadir. Debe usar la misma contraseña que se creó durante la implementación inicial de NetApp HCI.
10. Seleccione **continuar**.
11. Si creó un clúster de centro de datos de vSphere nuevo, en la página Network Topology, seleccione una topología de red para que coincida con los nodos de computación nuevos que se añaden.



Solo puede seleccionar la opción de dos cables si los nodos de computación utilizan la topología de dos cables y la implementación de NetApp HCI existente se configuró con identificadores de VLAN.

12. En la página Available Inventory, seleccione el nodo que desea añadir a la instalación de NetApp HCI existente.



Para algunos nodos de computación, es posible que deba habilitar EVC en el nivel más alto admitido por la versión de vCenter antes de añadirlos a la instalación. Debe utilizar el cliente de vSphere a fin de habilitar EVC para estos nodos de computación. Después de activarlo, actualice la página **Inventario** e intente agregar de nuevo los nodos de computación.

13. Seleccione **continuar**.
14. Opcional: Si creó un nuevo clúster de centro de datos de vSphere, en la página Network Settings, importe la información de la red desde una implementación de NetApp HCI existente seleccionando la casilla de comprobación **Copiar configuración desde un clúster existente**. Esto rellena la información de la pasarela y de la subred predeterminadas para cada red.
15. En la página Network Settings, se ha detectado parte de la información de red desde la implementación inicial. El nodo de computación nuevo se enumera por número de serie, y es necesario asignarle información de red nueva. Para el nodo de computación nuevo, realice los siguientes pasos:
 - a. Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo Detected Naming Prefix e insértelo como prefijo para el nuevo nombre de host único que añade en el campo **nombre de host**.
 - b. En el campo **Dirección IP de administración**, introduzca una dirección IP de administración para el nodo de computación que está en la subred de la red de administración.
 - c. En el campo vMotion IP Address, introduzca una dirección IP de vMotion para el nodo de computación que está en la subred de la red de vMotion.
 - d. En el campo iSCSI A - IP Address, introduzca una dirección IP para el primer puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.
 - e. En el campo iSCSI B - IP Address, introduzca una dirección IP para el segundo puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.
16. Seleccione **continuar**.
17. En la página Review de la sección Network Settings, el nodo nuevo se muestra en texto en negrita. Si necesita hacer cambios en la información de alguna sección, realice los pasos siguientes:
 - a. Seleccione **Editar** para esa sección.

- b. Cuando termine de hacer los cambios, haga clic en Continue en cualquiera de las páginas subsiguientes para regresar a la página Review.
18. Opcional: Si no desea enviar estadísticas del clúster ni información de soporte a los servidores SolidFire Active IQ alojados en NetApp, desactive la casilla de comprobación final. Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.
19. Seleccione **Agregar nodos**. Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.
20. Opcional: Verifique que el nodo de computación nuevo esté visible en vCenter.

NetApp HCI 1.4 P2, 1.4 y 1.3

Si la instalación de NetApp HCI ejecuta la versión 1.4P2, 1.4 o 1.3, puede usar el motor de implementación de NetApp para añadir el nodo al clúster.

Lo que necesitará

- Compruebe que la instancia de vSphere que utiliza NetApp HCI tenga licencia vSphere Enterprise Plus si se va a ampliar una implementación con switches virtuales distribuidos.
- Compruebe que ninguna de las instancias de vCenter o vSphere que se utilizan con NetApp HCI tenga licencias caducadas.
- Asegúrese de tener direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (cada nodo nuevo debe instalarse en la misma red que los nodos existentes de su tipo).
- Compruebe que dispone de las credenciales de cuenta de administrador de vCenter preparadas.
- Asegúrese de que cada nodo nuevo utilice la misma topología y el mismo cableado de red que los clústeres de computación o almacenamiento existentes.

Pasos

1. Vaya a la dirección IP de gestión de uno de los nodos de almacenamiento existentes:
http://<storage_node_management_IP_address>/
2. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

3. Seleccione **amplíe su instalación**.
4. En la página de bienvenida, seleccione **Sí**.
5. En la página End User License, realice las siguientes acciones:
 - a. Lea el contrato de licencia para usuario final de VMware.
 - b. Si acepta los términos, seleccione **Acepto** al final del texto del acuerdo.
6. Seleccione **continuar**.
7. En la página vCenter, realice los pasos siguientes:
 - a. Introduzca un FQDN o una dirección IP y credenciales de administrador para la instancia de vCenter asociada con la instalación de NetApp HCI.
 - b. Seleccione **continuar**.

- c. Seleccione un centro de datos de vSphere existente al cual añadir el nodo de computación nuevo.
- d. Seleccione un clúster de vSphere con el que se debe asociar el nodo de computación nuevo.



Debe habilitar EVC antes de continuar si va a añadir un nodo de computación con una generación de CPU que es diferente a la generación de CPU de los nodos de computación existentes, y la función Enhanced vMotion Compatibility (EVC) está deshabilitada en la instancia de vCenter de control. Esto garantiza que se complete la funcionalidad vMotion después de la ampliación.

- e. Seleccione **continuar**.
8. En la página ESXi Credentials, cree credenciales de administrador ESXi para el nodo de computación que va a añadir. Debe usar las mismas credenciales maestras que se crearon durante la implementación inicial de NetApp HCI.
9. Seleccione **continuar**.
10. En la página Available Inventory, seleccione el nodo que desea añadir a la instalación de NetApp HCI existente.



Para algunos nodos de computación, es posible que deba habilitar EVC en el nivel más alto admitido por la versión de vCenter antes de añadirlos a la instalación. Debe utilizar el cliente de vSphere a fin de habilitar EVC para estos nodos de computación. Después de habilitar dicha función, actualice la página Inventory e intente añadir nuevamente los nodos de computación.

11. Seleccione **continuar**.
12. En la página Network Settings, realice los pasos siguientes:
 - a. Compruebe la información detectada en la implementación inicial.
 - b. Cada nodo de computación nuevo se enumera por número de serie, y es necesario asignarle información de red nueva. Para cada nodo de almacenamiento nuevo, realice los siguientes pasos:
 - i. Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo Detected Naming Prefix e insértelo como prefijo para el nuevo nombre de host único que añade en el campo Hostname.
 - ii. En el campo Management IP Address, introduzca una dirección IP de gestión para el nodo de computación que está en la subred de la red de gestión.
 - iii. En el campo vMotion IP Address, introduzca una dirección IP de vMotion para el nodo de computación que está en la subred de la red de vMotion.
 - iv. En el campo iSCSI A - IP Address, introduzca una dirección IP para el primer puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.
 - v. En el campo iSCSI B - IP Address, introduzca una dirección IP para el segundo puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.
 - c. Seleccione **continuar**.
13. En la página Review de la sección Network Settings, el nodo nuevo se muestra en texto en negrita. Si desea hacer cambios en la información de alguna sección, realice los pasos siguientes:
 - a. Seleccione **Editar** para esa sección.
 - b. Cuando termine de hacer los cambios, seleccione **continuar** en cualquier página posterior para volver a la página Revisión.

14. Opcional: Si no desea enviar estadísticas del clúster ni información de soporte a los servidores Active IQ alojados en NetApp, desactive la casilla de comprobación final. Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.
15. Seleccione **Agregar nodos**. Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.
16. Opcional: Verifique que el nodo de computación nuevo esté visible en vCenter.

NetApp HCI 1.2, 1.1 y 1.0

Después de reemplazar físicamente el nodo, debería volver a añadirlo al clúster VMware ESXi y realizar varias configuraciones de red para poder usar todas las funcionalidades disponibles.



Debe tener una consola o teclado, vídeo y ratón (KVM) para realizar estos pasos.

Pasos

1. Instale y configure VMware ESXi versión 6.0.0 de la siguiente manera:
 - a. En la pantalla de la consola remota o KVM, seleccione **Control de alimentación > Configurar restablecimiento de energía**. Con esto se reinicia el nodo.
 - b. En la ventana Boot Menu (Menú de inicio) que se abre, seleccione **ESXi Install** (instalación de ESXi) pulsando la tecla flecha abajo.



Esta ventana permanece abierta sólo durante cinco segundos. Si no realiza la selección en cinco segundos, debe reiniciar el nodo de nuevo.

- c. Pulse **Intro** para iniciar el proceso de instalación.
 - d. Complete los pasos del asistente de instalación.



Cuando se le solicite seleccionar el disco en el que instalar ESXi, debe seleccionar la segunda unidad de disco de la lista seleccionando la tecla flecha abajo. Cuando se le solicite introducir una contraseña raíz, debe introducir la misma contraseña que configuró en el motor de implementación de NetApp al configurar NetApp HCI.

- e. Una vez finalizada la instalación, pulse **Intro** para reiniciar el nodo.



De forma predeterminada, el nodo se reinicia con el SO de inicio de NetApp HCI. Debe realizar una configuración única en el nodo para que utilice VMware ESXi.

2. Configure VMware ESXi en el nodo de la siguiente manera:
 - a. En la ventana de inicio de sesión de la interfaz de usuario del terminal (TUI) de Bootstrap OS de NetApp HCI, introduzca la siguiente información:
 - i. Nombre de usuario: Elemento
 - ii. Contraseña: ¡CcatTheFire!
 - b. Pulse la tecla flecha abajo para seleccionar **OK**.
 - c. Pulse **Intro** para iniciar sesión.
 - d. En el menú principal, utilice la tecla flecha abajo para seleccionar **túnel de soporte > túnel de**

soporte abierto.

e. En la ventana que aparece, introduzca la información del puerto.



Debe ponerse en contacto con el soporte de NetApp para obtener esta información. El soporte de NetApp inicia sesión en el nodo para establecer el archivo de configuración de arranque y completar la tarea de configuración.

f. Reinicie el nodo.

3. Configure la red de administración de la siguiente manera:

a. Inicie sesión en VMware ESXi. Para ello, introduzca las siguientes credenciales:

i. Nombre de usuario: Raíz

ii. Password: La contraseña que configuró al instalar VMware ESXi.



La contraseña debe coincidir con la configuración en el motor de implementación de NetApp al configurar NetApp HCI.

b. Seleccione **Configurar red de administración** y pulse **Intro**.

c. Seleccione **Adaptadores de red** y pulse **Intro**.

d. Seleccione **vmnic2** y **vmnic3**, y pulse **Enter**.

e. Seleccione **Configuración IPv4** y pulse la barra espaciadora en el teclado para seleccionar la opción de configuración estática.

f. Introduzca la dirección IP, la máscara de subred y la información de la puerta de enlace predeterminada y pulse **Intro**. Puede reutilizar la información que copió antes de quitar el nodo. La dirección IP que introdujo aquí es la dirección IP de red de gestión que copió anteriormente.

g. Pulse **Esc** para salir de la sección Configurar red de administración.

h. Seleccione **Sí** para aplicar los cambios.

4. Configure la red de modo que el nodo se sincronice con los otros nodos del clúster de la siguiente manera:

Plugin de Element para vCenter 5.0 y versiones posteriores

A partir del plugin de Element para vCenter 5,0, añada el nodo (host) al centro de datos.

- a. En VMware vSphere Web Client, seleccione **Inventario > Hosts and Clusters**.
- b. Haga clic con el botón derecho en el centro de datos y seleccione **Agregar host**.

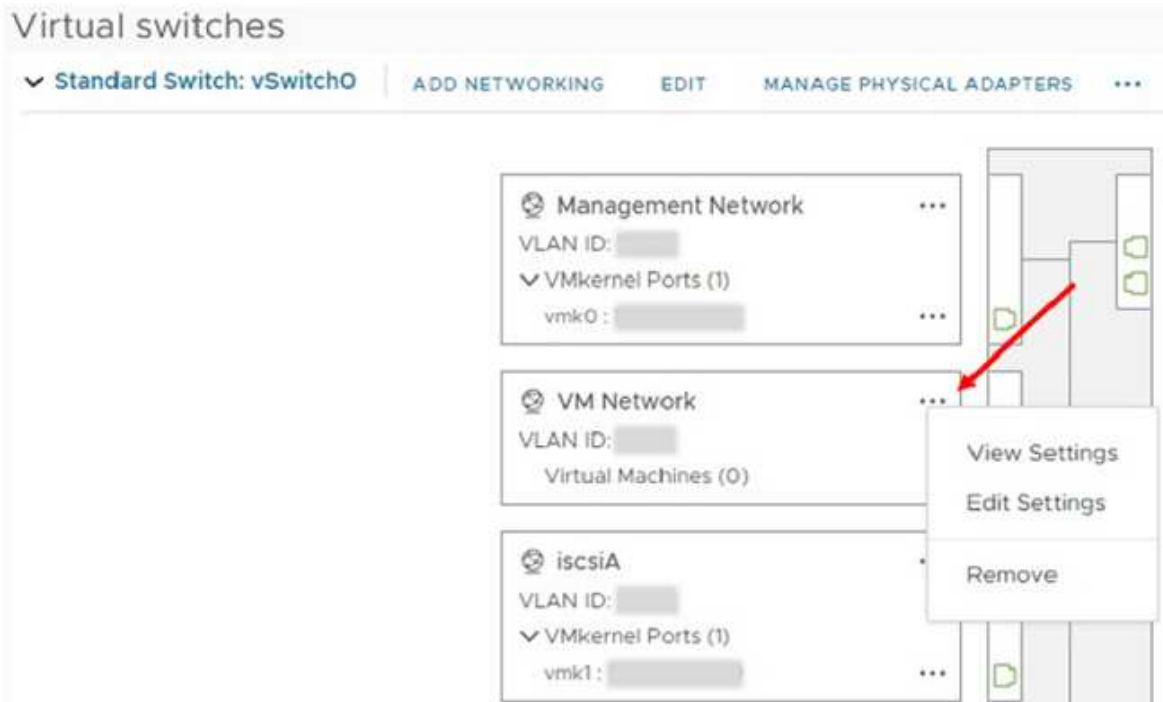
El asistente le guiará a través de la adición del host.



Cuando se le solicite introducir el nombre de usuario y la contraseña, utilice las siguientes credenciales: Nombre de usuario: Root Password: La contraseña que configuró en el motor de implementación de NetApp al configurar NetApp HCI

Es posible que el nodo tarde unos minutos en añadirse al clúster. Una vez completado el proceso, el nodo que se acaba de añadir se muestra en el clúster.

- c. Seleccione el nodo y, a continuación, seleccione **Configurar > Redes > Conmutadores virtuales** y realice los siguientes pasos:
 - i. Expandir **vSwitch0**.
 - ii. En el gráfico que se muestra, seleccione la red de VM ... Icono seguido de **Eliminar**.

