Conceptos

Element Software

NetApp
January 15, 2024

Tabla de contenidos

Conceptos

Conozca los conceptos básicos relacionados con el software Element.

- "Información general del producto"
- Información general de la arquitectura de SolidFire
- Nodos
- De clúster
- "Seguridad"
- Cuentas y permisos
- "Volúmenes"
- Protección de datos
- Rendimiento y calidad del servicio

Obtenga más información

- "Información general sobre el almacenamiento all-flash de SolidFire"
- "Documentación de SolidFire y el software Element"

Información general del producto

Un sistema de almacenamiento all-flash de SolidFire consta de componentes de hardware diferenciados (unidad y nodos) que se combinan en un pool de recursos de almacenamiento único. Este clúster unificado se presenta como un único sistema de almacenamiento para que lo utilicen clientes externos y se gestiona con el software NetApp Element.

Mediante la interfaz de Element, la API u otras herramientas de gestión, puede supervisar el rendimiento y la capacidad de almacenamiento del clúster de SolidFire y gestionar la actividad de almacenamiento en una infraestructura multi-tenant.

Funciones de SolidFire

Un sistema SolidFire ofrece las siguientes funciones:

- Ofrece almacenamiento de alto rendimiento para su infraestructura de cloud privado a gran escala
- Ofrece una escala flexible que le permite satisfacer las cambiantes necesidades de almacenamiento
- Utiliza una interfaz de software Element de gestión de almacenamiento condicionada por la API
- Garantiza el rendimiento utilizando políticas de calidad de servicio
- Incluye equilibrio de carga automático en todos los nodos del clúster
- Los clústeres se reequilibran automáticamente cuando se agregan o se quitan nodos

Puesta en marcha de SolidFire

Utilice los nodos de almacenamiento que proporciona NetApp e integrados con el software NetApp Element.

"Información general de la arquitectura de almacenamiento all-flash de SolidFire"

Obtenga más información

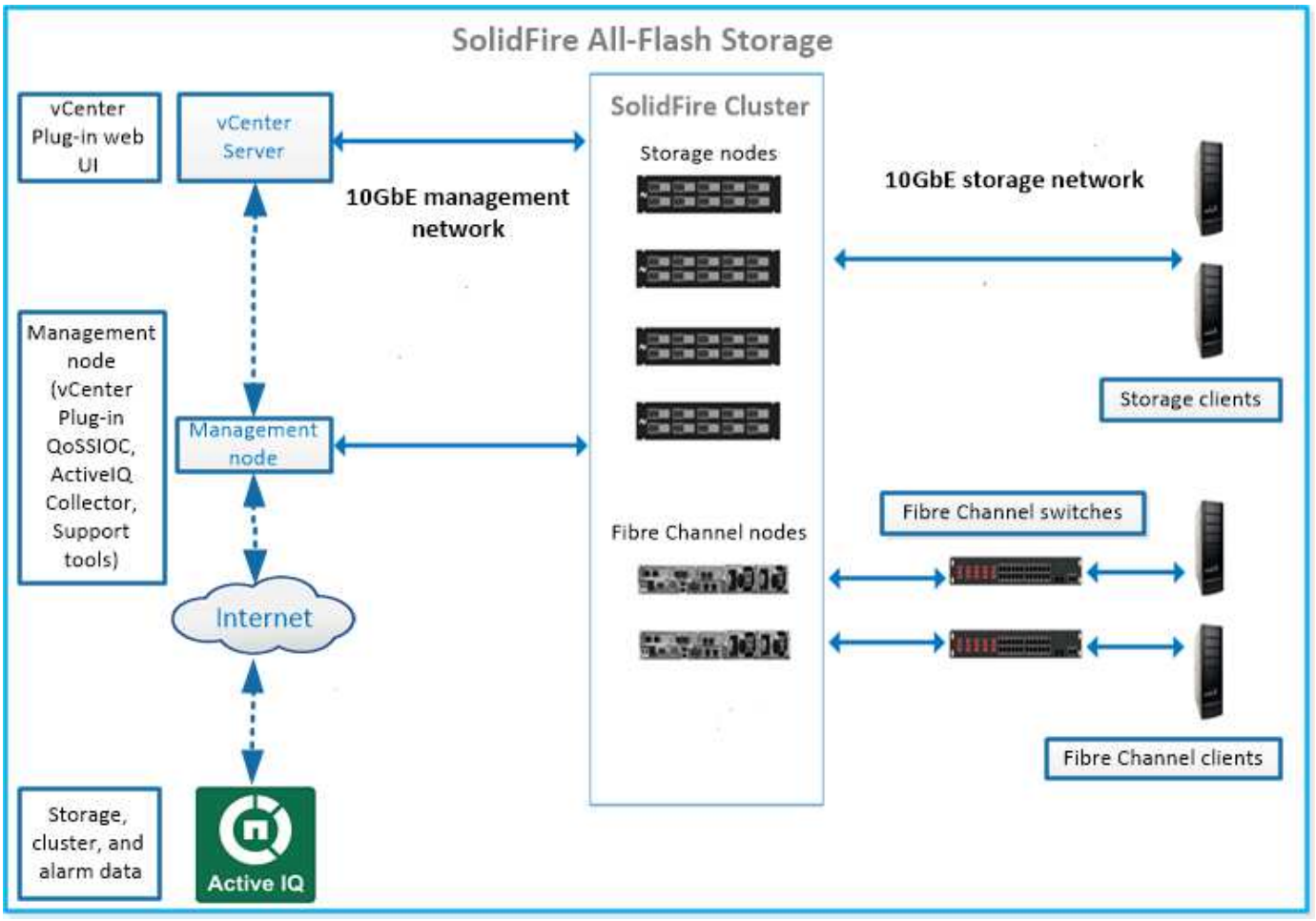
- "Información general sobre el almacenamiento all-flash de SolidFire"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Información general de la arquitectura de SolidFire

