Conceptos

HCI

NetApp
June 11, 2024

Tabla de contenidos

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
`https://[IPv4 address of Bond1G interface on a storage node]`	Acceda al asistente del motor de implementación de NetApp para instalar y configurar NetApp HCI. "Leer más."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </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."
`https://[IP address]:442`	Desde la interfaz de usuario por nodo, acceda a la configuración de red y clúster y utilice pruebas y utilidades del sistema. "Leer más".
`https://[management node IP address]:9443`	Registre el paquete del plugin de vCenter en vSphere Web Client.
`https://activeiq.solidfire.com`	Supervise los datos y reciba alertas sobre los cuellos de botella de rendimiento o los problemas potenciales del sistema.
`https://<ManagementNodeIP>/mnode`	Actualice manualmente los servicios de gestión mediante la interfaz de usuario de API DE REST desde el nodo de gestión.
`https://[storage cluster MVIP address]`	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 de son elementos de hardware que proporcionan recursos de almacenamiento para un sistema NetApp HCI de. 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.

Requerimiento: Configure las VM de Witness Node para usar el almacén de datos local (predeterminado establecido por NDE) para el nodo de cálculo. No debe configurarlos en almacenamiento compartido, como los volúmenes de almacenamiento de SolidFire. Para evitar que las máquinas virtuales se migren automáticamente, establezca el nivel de automatización Distributed Resource Scheduler (DRS) para la máquina virtual Witness Node en **Disabled**. 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).

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".

Más información acerca de "Requisitos de recursos del nodo de observación" y.. "Requisitos de dirección IP de los nodos de observación".

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 relevo 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

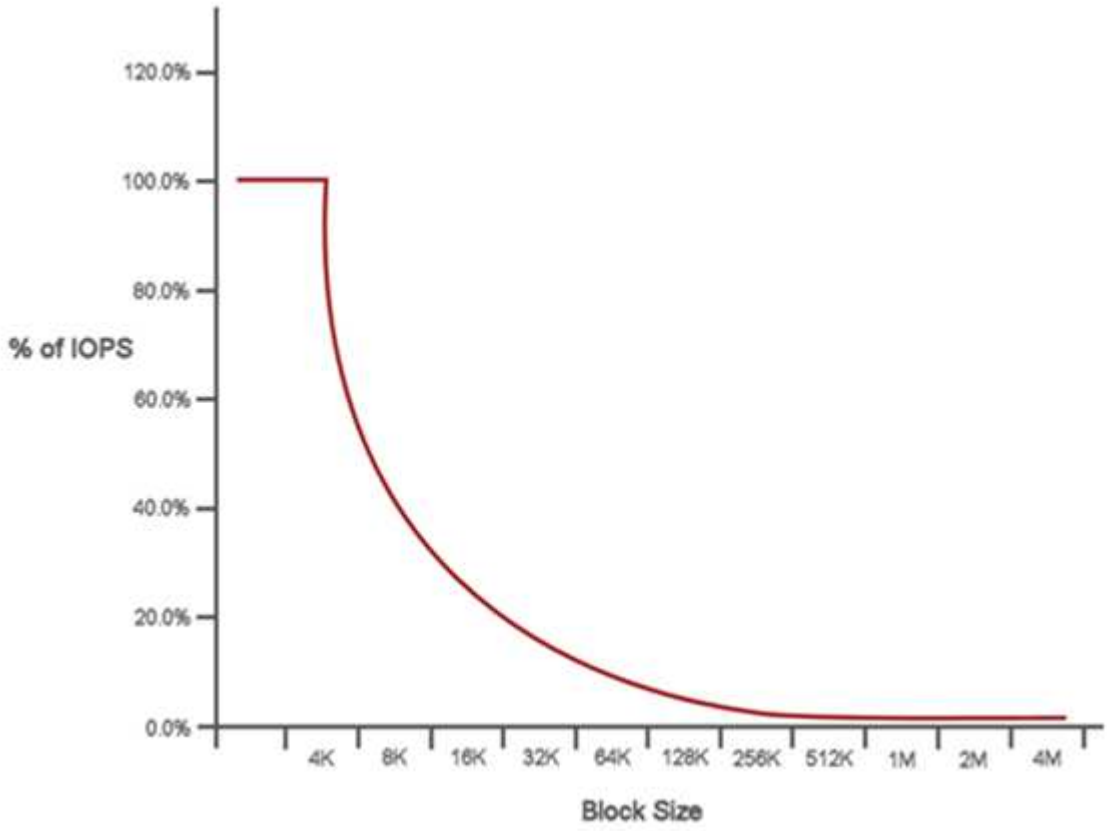
*Estas estimaciones son aproximadas. **Max IOPS y Burst IOPS se pueden establecer con un valor máximo de 200,000 000; sin embargo, este valor solo se permite para destapar de forma efectiva el rendimiento de un volumen. El rendimiento máximo en el mundo real de un volumen está limitado por el uso del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