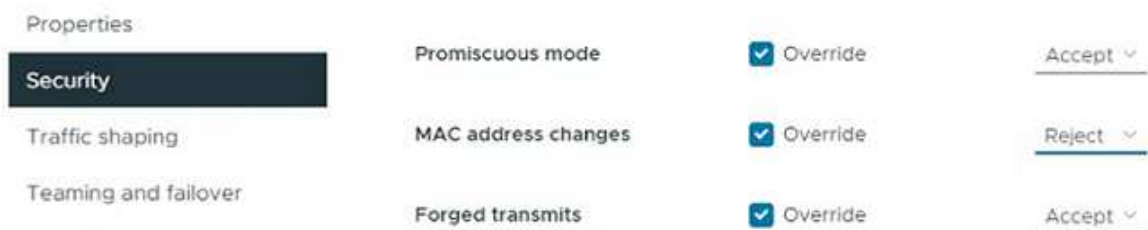


- iii. Confirme la acción.
 - iv. Seleccione **EDIT** en el encabezado vSwitch0.
 - v. En la ventana vSwitch0 - Editar configuración, seleccione **Teaming y failover**.
 - vi. Compruebe que vmnic3 aparece en Adaptadores en espera y seleccione **OK**.
- d. En el gráfico que se muestra, seleccione la red de administración ... Icono seguido de **Editar configuración**.

Virtual switches

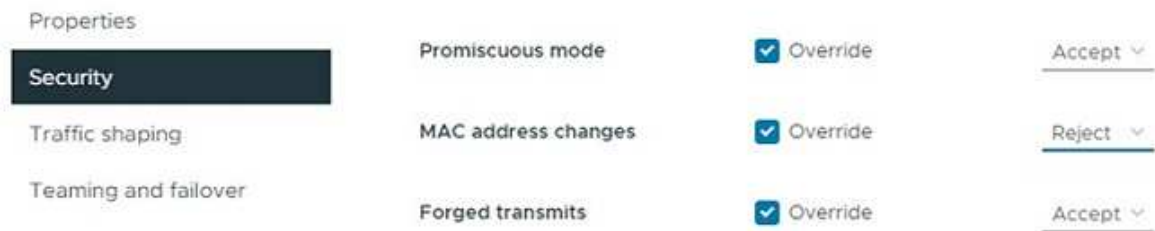


- i. En la ventana Management Network - Edit settings (Editar configuración), seleccione **Teaming y failover**.
 - ii. Compruebe que vmnic3 aparece en Adaptadores en espera y seleccione **OK**.
- e. Seleccione **Agregar red** en el encabezado vSwitch0 e introduzca los siguientes detalles en la ventana que se muestra:
- i. Para el tipo de conexión, seleccione **Grupo de puertos de máquina virtual para un conmutador estándar** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione **Nuevo interruptor estándar** y seleccione **Siguiente**.
 - iii. En Crear un conmutador estándar, mueva vmnic0 y vmnic4 a Adaptadores activos y seleccione **Siguiente**.
 - iv. En Configuración de conexión, compruebe que VM Network es la etiqueta de red y, si es necesario, introduzca el ID de VLAN.
 - v. Seleccione **Siguiente**.
 - vi. Revise la pantalla Listo para completar y seleccione **Finalizar**.
- f. Expanda vSwitch1 y seleccione **EDIT** para editar la configuración de la siguiente manera:
- i. En Propiedades, establezca MTU en 9000 y seleccione **Aceptar**.
- g. En el gráfico que se muestra, seleccione la red de VM ... Icono seguido de **Editar**.
- i. Seleccione **Seguridad** y realice las siguientes selecciones:

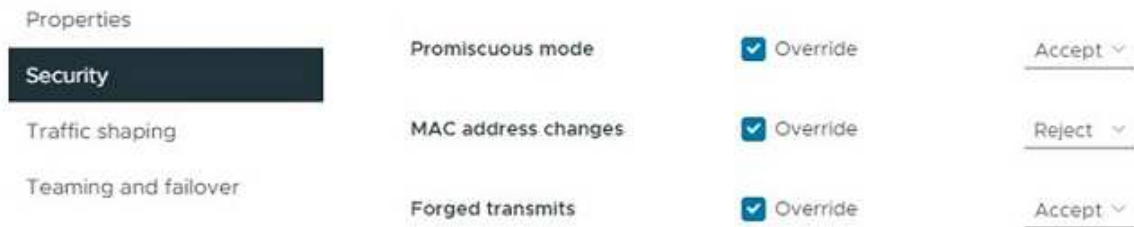


- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
- iii. Mueva vmnic0 a Adaptadores en espera.

- iv. Seleccione **OK**.
- h. Seleccione **ADD NETWORKING** en el encabezado vSwitch1 e introduzca los siguientes detalles en la ventana Add Networking:
 - i. Para el tipo de conexión, seleccione **adaptador de red de VMkernel** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione la opción de utilizar un conmutador estándar existente, vaya a vSwitch1 y seleccione **Siguiente**.
 - iii. En Crear un conmutador estándar, mueva vmnic1 y vmnic5 a Adaptadores activos y seleccione **Siguiente**.
 - iv. En Propiedades de puerto, cambie la etiqueta de red a vMotion, seleccione la casilla de verificación para el tráfico de vMotion en Habilitar servicios y seleccione **Siguiente**.
 - v. En Configuración de IPv4, proporcione la información de IPv4 y seleccione **Siguiente**.
 - vi. Si está listo para continuar, seleccione **Finalizar**.
- i. En el gráfico que se muestra, seleccione vMotion ... Icono seguido de **Editar**.
 - i. Seleccione **Seguridad** y realice las siguientes selecciones:



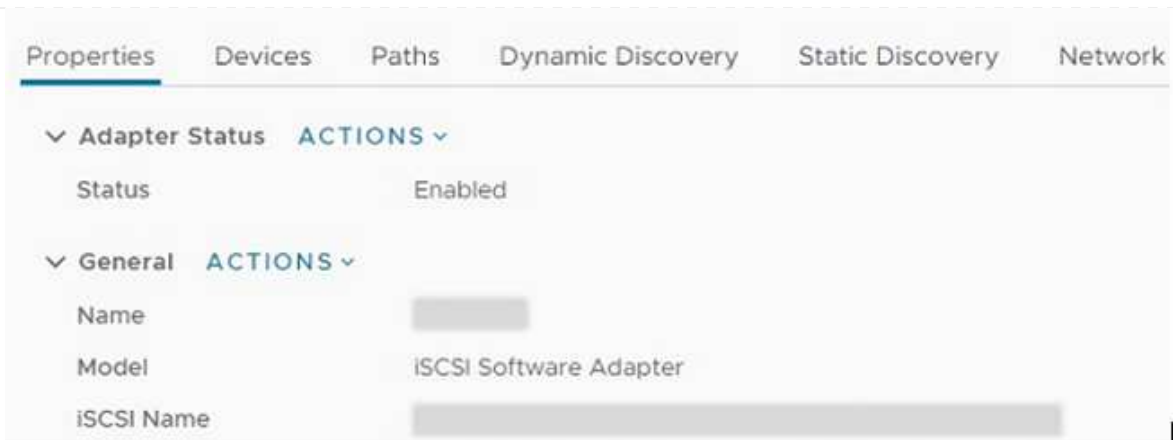
- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
- iii. Mueva vmnic4 a Adaptadores en espera.
- iv. Seleccione **OK**.
- j. Seleccione **ADD NETWORKING** en el encabezado vSwitch1 e introduzca los siguientes detalles en la ventana Add Networking:
 - i. Para el tipo de conexión, seleccione **adaptador de red de VMkernel** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione **Nuevo interruptor estándar** y seleccione **Siguiente**.
 - iii. En Crear un conmutador estándar, mueva vmnic1 y vmnic5 a Adaptadores activos y seleccione **Siguiente**.
 - iv. En Propiedades de puerto, cambie la etiqueta de red a iSCSI-B y seleccione **Siguiente**.
 - v. En Configuración de IPv4, proporcione la información de IPv4 y seleccione **Siguiente**.
 - vi. Si está listo para continuar, seleccione **Finalizar**.
- k. Expanda **vSwitch2** y seleccione **EDIT**:
 - i. En Propiedades, establezca MTU en 9000 y seleccione **Aceptar**.
- l. En el gráfico que se muestra, seleccione iSCSI-B. ... Icono seguido de **Editar**.
 - i. Seleccione **Seguridad** y realice las siguientes selecciones:



- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
 - iii. Mueva vmnic1 a adaptadores no utilizados.
 - iv. Seleccione **OK**.
- m. Seleccione **ADD NETWORKING** en el encabezado vSwitch1 e introduzca los siguientes detalles en la ventana Add Networking:
- i. Para el tipo de conexión, seleccione **adaptador de red de VMkernel** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione la opción de utilizar un conmutador estándar existente, vaya a vSwitch2 y seleccione **Siguiente**.
 - iii. En Propiedades de puerto, cambie la etiqueta de red a iSCSI-A y seleccione **Siguiente**.
 - iv. En Configuración de IPv4, proporcione la información de IPv4 y seleccione **Siguiente**.
 - v. Si está listo para continuar, seleccione **Finalizar**.
- n. En el gráfico que se muestra, seleccione iSCSI-A. ... Icono seguido de **Editar**.
- i. Seleccione **Seguridad** y realice las siguientes selecciones:



- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
 - iii. Mueva vmnic5 a los adaptadores no utilizados mediante el icono de flecha.
 - iv. Seleccione **OK**.
- o. Con el nodo recién agregado seleccionado y la pestaña Configurar abierta, seleccione **Almacenamiento > Adaptadores de almacenamiento** y realice los siguientes pasos:
- i. Seleccione la lista **ADD SOFTWARE ADAPTER**.
 - ii. Seleccione **Añadir adaptador iSCSI** y seleccione **OK**.
 - iii. En Adaptadores de almacenamiento, seleccione el adaptador iSCSI
 - iv. En Propiedades > General, copie el nombre iSCSI.



Necesita el nombre de iSCSI cuando se crea el iniciador.

- p. Realice los siguientes pasos en el complemento vCenter para SolidFire de NetApp:
- Seleccione la instancia de destino.
 - Seleccione **Gestión**.
 - Seleccione el clúster de destino.
 - Seleccione **Administración > Iniciadores**.
 - Seleccione **Crear iniciador**.
 - Introduzca la dirección de IQN que copió anteriormente en el campo IQN/WWPN.
 - Seleccione **OK**.
 - Seleccione el nuevo iniciador.
 - Seleccione **Lista de acciones > Acciones masivas** y seleccione **Agregar al grupo de acceso**.
 - Seleccione el grupo de acceso de destino y seleccione **Agregar**.
- q. En VMware vSphere Web Client, en Storage Adapters, seleccione el adaptador iSCSI y realice los pasos siguientes:
- Seleccione **Descubrimiento dinámico > Agregar**.
 - Introduzca la dirección IP de SVIP en el campo iSCSI Server.



Para obtener la dirección IP de SVIP, seleccione **Administración de NetApp Element** y copie la dirección IP de SVIP. Deje el número de puerto predeterminado tal cual. Debería ser 3260.

- Seleccione **OK**.
- Seleccione **Enlace de puerto de red** y seleccione **ADD**.
- Seleccione iSCSI-A e iSCSI-B y seleccione **OK**.
- Seleccione **RESCAN ADAPTADOR**.
- Seleccione **VOLVER A ESCANEAR ALMACENAMIENTO**. Busque nuevos volúmenes VMFS y seleccione **OK**.
- Una vez finalizada la repetición de la exploración, compruebe si los volúmenes del clúster y los almacenes de datos están visibles en el nuevo nodo de computación (host).

Plugin de Element para vCenter 4.10 y versiones anteriores

Para el plugin de Element para vCenter 4,10 y versiones anteriores, añada el nodo (host) al clúster.

- a. En VMware vSphere Web Client, seleccione **hosts and Clusters**.
- b. Haga clic con el botón derecho del ratón en el clúster al que desea agregar el nodo y seleccione **Agregar host**.

El asistente le guiará a través de la adición del host.

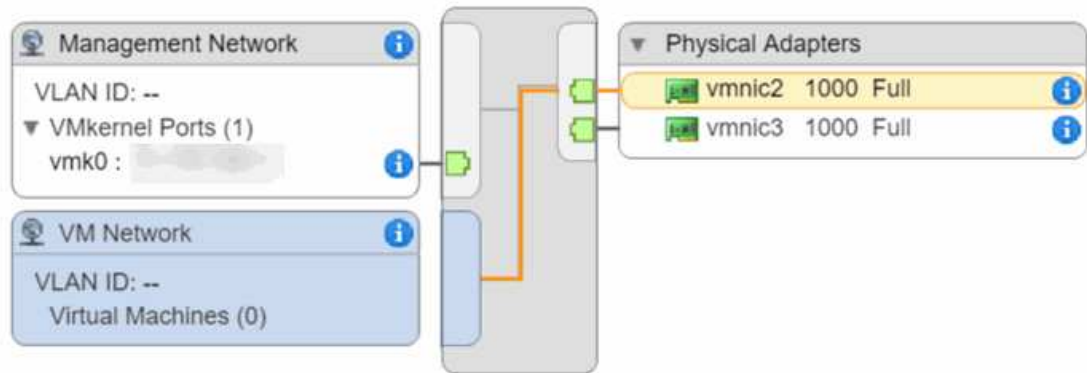


Cuando se le solicite introducir el nombre de usuario y la contraseña, utilice las siguientes credenciales: Nombre de usuario: Root Password: La contraseña que configuró en el motor de implementación de NetApp al configurar NetApp HCI

Es posible que el nodo tarde unos minutos en añadirse al clúster. Una vez completado el proceso, el nodo que se acaba de añadir se muestra en el clúster.

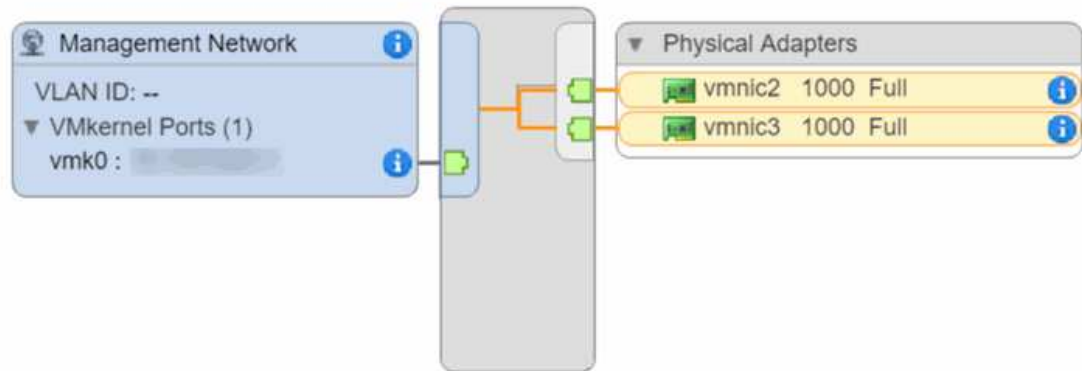
- c. Seleccione el nodo y, a continuación, seleccione **Administrar > redes > conmutadores virtuales** y realice los pasos siguientes:
 - i. Seleccione **vSwitch0**. Solo debe ver vSwitch0 que aparece en la tabla que se muestra.
 - ii. En el gráfico que se muestra, seleccione **VM Network** y haga clic en **X** para eliminar el grupo de puertos de red VM.