Un sistema de almacenamiento all-flash SolidFire consta de componentes de hardware diferenciados (unidad y nodos) que se combinan en un pool de recursos de almacenamiento con el software NetApp Element que se ejecuta de manera independiente en cada nodo. Este único sistema de almacenamiento se gestiona como una única entidad utilizando la interfaz de usuario del software Element, la API y otras herramientas de gestión.

Un sistema de almacenamiento SolidFire incluye los siguientes componentes de hardware:

- **Cluster**: El concentrador del sistema de almacenamiento SolidFire que es una colección de nodos.
- **Nodes**: Los componentes de hardware agrupados en un cluster. Existen dos tipos de nodos:
  - Nodos de almacenamiento, que son servidores que contienen una colección de unidades
  - Nodos Fibre Channel (FC), que se utilizan para conectarse a clientes FC
- **Drives**: Se utiliza en los nodos de almacenamiento para almacenar datos para el clúster. Un nodo de almacenamiento contiene dos tipos de unidades:
  - Las unidades de metadatos de volúmenes almacenan información que define los volúmenes y otros objetos dentro de un clúster.
  - Las unidades de bloques almacenan bloques de datos para los volúmenes.



Puede gestionar, supervisar y actualizar el sistema mediante la interfaz de usuario web de Element y otras herramientas compatibles:

- "Interfaces de software de SolidFire"
- "SolidFire Active IQ"
- "Nodo de gestión para el software Element"
- "Servicios de gestión"

Direcciones URL comunes

Estas son las URL comunes que utiliza con un sistema de almacenamiento all-flash de SolidFire:

URL	Descripción
`https://[storage cluster MVIP address]`	Acceda a la interfaz de usuario del software NetApp Element.
`https://activeiq.solidfire.com`	Supervise los datos y reciba alertas sobre los cuellos de botella de rendimiento o los problemas potenciales del sistema.
`https://[management node IP address]`	Acceda a Hybrid Cloud Control de NetApp para actualizar sus servicios de gestión de actualizaciones e instalación del almacenamiento.