Standard switch: vSwitch0 (VM Network)



- iii. Confirme la acción.
- iv. Seleccione **vSwitch0** y, a continuación, seleccione el icono del lápiz para editar los ajustes.
- v. En la ventana vSwitch0 - Editar configuración, seleccione **Teaming y failover**.
- vi. Asegúrese de que vmnic3 aparece en Adaptadores en espera y seleccione **OK**.
- vii. En el gráfico que se muestra, seleccione **Red de administración** y seleccione el icono del lápiz para editar los ajustes.

Standard switch: vSwitch0 (Management Network)



- viii. En la ventana Management Network - Edit settings (Editar configuración), seleccione **Teaming y failover**.
- ix. Mueva vmnic3 a los adaptadores en espera mediante el icono de flecha y seleccione **OK**.
- d. En el menú desplegable acciones, seleccione **Agregar red** e introduzca los siguientes detalles en la ventana que aparece:
 - i. Para el tipo de conexión, seleccione **Grupo de puertos de máquina virtual para un conmutador estándar** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione la opción para añadir un nuevo conmutador estándar y seleccione **Siguiente**.
 - iii. Seleccione **+**.
 - iv. En la ventana Add Physical Adapters to Switch (Agregar adaptadores físicos a conmutador), seleccione vmnic0 y vmnic4 y seleccione **OK**. Vmnic0 y vmnic4 se enumeran ahora con adaptadores activos.
 - v. Seleccione **Siguiente**.
 - vi. En Configuración de conexión, compruebe que VM Network es la etiqueta de red y seleccione **Siguiente**.
 - vii. Si está listo para continuar, seleccione **Finalizar**. VSwitch1 se muestra en la lista de switches virtuales.
- e. Seleccione **vSwitch1** y seleccione el icono del lápiz para editar los ajustes de la siguiente manera:
 - i. En Propiedades, establezca MTU en 9000 y seleccione **Aceptar**. En el gráfico que se muestra, seleccione **VM Network** y haga clic en el icono del lápiz para editar los ajustes de la siguiente manera:
- f. Seleccione **Seguridad** y realice las siguientes selecciones:

Promiscuous mode:	<input checked="" type="checkbox"/> Override	Accept	▼
MAC address changes:	<input checked="" type="checkbox"/> Override	Reject	▼
Forged transmits:	<input checked="" type="checkbox"/> Override	Accept	▼

- i. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
 - ii. Mueva vmnic0 a los adaptadores en espera mediante el icono de flecha.
 - iii. Seleccione **OK**.
- g. Con vSwitch1 seleccionada, en el menú desplegable acciones, seleccione **Agregar red** e introduzca los siguientes detalles en la ventana que se muestra:
- i. Para el tipo de conexión, seleccione **adaptador de red de VMkernel** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione la opción de utilizar un conmutador estándar existente, vaya a vSwitch1 y seleccione **Siguiente**.
 - iii. En Propiedades de puerto, cambie la etiqueta de red a vMotion, seleccione la casilla de verificación para el tráfico de vMotion en Habilitar servicios y seleccione **Siguiente**.
 - iv. En Configuración de IPv4, proporcione la información de IPv4 y seleccione **Siguiente**. La dirección IP que introduzca aquí es la dirección IP de vMotion que copió anteriormente.
 - v. Si está listo para continuar, seleccione **Finalizar**.
- h. En el gráfico que se muestra, seleccione vMotion y seleccione el icono del lápiz para editar la configuración del siguiente modo:
- i. Seleccione **Seguridad** y realice las siguientes selecciones:

Promiscuous mode:	<input checked="" type="checkbox"/> Override	Accept	▼
MAC address changes:	<input checked="" type="checkbox"/> Override	Reject	▼
Forged transmits:	<input checked="" type="checkbox"/> Override	Accept	▼

- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
 - iii. Mueva vmnic4 a los adaptadores en espera mediante el icono de flecha.
 - iv. Seleccione **OK**.
- i. Con vSwitch1 seleccionada, en el menú desplegable acciones, seleccione **Agregar red** e introduzca los siguientes detalles en la ventana que se muestra:
- i. Para el tipo de conexión, seleccione **adaptador de red de VMkernel** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione la opción para añadir un nuevo conmutador estándar y seleccione **Siguiente**.
 - iii. Seleccione **+**.
 - iv. En la ventana Add Physical Adapters to Switch (Agregar adaptadores físicos a conmutador), seleccione vmnic1 y vmnic5 y seleccione **OK**. Vmnic1 y vmnic5 se enumeran ahora con

adaptadores activos.

- v. Seleccione **Siguiente**.
- vi. En Propiedades de puerto, cambie la etiqueta de red a iSCSI-B y seleccione **Siguiente**.
- vii. En Configuración de IPv4, proporcione la información de IPv4 y seleccione **Siguiente**. La dirección IP introducida aquí es la dirección IP de iSCSI-B que se copió anteriormente.
- viii. Si está listo para continuar, seleccione **Finalizar**. VSwitch2 se muestra en la lista de switches virtuales.
- j. Seleccione **vSwitch2** y seleccione el icono de lápiz para editar los ajustes de la siguiente manera:
 - i. En Propiedades, establezca MTU en 9000 y seleccione **Aceptar**.
- k. En el gráfico que se muestra, seleccione **iSCSI-B** y seleccione el icono del lápiz para editar los ajustes de la siguiente manera:
 - i. Seleccione **Seguridad** y realice las siguientes selecciones:

Promiscuous mode:	<input checked="" type="checkbox"/> Override	Accept	▼
MAC address changes:	<input checked="" type="checkbox"/> Override	Reject	▼
Forged transmits:	<input checked="" type="checkbox"/> Override	Accept	▼

- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
- iii. Mueva vmnic1 a los adaptadores no utilizados mediante el icono de flecha.
- iv. Seleccione **OK**.
- l. En el menú desplegable acciones, seleccione **Agregar red** e introduzca los siguientes detalles en la ventana que aparece:
 - i. Para el tipo de conexión, seleccione **adaptador de red de VMkernel** y seleccione **Siguiente**.
 - ii. Para el dispositivo de destino, seleccione la opción de utilizar un conmutador estándar existente, vaya a vSwitch2 y seleccione **Siguiente**.
 - iii. En Propiedades de puerto, cambie la etiqueta de red a iSCSI-A y seleccione **Siguiente**.
 - iv. En Configuración de IPv4, proporcione la información de IPv4 y seleccione **Siguiente**. La dirección IP introducida aquí es la dirección IP de iSCSI-A que se copió anteriormente.
 - v. Si está listo para continuar, seleccione **Finalizar**.
- m. En el gráfico que se muestra, seleccione **iSCSI-A** y seleccione el icono del lápiz para editar los ajustes de la siguiente manera:
 - i. Seleccione **Seguridad** y realice las siguientes selecciones:

Promiscuous mode:	<input checked="" type="checkbox"/> Override	Accept	▼
MAC address changes:	<input checked="" type="checkbox"/> Override	Reject	▼
Forged transmits:	<input checked="" type="checkbox"/> Override	Accept	▼

- ii. Seleccione **Teaming y failover** y seleccione la casilla de verificación **Override**.
 - iii. Mueva vmnic5 a los adaptadores no utilizados mediante el icono de flecha.
 - iv. Seleccione **OK**.
- n. Con el nuevo nodo agregado seleccionado y la ficha gestionar abierta, seleccione **almacenamiento > Adaptadores de almacenamiento** y realice los siguientes pasos:
- i. Seleccione **+** y seleccione **Software iSCSI Adapter**.
 - ii. Para agregar el adaptador iSCSI, seleccione **Aceptar** en el cuadro de diálogo.
 - iii. En Adaptadores de almacenamiento, seleccione el adaptador iSCSI y, en la ficha Propiedades, copie el nombre iSCSI.

Properties	Devices	Paths	Targets	Network Port Binding	Advanced Options
Status	Enabled				
General					
Name	vmhba40				
Model	iSCSI Software Adapter				
iSCSI Name	[REDACTED]				
iSCSI Alias					



Necesita el nombre de iSCSI cuando se crea el iniciador.

- o. Realice los siguientes pasos en el complemento vCenter para SolidFire de NetApp:
 - i. Seleccione **Gestión > iniciadores > Crear**.
 - ii. Seleccione **Crear un único iniciador**.
 - iii. Introduzca la dirección de IQN que copió anteriormente en el campo IQN/WWPN.
 - iv. Seleccione **OK**.
 - v. Seleccione **acciones masivas** y seleccione **Agregar a grupo de acceso de volumen**.
 - vi. Seleccione **NetApp HCI** y seleccione **Agregar**.
- p. En VMware vSphere Web Client, en Storage Adapters, seleccione el adaptador iSCSI y realice los pasos siguientes:
 - i. En Detalles del adaptador, seleccione **objetivos > descubrimiento dinámico > Agregar**.
 - ii. Introduzca la dirección IP de SVIP en el campo iSCSI Server.



Para obtener la dirección IP de SVIP, seleccione **Administración de NetApp Element** y copie la dirección IP de SVIP. Deje el número de puerto predeterminado tal cual. Debería ser 3260.

- iii. Seleccione **OK**. Se muestra un mensaje que recomienda volver a analizar el adaptador de almacenamiento.
- iv. Seleccione el icono de reexploración.



- v. En Detalles del adaptador, seleccione **enlace del puerto de red** y seleccione **+**.
- vi. Active las casillas de verificación de iSCSI-B e iSCSI-A y haga clic en OK. Se muestra un mensaje que recomienda volver a analizar el adaptador de almacenamiento.
- vii. Seleccione el icono de reexploración. Una vez que haya finalizado la detección, verifique si los volúmenes del clúster están visibles en el nodo de computación nuevo (host).

Paso 5: Vuelva a poner en marcha nodos testigos para clústeres de almacenamiento de dos y tres nodos

Después de reemplazar físicamente el nodo de computación con fallos, debe volver a poner en marcha la máquina virtual del nodo de testimonio de NetApp HCI si el nodo de computación con errores alojaba el nodo de testigo. Estas instrucciones solo se aplican a nodos de computación que forman parte de una instalación de NetApp HCI con clústeres de almacenamiento de dos o tres nodos.

Lo que necesitará

- Recopile la siguiente información:
 - El nombre del clúster del clúster de almacenamiento
 - La máscara de subred, la dirección IP de puerta de enlace, el servidor DNS y la información de dominio para la red de gestión
 - Máscara de subred para la red de almacenamiento
- Compruebe que tenga acceso al clúster de almacenamiento para poder añadir los nodos de testigo al clúster.
- Considere las siguientes condiciones para ayudar a decidir si se debe eliminar el nodo de testigo existente de VMware vSphere Web Client o el clúster de almacenamiento:
 - Si desea utilizar el mismo nombre de máquina virtual para el nuevo nodo de prueba, debe eliminar todas las referencias al nodo de prueba antiguo de vSphere.
 - Si desea utilizar el mismo nombre de host en el nuevo nodo de testigo, primero debe eliminar el nodo de testigo antiguo del clúster de almacenamiento.

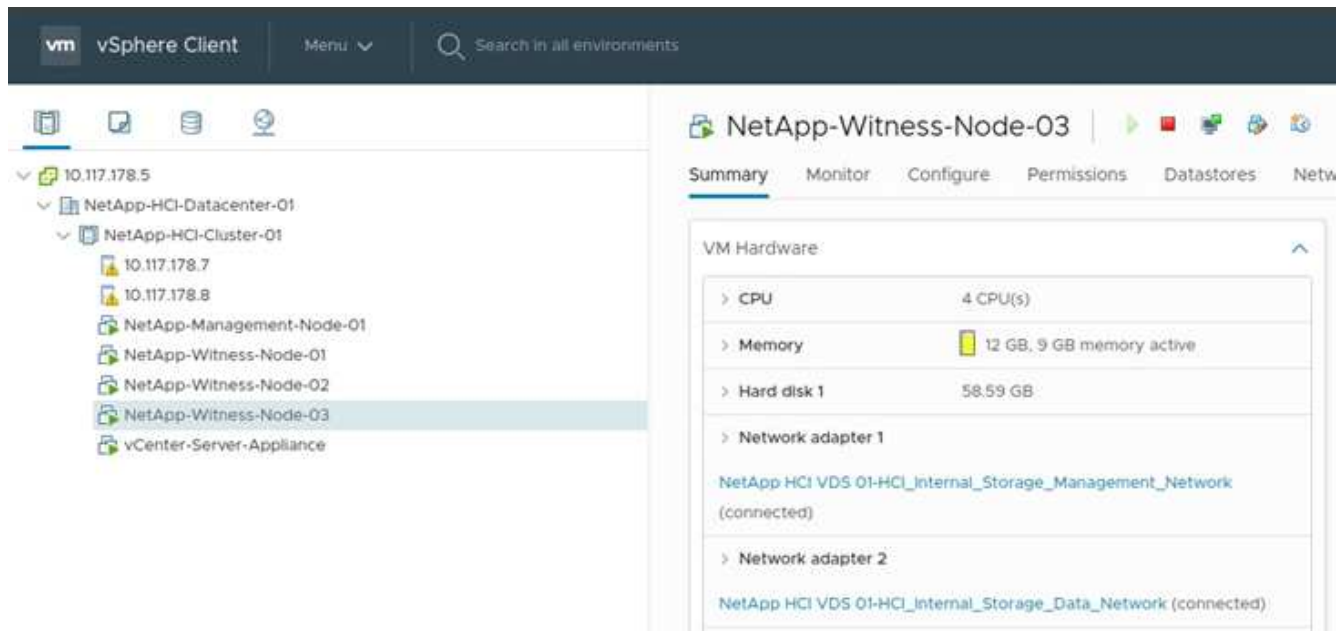


No puede quitar el nodo testigo antiguo si el clúster está inactivo en solo dos nodos de almacenamiento físico (y no hay nodos de testigo). En esta situación, primero debe agregar el nuevo nodo testigo al clúster antes de eliminar el antiguo. Puede quitar el nodo de testigo del clúster mediante el punto de extensión NetApp Element Management.

¿Cuándo debe volver a poner en marcha los nodos de los testigos?

Debe volver a poner en marcha nodos de testigos en las siguientes situaciones:

- Se reemplazó un nodo de computación con errores que forma parte de una instalación de NetApp HCI, que tiene un clúster de almacenamiento de dos o tres nodos y el nodo de computación con errores alojaba una máquina virtual de nodos testigos.
- Ha realizado el procedimiento de retorno a la imagen de fábrica (RTFI) en el nodo de computación.
- La máquina virtual del nodo de testigo está dañada.
- La máquina virtual del nodo de testigo se ha quitado accidentalmente de ESXi. El equipo virtual se configura usando la plantilla que se crea como parte de la puesta en marcha inicial con el motor de puesta en marcha de NetApp. Este es un ejemplo del aspecto que tiene una VM de nodo de prueba:



Si ha eliminado la plantilla de máquina virtual, debe ponerse en contacto con el soporte de NetApp para obtener la imagen de nodo de testigo .ova y volver a ponerlas en marcha. Puede descargar la plantilla en "[aquí \(se requiere inicio de sesión\)](#)". No obstante, debe solicitar ayuda al equipo de soporte para recibir asesoramiento sobre la configuración.

Pasos

1. En VMware vSphere Web Client, seleccione **hosts and Clusters**.
2. Haga clic con el botón derecho del ratón en el nodo de computación que alojará la VM de Witness Node y seleccione **Nueva máquina virtual**.
3. Seleccione **desplegar desde plantilla** y seleccione **Siguiente**.
4. Siga los pasos del asistente:

- a. Seleccione **Data Center**, localice la plantilla de VM y seleccione **Siguiente**.
- b. Escriba un nombre para la máquina virtual con el siguiente formato: NetApp-Witness-Node-##



debe ser reemplazado por un número.

- c. Deje la selección predeterminada para la ubicación de la VM tal cual y seleccione **Siguiente**.
 - d. Deje la selección predeterminada para el recurso de computación de destino tal y como está, y seleccione **Siguiente**.
 - e. Seleccione el almacén de datos local y seleccione **Siguiente**. El espacio libre en el almacén de datos local varía según la plataforma de computación.
 - f. Seleccione **encendido de la máquina virtual tras la creación** en la lista de opciones de implementación y seleccione **Siguiente**.
 - g. Revise las selecciones y seleccione **Finalizar**.
5. Configure la red de gestión y almacenamiento y la configuración del clúster para el nodo de observación de la siguiente manera:
- a. En VMware vSphere Web Client, seleccione **hosts and Clusters**.
 - b. Haga clic con el botón derecho del ratón en el nodo testigo y encírelo si aún no está encendido.
 - c. En la vista Resumen del nodo testigo, seleccione **Iniciar Web Console**.
 - d. Espere a que el nodo testigo arranque hasta el menú con el fondo azul.
 - e. Seleccione cualquier lugar dentro de la consola para acceder al menú.
 - f. Configure la red de administración de la siguiente manera:
 - i. Pulse la tecla de flecha hacia abajo para desplazarse a Red y, a continuación, pulse **Intro** para aceptar.
 - ii. Desplácese hasta **Configuración de red** y pulse **Intro** para aceptar.
 - iii. Desplácese hasta **net0** y pulse **Intro** para aceptar.
 - iv. Pulse **Tab** hasta llegar al campo IPv4 y, si procede, elimine la IP existente en el campo e introduzca la información IP de administración para el nodo testigo. Compruebe también la máscara de subred y la puerta de enlace.



No se aplicará ningún etiquetado de VLAN en el nivel de host de VM; el etiquetado se gestionará en vSwitch.

- v. Pulse **Tab** para desplazarse a OK y pulse **Enter** para guardar los cambios. Tras la configuración de la red de gestión, la pantalla vuelve a la red.
- g. Configure la red de almacenamiento de la siguiente manera:
- i. Pulse la tecla de flecha hacia abajo para desplazarse a Red y, a continuación, pulse **Intro** para aceptar.
 - ii. Desplácese hasta **Configuración de red** y pulse **Intro** para aceptar.
 - iii. Desplácese hasta **net1** y, a continuación, pulse **Intro** para aceptar.
 - iv. Pulse **Tab** hasta llegar al campo IPv4 y, si procede, elimine la IP existente en el campo e introduzca la información IP de almacenamiento para el nodo testigo.
 - v. Pulse **Tab** para desplazarse a OK y pulse **Enter** para guardar los cambios.

vi. Establezca MTU en 9000.



Si no se establece MTU antes de agregar el nodo de testimonio al clúster, puede ver advertencias del clúster para ver una configuración de MTU inconsistente. Esto puede evitar que se ejecute la recopilación de basura y causar problemas de rendimiento.

vii. Pulse **Tab** para desplazarse a OK y pulse **Enter** para guardar los cambios. Después de la configuración de la red de almacenamiento, la pantalla vuelve a la red.

h. Configure las opciones del clúster de la siguiente manera:

i. Pulse **Tab** para ir a Cancelar y pulse **Intro**.

ii. Vaya a **Configuración del clúster** y, a continuación, pulse **Intro** para aceptar.

iii. Pulse **Tab** para desplazarse hasta Cambiar configuración y pulse **Enter** para Cambiar configuración.

iv. Pulse **TAB** para desplazarse al campo Nombre de host e introduzca el nombre de host.

v. Pulse la tecla de flecha hacia abajo para acceder al campo Cluster e introduzca el nombre del clúster en el clúster de almacenamiento.

vi. Pulse la tecla **Tab** para desplazarse hasta el botón OK y pulse **Intro**.

6. Añada el nodo de testigo al clúster de almacenamiento de la siguiente manera:

a. Desde vSphere Web Client, acceda al punto de extensión NetApp Element Management desde la pestaña **Accesos directos** o el panel lateral.

b. Seleccione **Administración de NetApp Element > clúster**.

c. Seleccione la subpestaña **Nodes**.

d. Seleccione **pendiente** en la lista desplegable para ver la lista de nodos. El nodo testigo debe aparecer en la lista nodos pendientes.

e. Seleccione la casilla de verificación del nodo que desea agregar y seleccione **Agregar nodo**. Una vez completada la acción, el nodo aparecerá en la lista de nodos activos del clúster.

Cambie la contraseña si ha recibido un nodo de repuesto con una contraseña BMC no estándar

Algunos nodos de repuesto pueden enviarse con contraseñas no estándar para la IU del controlador de gestión en placa base (BMC). Si recibe un nodo de sustitución con una contraseña BMC no estándar, debe cambiar la contraseña a la predeterminada, ADMIN.

Pasos

1. Identifique si ha recibido un nodo de sustitución con una contraseña no estándar de BMC:

a. Busque una etiqueta en el puerto IPMI en la parte posterior del nodo de reemplazo que recibió. Si encuentra una pegatina situada en el puerto IPMI, significa que ha recibido un nodo con una contraseña BMC no estándar. Consulte la siguiente imagen de ejemplo:



- b. Anote la contraseña.
2. Inicie sesión en la interfaz de usuario del BMC utilizando la contraseña única que se encuentra en la pegatina.
3. Seleccione **valor predeterminado de fábrica**, seleccione el botón de opción **Eliminar ajustes actuales y configure los valores predeterminados del usuario EN ADMIN/ADMIN**:
4. Seleccione **Restaurar**.
5. Cierre sesión y, a continuación, vuelva a iniciar sesión para confirmar que las credenciales se han modificado.

Actualice el firmware del BMC en el nodo

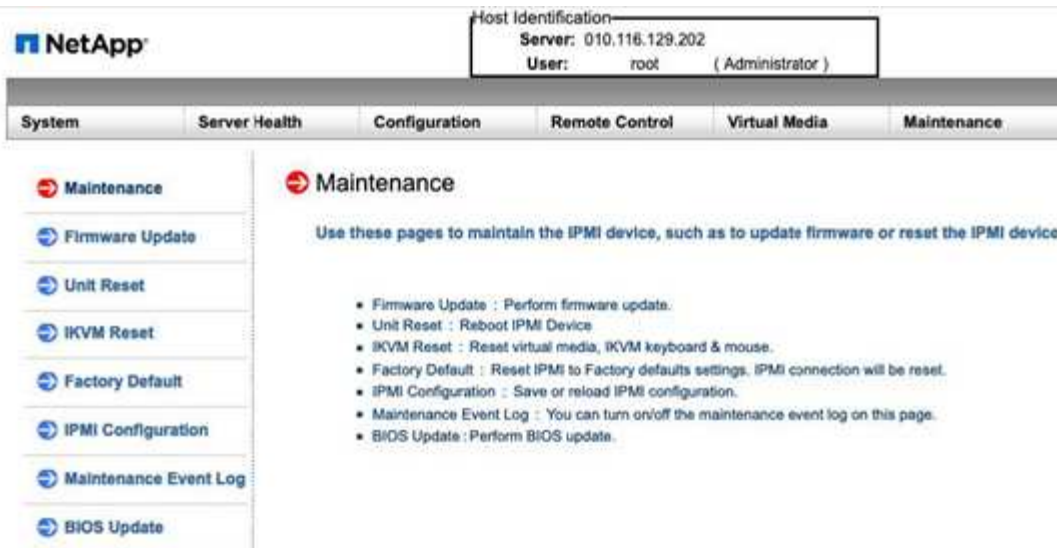
Después de sustituir el nodo de computación, es posible que tenga que actualizar la versión de firmware. Puede descargar el archivo de firmware más reciente en el menú desplegable del "[Sitio de soporte de NetApp](#) (se requiere inicio de sesión)".

Pasos

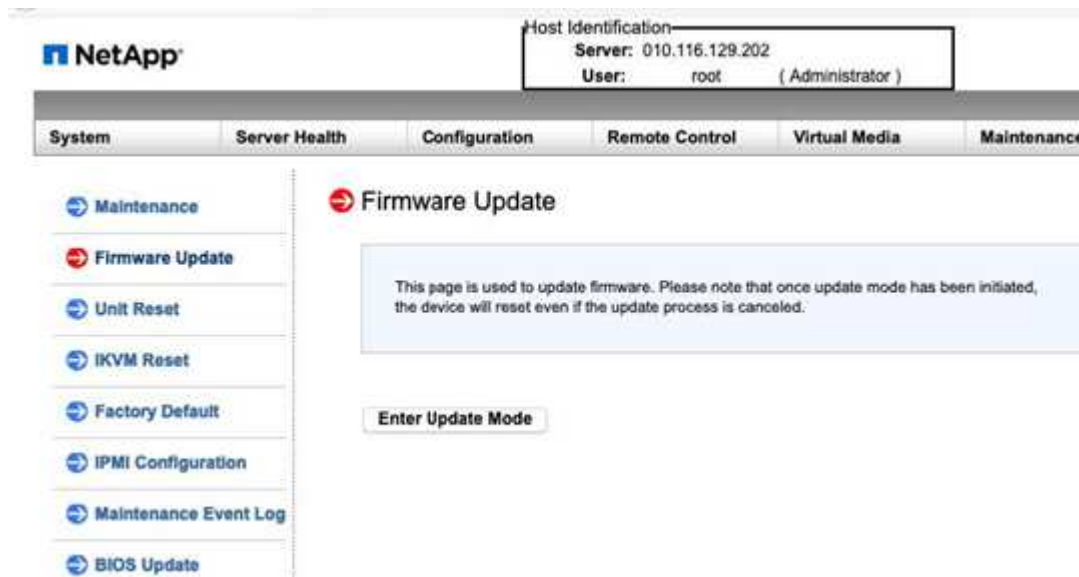
1. Inicie sesión en la interfaz de usuario del controlador de administración de la placa base (BMC).
2. Seleccione **Mantenimiento > actualización del firmware**.

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help
System	FRU Reading	Hardware Information	System	Firmware Revision : 03.25 Firmware Build Time : 06/12/2017 BIOS Version : NA2.1 BIOS Build Time : 07/10/2017 Redfish Version : 1.0.1 CPLD Version : 01.a1.06	IP address : 010.063.104.248 BMC MAC address : 0c:c4:7a:29:c1:d0 System LAN1 MAC address : 0c:c4:7a:f3:00:00:00:00 System LAN2 MAC address : 0c:c4:7a:f3:00:00:00:00 System LAN3 MAC address : 0c:c4:7a:d6:67:eb System LAN4 MAC address : 0c:c4:7a:d6:67:eb	Firmware Update Unit Reset iKVM Reset Factory Default IPMI Configuration System Event Log BIOS Update System Crash Dump	

3. Desde la consola del BMC, seleccione **Mantenimiento**.



4. En la ficha Mantenimiento, seleccione **actualización del firmware** en la navegación de la izquierda de la interfaz de usuario y seleccione **Entrar en modo de actualización**.



5. Seleccione **Sí** en el cuadro de diálogo de confirmación.
6. Seleccione **examinar** para seleccionar la imagen del firmware que desea cargar y seleccione **cargar firmware**. Cargar firmware desde una ubicación fuera de las proximidades directas del nodo puede provocar largos tiempos de carga y posibles tiempos de espera.
7. Permita las comprobaciones de configuración Preserve y seleccione **Iniciar actualización**. La actualización debería tardar aproximadamente 5 minutos. Si el tiempo de carga supera los 60 minutos, cancele la carga y transfiera el archivo a una máquina local cerca del nodo. Si se agota el tiempo de espera de la sesión, es posible que vea una serie de alertas al intentar volver a iniciar sesión en el área de actualización del firmware de la interfaz de usuario de BMC. Si cancela la actualización, se le redirigirá a la página de inicio de sesión.
8. Una vez finalizada la actualización, seleccione **Aceptar** y espere a que se reinicie el nodo. Inicie sesión después de la actualización y seleccione **sistema** para comprobar que la versión de **Revisión de firmware** coincide con la versión que ha cargado.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Sustituya los nodos H410S

Debe sustituir un nodo de almacenamiento en caso de que falle el módulo de memoria en línea doble (DIMM), un fallo de la CPU, problemas de la tarjeta Radian, otros problemas de la placa base o si no se enciende. Las alarmas en VMware vSphere Web Client le alertan de un nodo de almacenamiento falla. Debe usar la interfaz de usuario del software NetApp Element para obtener el número de serie (etiqueta de servicio) del nodo con errores. Necesita esta información para localizar el nodo con errores en el chasis.

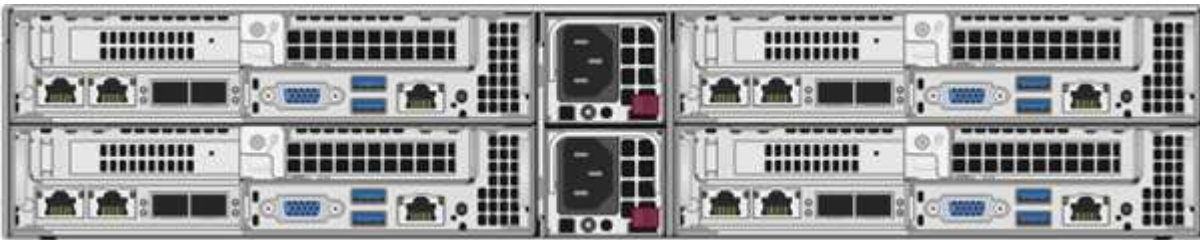
Lo que necesitará

- Determinó que el nodo de almacenamiento debe sustituirse.
- Tiene un nodo de almacenamiento de reemplazo.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.
- Ha etiquetado cada cable conectado al nodo de almacenamiento.

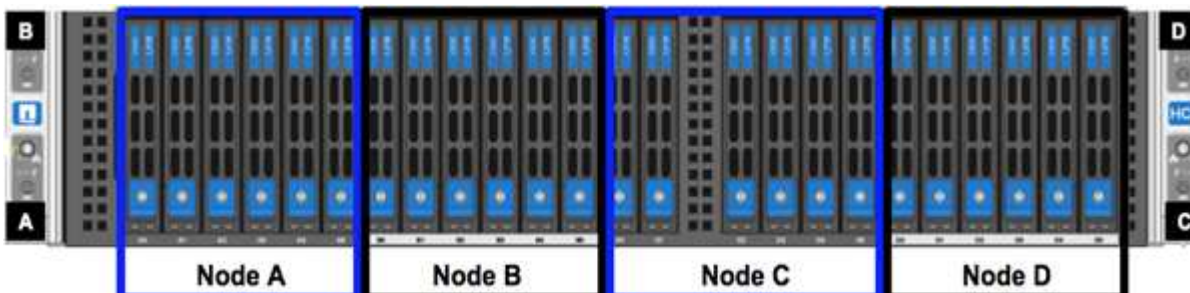
Acerca de esta tarea

El procedimiento de reemplazo se aplica a los nodos de almacenamiento H410S en un chasis NetApp HCI de cuatro nodos y unidad rack doble (2U).