URL	Descripción
`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]/mnode`	Utilice la API DE REST de los servicios de gestión y otras funcionalidades desde el nodo de gestión."Leer más."
`https://[management node IP address]:9443`	Registre el paquete del plugin de vCenter en vSphere Web Client."Leer más."

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Interfaces de software de SolidFire

Puede gestionar un sistema de almacenamiento SolidFire mediante diferentes interfaces de software de NetApp Element y utilidades de integración.

Opciones

- Interfaz de usuario de software NetApp Element
- API de software NetApp Element
- Plugin de NetApp Element para vCenter Server
- Control del cloud híbrido de NetApp
- Las interfaces de usuario de los nodos de gestión
- Utilidades y herramientas de integración adicionales

Interfaz de usuario de software NetApp Element

Permite configurar el almacenamiento Element, supervisar la capacidad y el rendimiento del clúster y gestionar la actividad de almacenamiento en una infraestructura multi-tenant. Element es el sistema operativo de almacenamiento como pieza central de un clúster de SolidFire. El software Element se ejecuta de forma independiente en todos los nodos del clúster y permite que los nodos del clúster combinen los recursos que se presentan como un único sistema de almacenamiento a clientes externos. El software Element es responsable de toda la coordinación, escalado y gestión del clúster en su conjunto. La interfaz de software se creó sobre la API de Element.

"Gestionar el almacenamiento con el software Element"

API de software NetApp Element

Permite utilizar un conjunto de objetos, métodos y rutinas para gestionar el almacenamiento Element. La API de Element se basa en el protocolo JSON-RPC a través de HTTPS. Puede supervisar las operaciones de API en la interfaz de usuario de Element mediante la habilitación del registro de API, lo cual permite ver los métodos que se emiten al sistema. Puede activar tanto las solicitudes como las respuestas para ver cómo responde el sistema a los métodos que se emiten.

"Gestione el almacenamiento con la API de Element"

Plugin de NetApp Element para vCenter Server

Permite configurar y gestionar clústeres de almacenamiento que ejecutan el software Element mediante una interfaz alternativa para la interfaz de usuario de Element en VMware vSphere.

"Plugin de NetApp Element para vCenter Server"

Control del cloud híbrido de NetApp

Permite actualizar los servicios de gestión y almacenamiento de Element y gestionar los activos de almacenamiento mediante la interfaz de NetApp Hybrid Cloud Control.

"Gestione y supervise el almacenamiento con la información general de Hybrid Cloud Control de NetApp"

Las interfaces de usuario de los nodos de gestión

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 clúster, así como las pruebas y utilidades del sistema operativo. Desde la interfaz de usuario de la API DE REST, puede acceder a un menú de API relacionadas con el servicio que controlan las funcionalidades del sistema basadas en el servicio desde el nodo de gestión.

Utilidades y herramientas de integración adicionales

Si bien generalmente se gestiona el almacenamiento con NetApp Element, la API de NetApp Element y el plugin de NetApp Element para vCenter Server, puede usar utilidades y herramientas de integración adicionales para acceder al almacenamiento.

CLI de Element

"CLI de Element" Permite controlar un sistema de almacenamiento SolidFire mediante una interfaz de línea de comandos sin tener que utilizar la API de Element.

Herramientas de Element PowerShell

"Herramientas de Element PowerShell" Habilite usar una colección de funciones de Microsoft Windows PowerShell que utilizan la API de Element para gestionar un sistema de almacenamiento de SolidFire.

SDK de Element

"SDK de Element" Le permiten administrar el clúster de SolidFire mediante las siguientes herramientas:

- Element Java SDK: Permite a los programadores integrar la API de Element con el lenguaje de programación Java.
- Element .NET SDK: Permite a los programadores integrar la API de Element con la plataforma de programación .NET.
- Element Python SDK: Permite a los programadores integrar la API de elementos con el lenguaje de programación Python.