A continuación, se muestra la vista trasera de un chasis de cuatro nodos con nodos H410S:



A continuación, se muestra la vista frontal de un chasis de cuatro nodos con nodos H410S, mostrando las bahías que corresponden a cada nodo:



Descripción general de los pasos

A continuación se ofrece una descripción general de los pasos de este procedimiento:[Prepare para sustituir el nodo de almacenamiento](#)

[Sustituya el nodo de almacenamiento en el chasis](#)

[Añada el nodo de almacenamiento al clúster](#)

Prepare para sustituir el nodo de almacenamiento

Debe quitar correctamente el nodo de almacenamiento defectuoso del clúster antes de instalar el nodo de reemplazo. Puede hacer esto sin causar ninguna interrupción del servicio. Debe obtener el número de serie del nodo de almacenamiento con errores en la interfaz de usuario de Element y vincularlo con el número de serie de la etiqueta en la parte posterior del nodo.



En el caso de fallos de componentes donde el nodo sigue conectado y funcionando, por ejemplo, un fallo de un módulo de memoria en línea doble (DIMM), debe quitar las unidades del clúster antes de quitar el nodo con errores.

Pasos

1. Si tiene un error de DIMM, quite las unidades asociadas al nodo que va a reemplazar del clúster. Es posible usar la interfaz de usuario del software NetApp Element o el punto de extensión NetApp Element Management del plugin de Element para vCenter Server antes de quitar el nodo.
2. Quite los nodos mediante la interfaz de usuario del software NetApp Element o el punto de extensión NetApp Element Management del plugin de Element para vCenter Server:

Opción	Pasos
Usar la interfaz de usuario de Element	<ol style="list-style-type: none">a. En la interfaz de usuario de Element, seleccione Cluster > Nodes.b. Tenga en cuenta el número de serie (etiqueta de servicio) del nodo defectuoso. Necesita esta información para coincidir con el número de serie de la pegatina situada en la parte posterior del nodo.c. Después de anotar el número de serie, quite el nodo del clúster del siguiente modo:d. Seleccione acciones para el nodo que desea quitar.e. Seleccione Quitar. <p>Ahora puede quitar físicamente el nodo del chasis.</p>

Opción	Pasos
Usar el plugin de Element para la interfaz de usuario de vCenter Server	<ol style="list-style-type: none"> En el punto de extensión NetApp Element Management de vSphere Web Client, seleccione Gestión de NetApp Element > clúster. Seleccione la subpestaña Nodes. En la vista Active, seleccione la casilla de verificación de cada nodo que desee quitar y seleccione acciones > Quitar. Confirme la acción. Los nodos que se quitan de un clúster se muestran en la lista de nodos pendientes Pending.

Sustituya el nodo de almacenamiento en el chasis

Debe instalar el nodo de repuesto en la misma ranura del chasis desde el que quita el nodo con errores. Debe usar el número de serie que anotó en la interfaz de usuario y vincularlo con el número de serie de la parte posterior del nodo.



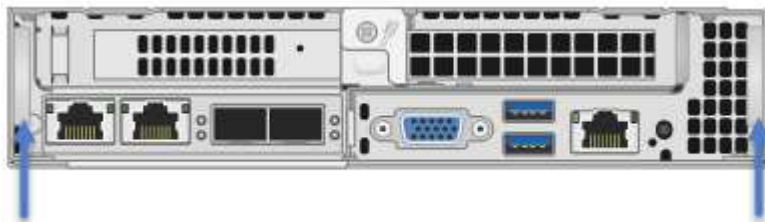
Asegúrese de tener protección antiestática antes de realizar los pasos aquí.

Pasos

- Desembale el nuevo nodo de almacenamiento y configúrelo en una superficie plana cerca del chasis. Mantenga el material de empaque durante el momento en que devuelve el nodo de error a NetApp.
- Etiquete cada cable que esté insertado en la parte posterior del nodo de almacenamiento que desea quitar. Después de instalar el nodo de almacenamiento nuevo, debe insertar los cables en los puertos originales.
- Desconecte todos los cables del nodo de almacenamiento.
- Tire hacia abajo del asa de leva en el lado derecho del nodo y tire del nodo para sacarlo con las dos asas de leva. El asa de leva que debe tirar hacia abajo tiene una flecha sobre ella para indicar la dirección en la que se mueve. El otro controlador de leva no se mueve y está allí para ayudarle a sacar el nodo.



Dé soporte al nodo con las dos manos cuando lo tire del chasis.



- Coloque el nodo en una superficie nivelada.
- Instale el nodo de reemplazo.
- Empuje el nodo hasta que oiga un clic.



Asegúrese de no utilizar una fuerza excesiva al deslizar el nodo en el chasis.

8. Vuelva a conectar los cables a los puertos desde los que se desconectaron originalmente. Las etiquetas que había conectado a los cables cuando los desconectó le ayudarán a guiar.



Si la apertura de flujo de aire de la parte trasera del chasis está bloqueada con cables o etiquetas, puede provocar fallos prematuros en los componentes debido al sobrecalentamiento. No fuerce los cables hacia los puertos, podría dañar los cables, los puertos o ambos.



Asegúrese de que el nodo de reemplazo esté cableado de la misma manera que los otros nodos del chasis.

9. Pulse el botón situado en la parte frontal del nodo para encender el nodo.

Añada el nodo de almacenamiento al clúster

Debe volver a añadir el nodo de almacenamiento al clúster. Los pasos varían en función de la versión de NetApp HCI que esté ejecutando.

Lo que necesitará

- Tiene direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (cada nodo nuevo debe instalarse en la misma red que los nodos existentes de su tipo).
- Tiene uno de los siguientes tipos de cuentas de clúster de almacenamiento de SolidFire:
 - La cuenta de administrador nativa que se creó durante la implementación inicial
 - Una cuenta de usuario personalizada con permisos de administración de dominios, unidades, volúmenes y nodos
- Cableó y encendió el nodo nuevo.
- Tiene la dirección IPv4 de gestión de un nodo de almacenamiento ya instalado. Para encontrar la dirección IP, vaya a la pestaña **Gestión de NetApp Element > clúster > nodos** del plugin de NetApp Element para vCenter Server.
- Comprobó que el nodo nuevo utiliza la misma topología y el mismo cableado de red que los clústeres de almacenamiento existentes.



Asegúrese de que la capacidad de almacenamiento esté dividida uniformemente en todos los chasis para obtener la mejor fiabilidad.

NetApp HCI 1.6P1 y posteriores

Puede utilizar el control del cloud híbrido de NetApp solo si se ejecuta su instalación de NetApp HCI en la versión 1.6P1 o posterior.

Pasos

1. Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>/manager/login
```


2. Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
3. En el panel expandir instalación, seleccione **expandir**.
4. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

5. En la página de bienvenida, seleccione **no**.
6. Seleccione **continuar**.
7. En la página Available Inventory, seleccione el nodo de almacenamiento que desea añadir a la instalación existente de NetApp HCI.
8. Seleccione **continuar**.
9. En la página Network Settings, se ha detectado parte de la información de red desde la implementación inicial. Cada nodo de almacenamiento nuevo se enumera por número de serie, y es necesario asignarle información de red nueva. Siga estos pasos:
 - a. Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo Detected Naming Prefix e insértelo como prefijo para el nuevo nombre de host único que añade en el campo Hostname.
 - b. En el campo Management IP Address, introduzca una dirección IP de gestión para el nodo de almacenamiento nuevo que está en la subred de la red de gestión.
 - c. En el campo Storage (iSCSI) IP Address, introduzca una dirección IP de iSCSI para el nodo de almacenamiento nuevo que está en la subred de la red de gestión.
 - d. Seleccione **continuar**.



La NetApp HCI puede tardar algún tiempo en validar las direcciones IP especificadas. El botón continuar estará disponible cuando se complete la validación de la dirección IP.

10. En la página Review de la sección Network Settings, se muestran los nodos nuevos en texto en negrita. Si necesita hacer cambios en la información de alguna sección, realice los pasos siguientes:
 - a. Seleccione **Editar** para esa sección.
 - b. Cuando termine de hacer los cambios, seleccione **continuar** en cualquier página posterior para volver a la página Revisión.
11. Opcional: Si no desea enviar estadísticas del clúster ni información de soporte a los servidores Active IQ alojados en NetApp, desactive la casilla de comprobación final. Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.
12. Seleccione **Agregar nodos**. Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.
13. Opcional: Verifique que los nodos de almacenamiento nuevos estén visibles en VMware vSphere Web Client.

NetApp HCI 1.4 P2, 1.4 y 1.3

Si la instalación de NetApp HCI ejecuta la versión 1.4P2, 1.4 o 1.3, puede usar el motor de implementación de NetApp para añadir el nodo al clúster.

Pasos

1. Vaya a la dirección IP de gestión de uno de los nodos de almacenamiento existentes:
http://<storage_node_management_IP_address>/
2. Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

3. Seleccione **amplíe su instalación**.
4. En la página de bienvenida, seleccione **no**.
5. Haga clic en **continuar**.
6. En la página Available Inventory, seleccione el nodo de almacenamiento que se va a añadir a la instalación de NetApp HCI.
7. Seleccione **continuar**.
8. En la página Network Settings, realice los pasos siguientes:
 - a. Compruebe la información detectada en la implementación inicial. Cada nodo de almacenamiento nuevo se enumera por número de serie, y es necesario asignarle información de red nueva. Para cada nodo de almacenamiento nuevo, realice los siguientes pasos:
 - i. Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo Detected Naming Prefix e insértelo como prefijo para el nuevo nombre de host único que añade en el campo Hostname.
 - ii. En el campo Management IP Address, introduzca una dirección IP de gestión para el nodo de almacenamiento nuevo que está en la subred de la red de gestión.
 - iii. En el campo Storage (iSCSI) IP Address, introduzca una dirección IP de iSCSI para el nodo de almacenamiento nuevo que está en la subred de la red de gestión.
 - b. Seleccione **continuar**.
 - c. En la página Review de la sección Network Settings, el nodo nuevo se muestra en texto en negrita. Si desea hacer cambios en la información de alguna sección, realice los pasos siguientes:
 - i. Seleccione **Editar** para esa sección.
 - ii. Cuando termine de hacer los cambios, seleccione **continuar** en cualquier página posterior para volver a la página Revisión.
9. Opcional: Si no desea enviar estadísticas del clúster ni información de soporte a los servidores Active IQ alojados en NetApp, desactive la casilla de comprobación final. Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.
10. Seleccione **Agregar nodos**. Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.
11. Opcional: Verifique que los nodos de almacenamiento nuevos estén visibles en VMware vSphere Web Client.

NetApp HCI 1.2, 1.1 y 1.0

Cuando instala el nodo, la interfaz de usuario del terminal (TUI) muestra los campos necesarios para configurar el nodo. Debe introducir la información de configuración que necesite para el nodo antes de

continuar con la adición del nodo al clúster.



La TUI debe usar para configurar información de red estática, así como información del clúster. Si utilizaba una gestión fuera de banda, debe configurarla en el nodo nuevo.

Debe tener una consola o teclado, vídeo, ratón (KVM) para realizar estos pasos y disponer de la información de red y clúster necesaria para configurar el nodo.

Pasos

1. Conecte un teclado y un monitor al nodo. La TUI aparece en el terminal tty1 con la pestaña Network Settings.
2. Utilice la navegación en pantalla para establecer la configuración de red de Bond1G y Bond10G del nodo. Debe introducir la siguiente información para Bond1G:
 - Dirección IP. Es posible reutilizar la dirección IP de gestión del nodo con errores.
 - Máscara de subred. Si no lo sabe, el administrador de red puede proporcionar esta información.
 - Dirección de pasarela. Si no lo sabe, el administrador de red puede proporcionar esta información. Debe introducir la siguiente información de Bond10G:
 - Dirección IP. Es posible reutilizar la dirección IP de almacenamiento del nodo con errores.
 - Máscara de subred. Si no lo sabe, el administrador de red puede proporcionar esta información.
3. Introduzca `s` para guardar la configuración y, a continuación, introduzca `y` para aceptar los cambios.
4. Introduzca `c` Para ir a la pestaña Cluster.
5. Use la navegación en pantalla para establecer el nombre de host y el clúster del nodo.



Si desea cambiar el nombre de host predeterminado por el nombre del nodo que ha quitado, debe hacerlo ahora.



Lo mejor es usar el mismo nombre para el nuevo nodo que el que sustituyó para evitar confusiones en el futuro.

6. Introduzca `s` para guardar la configuración. Los miembros del clúster cambian de Available a Pending.
7. En el plugin de NetApp Element para vCenter Server, seleccione **Gestión de NetApp Element > clúster > nodos**.
8. Seleccione **pendiente** en la lista desplegable para ver la lista de nodos disponibles.
9. Seleccione el nodo que desea agregar y seleccione **Agregar**.



Es posible que el nodo demore hasta 2 minutos en añadirse al clúster y que se muestre en nodos > Active.



Si se añaden las unidades a la vez, se pueden producir interrupciones. Para ver las prácticas recomendadas relacionadas con el adición y la eliminación de unidades, consulte ["Este artículo de la base de conocimientos"](#) (se requiere inicio de sesión).

10. Seleccione **unidades**.
11. Seleccione **Available** en la lista desplegable para ver las unidades disponibles.
12. Seleccione las unidades que desea agregar y seleccione **Agregar**.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Reemplace los nodos H610C y H615C

Debe reemplazar un chasis para reparar errores de nodo de computación relacionados con la CPU, la placa base o si no enciende. Si tiene un DIMM defectuoso en su nodo de computación H610C que ejecuta NetApp HCI Bootstrap OS versión 1.6 o posterior, puede sustituir el DIMM y no tiene que sustituir el chasis. En los nodos H615C, no es necesario sustituir el chasis si un DIMM falla; solo puede sustituir el DIMM con errores.

En el caso de H610C y H615C, los términos "nodo" y "chasis" se utilizan indistintamente, ya que el nodo y el chasis no son componentes separados.



NetApp recomienda el uso del motor de implementación de NetApp para añadir un nodo de computación de reemplazo. Si no puede continuar con la instalación del motor de puesta en marcha de NetApp para ESXi, consulte el artículo de la base de conocimientos de NetApp ["Cómo instalar ESXi en el nodo de computación NetApp HCI manualmente"](#).

Lo que necesitará

- Verificó que el nodo ha fallado.
- Tiene un chasis de reemplazo. Para solicitar una sustitución, debe ponerse en contacto con el soporte de NetApp.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.
- Ha etiquetado cada cable conectado al chasis.

Acerca de esta tarea

Las alarmas en VMware vSphere Web Client alertan de un fallo en un host. Debe coincidir con el número de serie del host con el error desde VMware vSphere Web Client con el número de serie en la etiqueta adhesiva que aparece en la parte posterior del nodo.

Paso 1: Prepárese para sustituir el nodo

Antes de reemplazar el nodo, debe migrar las máquinas virtuales (VM) alojadas en el nodo a un host disponible y quitar el nodo del clúster. Debe registrar detalles sobre el nodo, como el número de serie y la información de redes. La migración de las máquinas virtuales y el registro de los detalles del nodo también se aplica en caso de errores de componentes donde el nodo sigue conectado y funcionando; por ejemplo, un fallo de un módulo de memoria en línea doble (DIMM).

Pasos

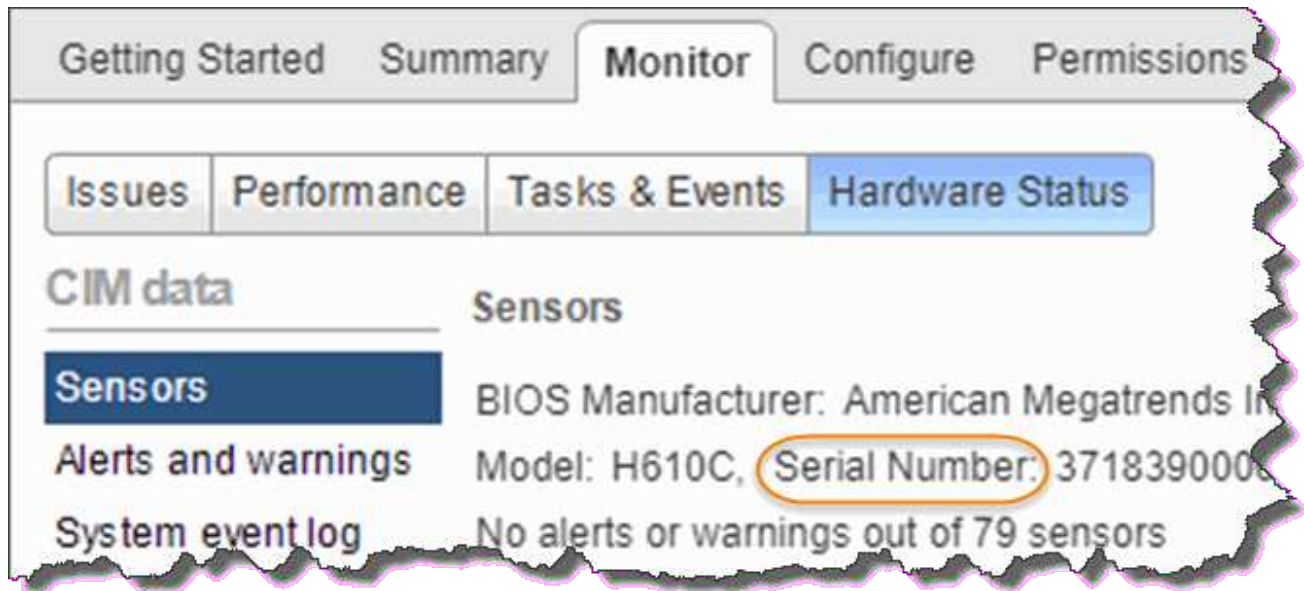
1. En VMware vSphere Web Client, realice los pasos necesarios para migrar las máquinas virtuales a otro host disponible.



Consulte la documentación de VMware para conocer los pasos de migración.

2. Seleccione el nodo que ha fallado y seleccione **Monitor > Estado del hardware > Sensores**.

3. Anote el número de serie del nodo con errores. La siguiente captura de pantalla es sólo un ejemplo:



Necesita el número de serie para identificar el chasis emparejando el número que ha indicado con el número de serie de la etiqueta en la parte posterior del nodo.

4. Haga clic con el botón derecho del ratón en el nodo que ha fallado y seleccione **Conexión > desconectar**.
5. Seleccione **Sí** para confirmar la acción.
6. Haga clic con el botón derecho del ratón en el nodo con errores y seleccione **Quitar del inventario**.
7. Haga clic en **Sí** para confirmar la acción.

Paso 2: Reemplace el nodo

Después de quitar el nodo con errores del clúster, puede quitar el chasis con errores e instalar el chasis de reemplazo.



Asegúrese de tener protección antiestática antes de realizar los pasos aquí.

Pasos

1. Desembale el nuevo chasis y configúrelo en una superficie nivelada. Conserve el material de empaque durante el momento en que devuelve el chasis fallido a NetApp.
2. Etiquete cada cable que esté insertado en la parte posterior del chasis que va a quitar. Después de instalar el nuevo chasis, debe insertar los cables nuevamente en los puertos originales.
3. Desconecte todos los cables de la parte posterior del chasis.
4. Retire el chasis desenroscando los tornillos de apriete manual de las orejas de montaje. Debe empaquetar y devolver el chasis con errores a NetApp.
5. Deslice el chasis de repuesto sobre los rieles.



Asegúrese de no utilizar una fuerza excesiva al deslizar el chasis sobre los rieles.

6. Solo para H615C. Quite los DIMM del chasis con errores e inserte estos DIMM en el chasis de reemplazo.



Debe sustituir los DIMM en las mismas ranuras desde las que se quitaron en el nodo con errores.

- Quite las dos unidades de suministro de alimentación de cada lado del chasis con errores e insértelas en el chasis de reemplazo.
- Vuelva a conectar los cables a los puertos desde los que se desconectaron originalmente. Las etiquetas que había añadido a los cables cuando los desconectó le ayudarán a guiar.



Si la apertura de flujo de aire de la parte trasera del chasis está bloqueada con cables o etiquetas, puede provocar fallos prematuros en los componentes debido al sobrecalentamiento. No fuerce los cables hacia los puertos, podría dañar los cables, los puertos o ambos.

- Encienda el chasis.

Paso 3: Agregar el nodo al clúster

Debe configurar NetApp HCI para usar el nodo de computación nuevo.

Lo que necesitará

- La instancia de vSphere que utiliza NetApp HCI tiene licencia vSphere Enterprise Plus si va a añadir el nodo a una implementación con switches virtuales distribuidos.
- Ninguna de las instancias de vCenter o vSphere que se utilizan con NetApp HCI tiene licencias caducadas.
- Tiene direcciones IPv4 gratuitas y sin usar en el mismo segmento de red que los nodos existentes (el nuevo nodo debe instalarse en la misma red que los nodos existentes de su tipo).
- Tiene listas las credenciales de cuenta de administrador de vCenter.

Pasos

- Abra la dirección IP del nodo de gestión en un navegador web. Por ejemplo:

```
https://<ManagementNodeIP>
```

- Inicie sesión en NetApp Hybrid Cloud Control proporcionando las credenciales de administrador del clúster de almacenamiento de NetApp HCI.
- En el panel expandir instalación, seleccione **expandir**.

El explorador abre el motor de implementación de NetApp.

- Inicie sesión en el motor de implementación de NetApp. Para ello, proporcione las credenciales de administrador del clúster de almacenamiento de NetApp HCI locales.



No se puede iniciar sesión con las credenciales de protocolo ligero de acceso a directorios.

- En la página de bienvenida, seleccione **Sí**.
- En la página End User License, realice las siguientes acciones:
 - Lea el contrato de licencia para usuario final de VMware.

b. Si acepta los términos, seleccione **Acepto** al final del texto del acuerdo.

7. Haga clic en Continuar.

8. En la página vCenter, realice los pasos siguientes:

a. Introduzca un FQDN o una dirección IP y credenciales de administrador para la instancia de vCenter asociada con la instalación de NetApp HCI.

b. Seleccione **continuar**.

c. Seleccione un centro de datos de vSphere existente al cual añadir nodos de computación nuevos o seleccione Create New Datacenter para añadir los nodos de computación nuevos a un centro de datos nuevo.



Si selecciona Create New Datacenter, el campo Cluster se completa automáticamente.

d. Si seleccionó un centro de datos existente, seleccione un clúster de vSphere con el que se deben asociar los nodos de computación nuevos.



Si NetApp HCI no puede reconocer la configuración de red del clúster que seleccionó para la ampliación, asegúrese de que la asignación vmkernel y vmnic para las redes de gestión, almacenamiento y vMotion se establezcan con los valores predeterminados de puesta en marcha.

e. Seleccione **continuar**.

9. En la página ESXi Credentials, introduzca una contraseña raíz ESXi para los nodos de computación que va a añadir. Debe usar la misma contraseña que se creó durante la implementación inicial de NetApp HCI.

10. Seleccione **continuar**.

11. Si creó un clúster de centro de datos de vSphere nuevo, en la página Network Topology, seleccione una topología de red para que coincida con los nodos de computación nuevos que se añaden.



Solo puede seleccionar la opción de dos cables si los nodos de computación utilizan la topología de dos cables y la implementación de NetApp HCI existente se configuró con identificadores de VLAN.

12. En la página Available Inventory, seleccione el nodo que se va a añadir a la instalación existente de NetApp HCI.



Para algunos nodos de computación, es posible que deba habilitar EVC en el nivel más alto admitido por la versión de vCenter antes de añadirlos a la instalación. Debe utilizar el cliente de vSphere a fin de habilitar EVC para estos nodos de computación. Después de habilitar dicha función, actualice la página Inventory e intente añadir nuevamente los nodos de computación.

13. Seleccione **continuar**.

14. Opcional: Si creó un nuevo clúster de centro de datos de vSphere, en la página Network Settings, importe la información de la red desde una implementación de NetApp HCI existente seleccionando la casilla de comprobación **Copiar configuración desde un clúster existente**. Esto rellena la información de la pasarela y de la subred predeterminadas para cada red.

15. En la página Network Settings, se ha detectado parte de la información de red desde la implementación inicial. Cada nodo de computación nuevo se enumera por número de serie, y es necesario asignarle información de red nueva. Para cada nodo de computación nuevo, realice los siguientes pasos:

- a. Si NetApp HCI detectó un prefijo de nomenclatura, cópielo desde el campo Detected Naming Prefix e insértelo como prefijo para el nuevo nombre de host único que añade en el campo Hostname.
 - b. En el campo Management IP Address, introduzca una dirección IP de gestión para el nodo de computación que está en la subred de la red de gestión.
 - c. En el campo vMotion IP Address, introduzca una dirección IP de vMotion para el nodo de computación que está en la subred de la red de vMotion.
 - d. En el campo iSCSI A - IP Address, introduzca una dirección IP para el primer puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.
 - e. En el campo iSCSI B - IP Address, introduzca una dirección IP para el segundo puerto iSCSI del nodo de computación que está en la subred de la red iSCSI.
16. Seleccione **continuar**.
17. En la página Review de la sección Network Settings, el nodo nuevo se muestra en texto en negrita. Si necesita hacer cambios en la información de alguna sección, realice los pasos siguientes:
- a. Seleccione **Editar** para esa sección.
 - b. Cuando termine de hacer los cambios, seleccione **continuar** en cualquier página posterior para volver a la página Revisión.
18. Opcional: Si no desea enviar estadísticas del clúster ni información de soporte a los servidores SolidFire Active IQ alojados en NetApp, desactive la casilla de comprobación final. Esta acción deshabilita la supervisión de diagnóstico y estado en tiempo real para NetApp HCI. Al deshabilitar esta función, se elimina la habilidad de NetApp para admitir y supervisar NetApp HCI de forma anticipada a fin de detectar y resolver problemas antes de que la producción se vea afectada.
19. Seleccione **Agregar nodos**. Puede supervisar el progreso mientras NetApp HCI añade y configura los recursos.
20. Opcional: Verifique que haya nodos de computación nuevos visibles en vCenter.

Paso 4: Instale los controladores de GPU

Los nodos de computación con unidades de procesamiento de gráficos (GPU) de NVIDIA, al igual que el nodo H610C, necesitan los controladores de software de NVIDIA instalados en VMware ESXi para poder aprovechar la potencia de procesamiento aumentada. Para instalar las controladoras de GPU, el nodo de computación debe tener una tarjeta GPU.

Pasos

1. Abra un explorador y vaya al portal de licencias de NVIDIA en la siguiente URL:
<https://nvid.nvidia.com/dashboard/>
2. Descargue la versión del paquete de controladores en su equipo, según su entorno.

En el siguiente ejemplo, se muestra la versión del paquete del controlador para vSphere 6,0, 6,5 y 6,7:

La versión de vSphere	Paquete de controladores
VSphere 6.0	NVIDIA-GRID-vSphere-6.0-390.94-390.96-392.05.zip
VSphere 6.5	NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip

La versión de vSphere	Paquete de controladores
VSphere 6.7	NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip

3. Extraiga el paquete de controladores del ordenador. El archivo .VIB resultante es el archivo de controlador sin comprimir.
4. Copie el archivo del controlador .VIB del equipo en ESXi que se ejecuta en el nodo de computación. La utilidad Protocolo de copia segura (SCP) está disponible en la mayoría de las distribuciones de Linux, o está disponible como una utilidad descargable para todas las versiones de Windows.

El ejemplo siguiente muestra los comandos de ESXi 6,0, 6,5 y 6,7. Los comandos asumen que el controlador está ubicado en el directorio \$HOME/nvidia/ESX6.x/ del host de gestión:

Opción	Descripción
ESXi 6.0	scp \$HOME/NVIDIA/ESX6.0/NVIDIA**.vib root@<ESXi_IP_ADDR>:./
ESXi 6.5	scp \$HOME/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:./
ESXi 6.7	scp \$HOME/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:./

5. Siga los pasos siguientes para iniciar sesión como root en el host ESXi e instalar NVIDIA vGPU Manager en ESXi.
 - a. Ejecute el siguiente comando para iniciar sesión en el host ESXi como usuario raíz:

```
ssh root@<ESXi_IP_ADDRESS>
```
 - b. Ejecute el siguiente comando para verificar que no hay controladores de GPU NVIDIA instalados actualmente:

```
nvidia-smi`Este comando debería devolver el mensaje `nvidia-smi: not found.
```
 - c. Ejecute los siguientes comandos para activar el modo de mantenimiento en el host e instale NVIDIA vGPU Manager desde el archivo VIB:

```
esxcli system maintenanceMode set --enable true
esxcli software vib install -v /NVIDIA**.vib`Debería ver el mensaje
`Operation finished successfully.
```
 - d. Ejecute el siguiente comando y compruebe que los ocho controladores de GPU aparecen en la lista del resultado del comando:

```
nvidia-smi
```
 - e. Ejecute el siguiente comando para comprobar que el paquete NVIDIA vGPU se ha instalado y cargado correctamente:

```
vmkload_mod -l | grep nvidia`El comando debería mostrar un resultado similar
al siguiente: `nvidia 816 13808
```
 - f. Ejecute los siguientes comandos para salir del modo de mantenimiento y reiniciar el host:

```
esxcli system maintenanceMode set -enable false
reboot -f
```

6. Repita los pasos 4-6 para cualquier otro nodo de computación recién implementado con GPU de NVIDIA.
7. Realice las siguientes tareas siguiendo las instrucciones del sitio de documentación de NVIDIA:
 - a. Instale el servidor de licencias de NVIDIA.
 - b. Configurar los invitados de máquinas virtuales para el software NVIDIA vGPU.
 - c. Si utiliza puestos de trabajo habilitados para vGPU en un contexto de infraestructura de puestos de trabajo virtuales (VDI), configure VMware Horizon View para el software vGPU de NVIDIA.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Sustituya los nodos H610S

Puede que deba sustituir el chasis si falla el ventilador, la unidad de procesamiento central (CPU) o el módulo de memoria en línea doble (DIMM), o bien si resuelve problemas de sobrecalentamiento o problemas con el proceso de arranque. El LED ámbar parpadeante de la parte frontal del chasis indica la posible necesidad de sustituir el chasis. Debe comunicarse con el soporte de NetApp antes de continuar.



Consulte ["Artículo de base de conocimientos"](#) Para obtener información acerca de los requisitos de instalación para los nodos H610S. Los nodos de almacenamiento H610S nuevos y de repuesto pueden tener requisitos de instalación adicionales según la versión existente del software Element del clúster de almacenamiento. Póngase en contacto con el soporte de NetApp si desea obtener más información.



Los términos "nodo" y "chasis" se utilizan indistintamente en el caso de H610S, que es un chasis de unidad de rack (1U).

Prácticas recomendadas para agregar y quitar unidades

Debe seguir estas prácticas recomendadas para añadir unidades al clúster:

- Añada todas las unidades de bloques y asegúrese de que la sincronización de bloques se complete antes de añadir las unidades de segmentos.
- Para el software Element 10.x y versiones posteriores, añada todas las unidades de bloques a la vez. Asegúrese de no hacerlo para más de tres nodos a la vez.
- Para el software Element 9.x y versiones anteriores, añada tres unidades a la vez que le permitan sincronizarse completamente antes de añadir el siguiente grupo de tres.
- Quite la unidad de segmentos y asegúrese de que la sincronización de segmentos se complete antes de quitar las unidades de bloques.
- Quite todas las unidades de bloques de un único nodo a la vez. Asegúrese de que toda la sincronización de bloques esté completa antes de moverse al siguiente nodo.

Lo que necesitará

- Se ha puesto en contacto con el soporte de NetApp. Si solicita una sustitución, debe tener un caso abierto con el soporte de NetApp.

- Ha obtenido el nodo de sustitución.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.
- Si necesita realizar el proceso Volver a la imagen de fábrica (RTFI), ha obtenido la llave USB. El soporte de NetApp puede ayudarle a decidir si necesita llevar a cabo el proceso RTFI.
- Tiene un teclado y un monitor.
- Ha quitado el nodo con errores correctamente del clúster.
- Si un DIMM ha dado error, ha quitado las unidades antes de quitar el nodo del clúster.

Acerca de esta tarea

Las alarmas en VMware vSphere Web Client alertan de un fallo en un host. Debe coincidir con el número de serie del host con el error desde VMware vSphere Web Client con el número de serie en la etiqueta adhesiva que aparece en la parte posterior del nodo.

Pasos

1. Localice la etiqueta de servicio en la parte frontal del chasis con errores.



2. Compruebe que el número de serie de la etiqueta de servicio coincida con el número de caso de soporte de NetApp cuando solicitó el chasis de reemplazo.
3. Conecte el teclado y el monitor a la parte posterior del chasis con errores.
4. Compruebe el número de serie del nodo con errores con el soporte de NetApp.
5. Apague el chasis.
6. Etiquete las unidades frontales y los cables posteriores con sus ubicaciones, de modo que se puedan volver a colocar en las mismas ubicaciones después de la sustitución.

Consulte la siguiente imagen para ver la colocación de las unidades en el chasis:



7. Quite los cables.
8. Retire el chasis desenroscando los tornillos de apriete manual de las orejas de montaje. Debe empaquetar y devolver el chasis con errores a NetApp.
9. Instale el chasis de repuesto.
10. Quite las unidades con cuidado del chasis que ha fallado e insértelas en el chasis de reemplazo.



Debe insertar las unidades en las mismas ranuras en las que estaban antes de quitarlas.

11. Quite las unidades de suministro de alimentación del chasis con errores e insértelas en el chasis de reemplazo.
12. Inserte los cables de suministro de alimentación y los cables de red en sus puertos originales.
13. Es posible que se inserten transceptores de factor de forma pequeño conectable (SFP) en los puertos 10 GbE del nodo de reemplazo. Debe quitarlos antes de conectar los puertos 10 GbE.



Consulte la documentación del proveedor del switch si el switch no reconoce los cables.

14. Encienda el chasis pulsando el botón de encendido situado en la parte frontal. El nodo tarda aproximadamente cinco minutos y 30 segundos en arrancar.
15. Realice los pasos de configuración.
 - Si el nodo H610S forma parte de una instalación de NetApp HCI, utilice Hybrid Cloud Control de NetApp para configurar el recurso de almacenamiento. Consulte "[Amplíe los recursos de almacenamiento de NetApp HCI](#)".
 - Si el nodo H610S forma parte de una instalación de almacenamiento all-flash de SolidFire, configure el nodo mediante la interfaz de usuario de software (IU) de NetApp Element. Comuníquese con el soporte de NetApp para obtener ayuda.

Obtenga más información

- "[Recursos de NetApp HCI](#)"
- "[Centro de documentación de SolidFire y el software Element](#)"

Sustituya las unidades de alimentación

Cada chasis incluye dos unidades de alimentación para redundancia de alimentación. Si una unidad de fuente de alimentación está defectuosa, debe sustituirla lo antes posible para garantizar que el chasis dispone de una fuente de alimentación redundante.

Lo que necesitará

- Ha determinado que la unidad de alimentación está defectuosa.
- Tiene una unidad de suministro de alimentación de repuesto.
- Ha comprobado que la segunda unidad de alimentación está en funcionamiento.

- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otras precauciones antiestáticas.

Acerca de esta tarea

El procedimiento de sustitución se aplica a los siguientes modelos de nodo:

- Chasis NetApp HCI de cuatro nodos y unidad rack doble (2U)
- Chasis de computación 2U H610C
- Una unidad de rack (1U) chasis de computación H615C
- Chasis de almacenamiento H610S de 1U



En el caso de H610C, H615C y H610S, los términos "nodo" y "chasis" se utilizan indistintamente porque el nodo y el chasis no son componentes separados, a diferencia de lo que sucede en el chasis 2U de cuatro nodos.

Las alarmas en VMware vSphere Web Client proporcionan información sobre la unidad de suministro de alimentación con fallos, para referirla como PS1 o PS2. En un chasis NetApp HCI 2U de cuatro nodos, PS1 hace referencia a la unidad de la fila superior del chasis y PS2 hace referencia a la unidad de la fila inferior del chasis. Puede sustituir la unidad de fuente de alimentación defectuosa mientras el chasis está encendido y en funcionamiento, siempre que la unidad de fuente de alimentación redundante esté funcionando.

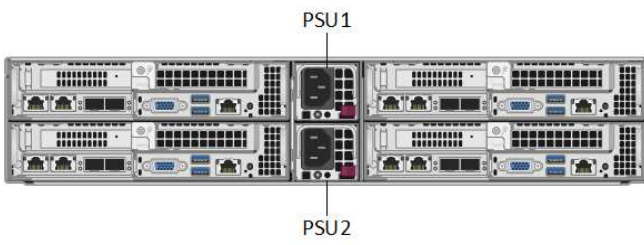
Pasos




1. Localice la unidad de alimentación defectuosa en el chasis. El indicador LED de la unidad defectuosa se ilumina en ámbar.



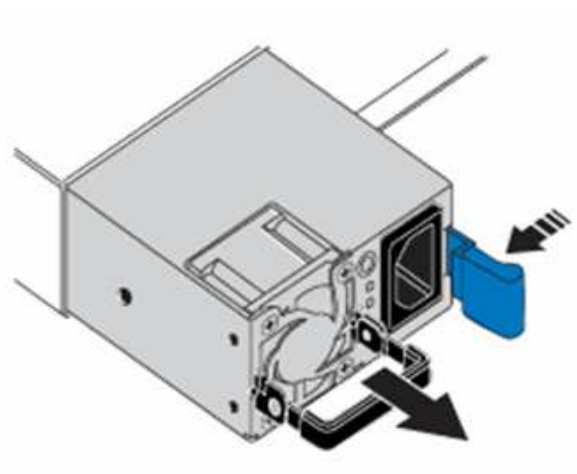
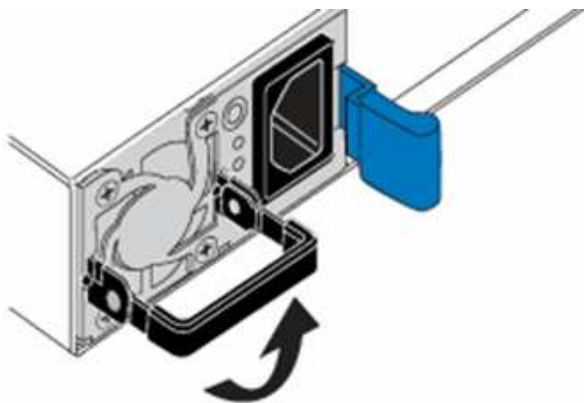
Las unidades de suministro de alimentación se encuentran de forma diferente según el tipo de chasis.

Consulte las siguientes imágenes para conocer las ubicaciones de las unidades de alimentación:

Modelo	Ubicación de las unidades de alimentación
Chasis de almacenamiento NetApp HCI 2U de cuatro nodos	 <p data-bbox="873 1585 928 1680"> </p> <p data-bbox="987 1585 1458 1717">Los nodos del chasis pueden parecer diferentes según el tipo de nodos (almacenamiento o computación) que tenga.</p>

Modelo	Ubicación de las unidades de alimentación
Chasis H610C	 <p data-bbox="911 306 959 327">PSU1</p> <p data-bbox="1354 306 1403 327">PSU0</p>
Chasis H615C	 <p data-bbox="902 480 951 501">PSU1</p> <p data-bbox="1346 480 1395 501">PSU0</p>
Chasis H610S	 <p data-bbox="902 653 951 674">PSU1</p> <p data-bbox="1346 653 1395 674">PSU0</p>

2. Desconecte el cable de alimentación de la unidad de alimentación.
3. Levante el asa de la leva y presione el pestillo azul para sacar la unidad de alimentación.

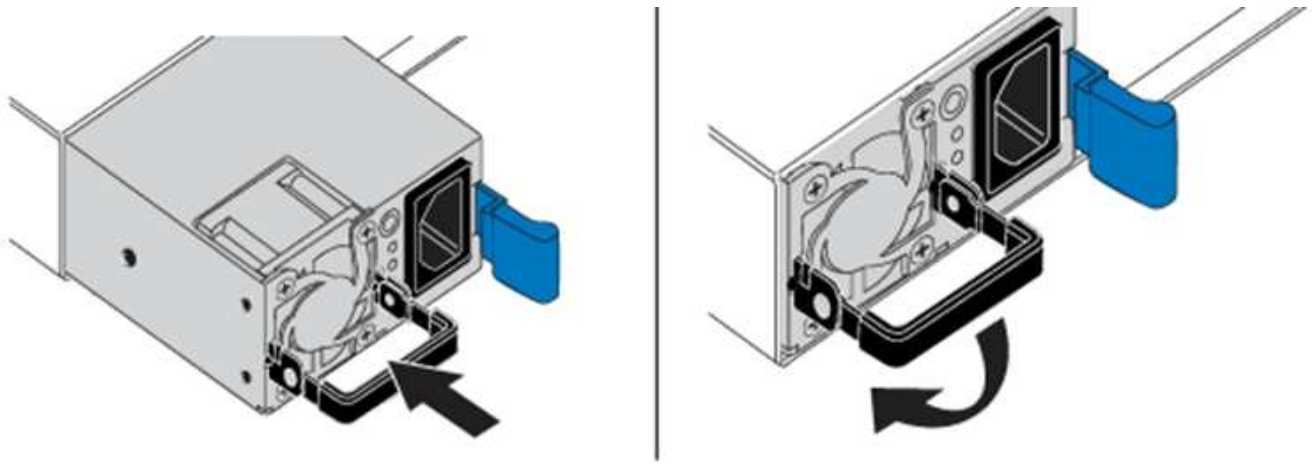


La ilustración es un ejemplo. La ubicación de la fuente de alimentación en el chasis y el color del botón de liberación varían según el tipo de chasis que tenga.



Asegúrese de utilizar ambas manos para soportar el peso de la unidad de alimentación.

4. Con ambas manos, alinee los bordes de la unidad de alimentación con la abertura del chasis, empuje suavemente la unidad hacia el chasis con el asa de leva hasta que encaje en su sitio y vuelva a colocar el mango de leva en la posición vertical.



5. Enchufe el cable de alimentación.
6. Devuelva la unidad defectuosa a NetApp siguiendo las instrucciones de la caja que le ha enviado.

Obtenga más información

- ["Recursos de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Sustituir los interruptores SN2010, SN2100 y SN2700

Puede sustituir sin interrupciones un switch SN2000 defectuoso siguiendo las prácticas recomendadas y pasos de NetApp.

Lo que necesitará

- Asegúrese de que Putty está instalado en el portátil y de que captura la salida. Vea este vídeo para aprender a configurar Putty para capturar la sesión de salida.

<https://img.youtube.com/vi/2LZfWH8HffA/maxresdefault.jpg>

- Asegúrese de ejecutar Config Advisor de NetApp antes y después de la sustitución. Esto puede ayudar a identificar otros problemas antes de que comience el mantenimiento. Descargue e instale Config Advisor, y acceda a la guía de inicio rápido desde ["aquí \(se requiere inicio de sesión\)"](#).
- Obtenga un cable de alimentación, las herramientas manuales básicas y las etiquetas.
- Asegúrese de haber planificado un plazo de mantenimiento de dos a cuatro horas.
- Familiarícese con los siguientes puertos del switch:

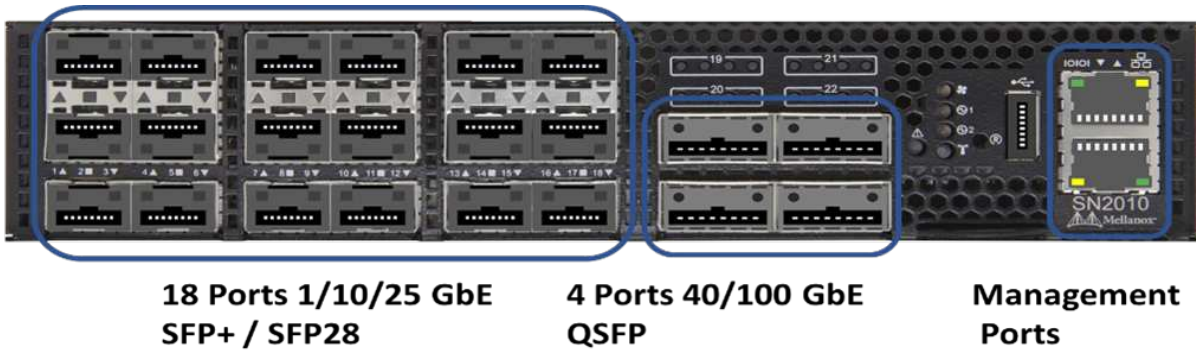


Figura 1. Cubierta del interruptor SN2010 y puertos

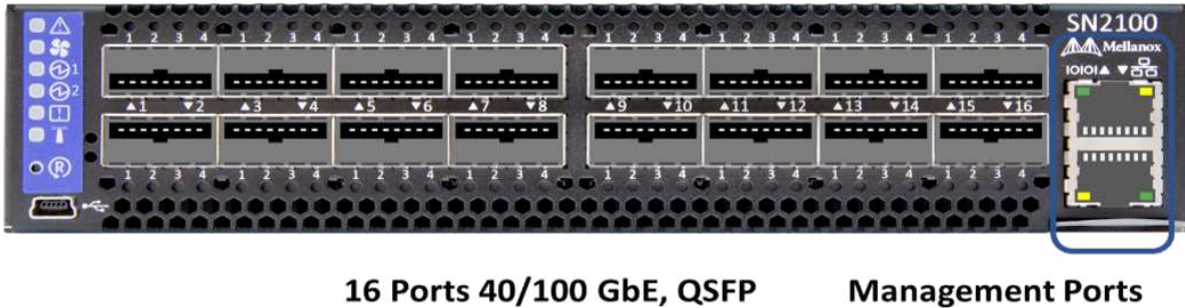


Figura 2. Cubierta del interruptor SN2100 y puertos



Figura 3. Parte trasera de los interruptores SN2010 y SN2100



Figura 4. Interruptor SN2700 delantero y trasero

Acerca de esta tarea

Debe realizar los pasos de este procedimiento en el siguiente orden. Esto es para garantizar que el tiempo de inactividad sea mínimo y que el interruptor de sustitución esté preconfigurado antes de sustituir el conmutador.



Póngase en contacto con el soporte de NetApp si necesita ayuda.

A continuación se ofrece una descripción general de los pasos del procedimiento:[Prepárese para sustituir el interruptor defectuoso](#)

[Cree el archivo de configuración](#)

[Retire el interruptor defectuoso e instale la sustitución](#)

[Verifique la versión del sistema operativo en el interruptor](#)

[Configure el interruptor de sustitución](#)

[Complete la sustitución](#)

Prepárese para sustituir el interruptor defectuoso

Realice los pasos siguientes antes de sustituir el interruptor defectuoso.

Pasos

1. Compruebe que el interruptor de sustitución es el mismo modelo que el interruptor defectuoso.
2. Etiquete todos los cables conectados al interruptor defectuoso.
3. Identifique el servidor de archivos externo en el que se guardan los archivos de configuración del switch.
4. Asegúrese de haber obtenido la siguiente información:
 - a. Interfaz utilizada para la configuración inicial: Puerto RJ-45 o interfaz de terminal serie.
 - b. Las credenciales necesarias para el acceso del switch: Dirección IP del puerto de administración del switch no defectuoso y del switch defectuoso.
 - c. Las contraseñas para el acceso de administración.

Cree el archivo de configuración

Puede configurar un conmutador mediante los archivos de configuración que cree. Elija una de las siguientes opciones para crear el archivo de configuración para el conmutador.

Opción	Pasos
Cree el archivo de configuración de copia de seguridad desde el conmutador defectuoso	<ol style="list-style-type: none"><li data-bbox="829 157 1455 226">1. Conéctese al switch de forma remota mediante SSH, como se muestra en el ejemplo siguiente: <pre data-bbox="865 258 1487 352">ssh admin@<switch_IP_address</pre><li data-bbox="829 390 1406 459">2. Entre en el modo de configuración como se muestra en el siguiente ejemplo: <pre data-bbox="865 491 1487 627">switch > enable switch # configure terminal</pre><li data-bbox="829 665 1479 735">3. Busque los archivos de configuración disponibles como se muestra en el siguiente ejemplo: <pre data-bbox="865 766 1487 936">switch (config) # switch (config) # show configuration files</pre><li data-bbox="829 974 1382 1043">4. Guarde el archivo de configuración de LA BANDEJA activa en un servidor externo: <pre data-bbox="865 1075 1487 1289">switch (config) # configuration upload my-filename scp://myusername@my- server/path/to/my/<file></pre>

Opción	Pasos
<p>Cree el archivo de configuración de copia de seguridad modificando el archivo desde otro conmutador</p>	<ol style="list-style-type: none"> <li data-bbox="833 159 1455 226">1. Conéctese al switch de forma remota mediante SSH, como se muestra en el ejemplo siguiente: <div data-bbox="867 260 1484 352" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>ssh admin@<switch_IP_address</pre> </div> <li data-bbox="833 390 1403 457">2. Entre en el modo de configuración como se muestra en el siguiente ejemplo: <div data-bbox="867 491 1484 625" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>switch > enable switch # configure terminal</pre> </div> <li data-bbox="833 663 1479 764">3. Cargue un archivo de configuración basado en texto desde el switch a un servidor externo, como se muestra en el siguiente ejemplo: <div data-bbox="867 798 1484 1054" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>switch (config) # switch (config) # configuration text file my-filename upload scp://root@my- server/root/tmp/my-filename</pre> </div> <li data-bbox="833 1092 1451 1192">4. Modifique los siguientes campos del archivo de texto para que coincidan con el conmutador defectuoso: <div data-bbox="867 1226 1484 1722" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>## Network interface configuration ## no interface mgmt0 dhcp interface mgmt0 ip address XX.XXX.XX.XXX /22 ## ## Other IP configuration ## hostname oldhostname</pre> </div>

Retire el interruptor defectuoso e instale la sustitución

Lleve a cabo los pasos necesarios para extraer el interruptor defectuoso e instalar la sustitución.

Pasos

1. Localice los cables de alimentación en el switch defectuoso.
2. Etiquete y desconecte los cables de alimentación después de reiniciar el interruptor.
3. Etiquete y desconecte todos los cables del interruptor defectuoso y fíjelos para evitar daños durante la sustitución del interruptor.
4. Retire el interruptor del rack.
5. Instale el interruptor de sustitución en el rack.
6. Conecte los cables de alimentación y los cables de puerto de gestión.



El interruptor se enciende automáticamente cuando se activa la alimentación de CA. No hay botón de encendido. Puede que el LED de estado del sistema demore hasta 5 minutos en ponerse en verde.

7. Conéctese al conmutador mediante el puerto de administración RJ-45 o la interfaz de terminal serie.

Verifique la versión del sistema operativo en el interruptor

Compruebe la versión del software del sistema operativo en el switch. La versión del interruptor defectuoso y el interruptor en buen estado deben coincidir.

Pasos

1. Conéctese al switch de forma remota mediante SSH.
2. Acceda al modo de configuración.
3. Ejecute el `show version` comando. Consulte el siguiente ejemplo:

```
SFPS-HCI-SW02-A (config) #show version
Product name:      Onyx
Product release:   3.7.1134
Build ID:          #1-dev
Build date:        2019-01-24 13:38:57
Target arch:       x86_64
Target hw:         x86_64
Built by:          jenkins@e4f385ab3f49
Version summary:   X86_64 3.7.1134 2019-01-24 13:38:57 x86_64

Product model:     x86onie
Host ID:           506B4B3238F8
System serial num: MT1812X24570
System UUID:       27fe4e7a-3277-11e8-8000-506b4b891c00

Uptime:            307d 3h 6m 33.344s
CPU load averages: 2.40 / 2.27 / 2.21
Number of CPUs:    4
System memory:     3525 MB used / 3840 MB free / 7365 MB total
Swap:              0 MB used / 0 MB free / 0 MB total
```

4. Si las versiones no coinciden, debería actualizar el sistema operativo. Consulte ["Guía de actualización de software de Mellanox"](#) para obtener más detalles.


Configure el interruptor de sustitución

Realice los pasos necesarios para configurar el interruptor de sustitución. Consulte ["Gestión de la configuración de Mellanox"](#) para obtener más detalles.

Pasos

1. Elija una de las opciones que se aplican a usted:

Opción	Pasos
Desde el archivo de configuración DE BIN	<ol style="list-style-type: none">1. Recupere el archivo de configuración DE BIN como se muestra en el siguiente ejemplo: <pre>switch (config) # configuration fetch scp://myusername@my- server/path/to/my/<file></pre>2. Cargue el archivo de configuración DE BIN que ha obtenido en el paso anterior, como se muestra en el siguiente ejemplo: <pre>switch (config) # configuration switch-to my-filename</pre>3. Tipo <code>yes</code> para confirmar el reinicio.

Opción	Pasos
Del archivo de texto	<ol style="list-style-type: none"> Restablezca el interruptor a los valores predeterminados de fábrica: <pre>switch (config) # reset factory keep-basic</pre> Aplicar el archivo de configuración basado en texto: <pre>switch (config) # configuration text file my-filename apply</pre> Cargue un archivo de configuración basado en texto desde el switch a un servidor externo, como se muestra en el siguiente ejemplo: <pre>switch (config) # switch (config) # configuration text file my-filename upload scp://root@my- server/root/tmp/my-filename</pre> <p> No es necesario reiniciar el archivo de texto.</p>

Complete la sustitución

Lleve a cabo los pasos necesarios para completar el procedimiento de sustitución.

Pasos

1. Inserte los cables utilizando las etiquetas que le guiarán.
2. Ejecución de Config Advisor de NetApp. Acceda a la Guía de inicio rápido desde "[aquí \(se requiere inicio de sesión\)](#)".
3. Compruebe su entorno de almacenamiento.
4. Devuelva el switch defectuoso a NetApp.

Obtenga más información

- "[Recursos de NetApp HCI](#)"
- "[Centro de documentación de SolidFire y el software Element](#)"

Sustituya el nodo de almacenamiento en un clúster de dos nodos

Antes de sustituir un nodo de almacenamiento que forma parte de un clúster de dos nodos, debería añadir primero un tercer nodo de almacenamiento (que requiere un nuevo conjunto de direcciones IP), permitir la sincronización completarse y eliminar el nodo defectuoso. El clúster permanece en el estado degradado hasta que un nodo de reemplazo se une al clúster.

Lo que necesitará

- Tiene nuevas direcciones IP de gestión y de almacenamiento.
- Verificó que el clúster muestra el `ClusterCannotSync` alerta después de que el nodo se desconecta. De este modo se garantiza que el clúster realice una resincronización completa cuando el nuevo nodo se vuelve a añadir al clúster. Esta alerta se muestra aproximadamente seis minutos después de que el nodo de almacenamiento se desconecta.
- Se ha puesto en contacto con el soporte de NetApp. Si solicita una sustitución, debe tener un caso abierto con el soporte de NetApp.
- Ha obtenido el nodo de sustitución.
- Usted tiene una muñequera de descarga electrostática (ESD), o usted ha tomado otra protección antiestática.

Acerca de esta tarea

Las alarmas en VMware vSphere Web Client alertan de un fallo en un host. Debe coincidir con el número de serie del host con el error desde VMware vSphere Web Client con el número de serie en la etiqueta adhesiva que aparece en la parte posterior del nodo.

Pasos

1. Quite físicamente el nodo defectuoso del rack. Los pasos dependen del tipo de nodo de almacenamiento que tenga. Consulte ["Sustituya los nodos H410S"](#) y.. ["Sustituya los nodos H610S"](#).



No quite el nodo del clúster en este momento.

2. Instale el nodo de repuesto en la misma ranura.
3. Cablee el nodo.
4. Encienda el nodo.
5. Conecte un teclado y un monitor al nodo.
6. Realice los pasos de configuración:
 - a. Configure la dirección IP de IPMI/BMC.
 - b. Configure el nodo nuevo con las direcciones IP de gestión y las direcciones IP de almacenamiento nuevas, y el nombre del clúster.
7. Una vez que el nodo se añade al clúster, añada las unidades.
8. Una vez finalizada la sincronización, quite las unidades con errores y el nodo con errores del clúster.
9. Utilice el control de cloud híbrido de NetApp para configurar el nodo de almacenamiento nuevo que ha añadido. Consulte ["Amplíe los recursos de almacenamiento de NetApp HCI"](#).

Obtenga más información

- ["Centro de documentación de NetApp HCI"](#)
- ["Centro de documentación de SolidFire y el software Element"](#)

Versiones anteriores de la documentación de NetApp HCI

La documentación de versiones anteriores de NetApp HCI está disponible por si no está ejecutando la versión más reciente.

- ["NetApp HCI 1.8P1"](#)
- ["NetApp HCI 1.8 y anteriores"](#)

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- ["Aviso sobre el rol de Ansible para las actualizaciones de computación"](#)
- ["Aviso para Ember OS 12.3.1"](#)
- ["Aviso para Ember OS 12.3"](#)
- ["Aviso para el nodo de gestión 12.3.1"](#)
- ["Aviso para el nodo de gestión 12.3"](#)
- ["Aviso para NetApp HCI 1.9P1"](#)
- ["Aviso para NetApp HCI 1.9"](#)
- ["Aviso para el paquete de firmware de almacenamiento 2.146"](#)
- ["Aviso para el paquete de firmware de computación 2.146"](#)
- ["Aviso para el paquete de firmware de almacenamiento 2.99.2"](#)
- ["Aviso para el paquete de firmware de computación 2.76"](#)
- ["Aviso para el paquete de firmware de almacenamiento 2.76"](#)

- "Aviso para el paquete de firmware de computación 2.27"
- "Aviso para el paquete de firmware de almacenamiento 2.27"
- "Aviso para ISO de firmware de computación"
- "Aviso de H610S BMC"
- "Aviso para servicios de gestión 2.25.42 (complemento NetApp Element para VMware vCenter Server 5,3.9)"
- "Aviso para servicios de gestión 2.24.40 (complemento NetApp Element para VMware vCenter Server 5,2.12)"
- "Aviso relativo a los servicios de gestión 2.23.64 (complemento NetApp Element para VMware vCenter Server 5.1.12)"
- "Aviso para servicios de gestión 2.22.7 (plugin de NetApp Element para vCenter Server 5.0.37)"
- "Aviso para servicios de gestión 2.21.61 (complemento NetApp Element para vCenter Server 4.10.12)"
- "Aviso para servicios de gestión 2.20.69 (plugin de NetApp Element para vCenter Server 4.9.14)"
- "Aviso para servicios de gestión 2.19.48 (plugin de NetApp Element para vCenter Server 4.8.34)"
- "Aviso para servicios de gestión 2.18.91 (plugin de NetApp Element para vCenter Server 4.7.10)"
- "Aviso para servicios de gestión 2.17.56 (plugin de NetApp Element para vCenter Server 4.6.32)"
- "Aviso para servicios de gestión 2.17.52 (plugin de NetApp Element para vCenter Server 4.6.29)"
- "Aviso para servicios de gestión 2.16 (plugin de NetApp Element para vCenter Server 4.6.29)"
- "Aviso para servicios de gestión 2.14 (plugin de NetApp Element para vCenter Server 4.5.42)"
- "Aviso para servicios de gestión 2.13 (plugin de NetApp Element para vCenter Server 4.5.42)"
- "Aviso para servicios de gestión 2.11 (plugin de NetApp Element para vCenter Server 4.4.72)"
- "Aviso para NetApp HCI 1.8"

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.