Suite de prueba de la API de SolidFire Postman

Permite a los programadores utilizar una colección de "Postman" Funciones que prueban las llamadas API de

Element.

Adaptador de replicación de almacenamiento de SolidFire

"Adaptador de replicación de almacenamiento de SolidFire" Se integra con VMware Site Recovery Manager (SRM) para permitir la comunicación con clústeres de almacenamiento de SolidFire replicados y ejecutar flujos de trabajo compatibles.

SolidFire Vro

"SolidFire Vro" Proporciona una forma cómoda de usar la API de Element para administrar su sistema de almacenamiento de SolidFire con VMware vRealize Orchestrator.

Proveedor VSS de SolidFire

"Proveedor VSS de SolidFire" Integra copias de sombra de VSS con copias de Snapshot de Element y clones.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

SolidFire Active IQ

"SolidFire Active IQ" es una herramienta web que proporciona vistas históricas actualizadas continuamente de los datos de todo el clúster. Es posible configurar alertas para eventos, umbrales o métricas específicos. SolidFire Active IQ le permite supervisar la capacidad y el rendimiento del sistema, así como mantenerse informado sobre el estado del clúster.

Puede encontrar la siguiente información sobre su sistema en SolidFire Active IQ:

- Número de nodos y estado de los nodos: En buen estado, sin conexión o fallo
- Representación gráfica de la CPU, el uso de memoria y la limitación de nodos
- Los detalles sobre el nodo, como el número de serie, la ubicación de la ranura en el chasis, el modelo y la versión del software NetApp Element que se ejecuta en el nodo de almacenamiento
- Información relacionada con la CPU y el almacenamiento sobre los equipos virtuales

Para obtener más información sobre SolidFire Active IQ, consulte "Documentación de SolidFire Active IQ".

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"
- "Herramientas del del sitio de soporte de NetApp para Active IQ"

Nodo de gestión para el software Element

La "Nodo de gestión (mNode)" Es una máquina virtual que se ejecuta en paralelo con uno o varios clústeres de almacenamiento basados en el 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.

El nodo de gestión 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.

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" se actualizan con frecuencia como paquetes de servicio.

Servicios de gestión para el almacenamiento all-flash de SolidFire

A partir de la versión Element 11.3, **servicios de administración** se alojan en el "nodo de gestión", permitiendo actualizaciones más rápidas de determinados servicios de software fuera de las versiones principales.

Los servicios de gestión proporcionan una funcionalidad de gestión centralizada y ampliada para el almacenamiento all-flash de SolidFire. Estos servicios incluyen "Control del cloud híbrido de NetApp", Telemetría del sistema de Active IQ, registro y actualizaciones de servicio, así como el servicio QoSSIOC para el plugin de Element para vCenter.

Más información acerca de "lanzamientos de servicios de gestión".

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 Element define varios roles de nodo para un clúster. Los tipos de roles de nodo son los siguientes:

- Nodo de gestión
- Nodo de almacenamiento
- Nodo Fibre Channel

estados de los nodos varía en función de la asociación del clúster.

Nodo de gestión

Un nodo de gestión es una máquina virtual que se usa para actualizar y proporcionar servicios del sistema, incluidos la supervisión y la telemetría, gestionar los activos y la configuración del clúster, ejecutar las pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la solución de problemas."Leer más"

Nodo de almacenamiento

Un nodo de almacenamiento SolidFire es un servidor que contiene una colección de unidades que se comunican entre sí a través de la interfaz de red Bond10G. 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 tienen las siguientes características:

- Cada nodo tiene un nombre único. Si un administrador no especifica un nombre de nodo, se usa el predeterminado, SF-XXXX, donde XXXX representa cuatro caracteres aleatorios generados por el sistema.
- Cada nodo tiene su propia caché de escritura de alto rendimiento de memoria de acceso aleatorio no volátil (NVRAM) con la que se mejora el rendimiento general del sistema y se reduce la latencia de escritura.
- Cada nodo 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.
- En cualquier momento que desee, se pueden añadir nodos al clúster o quitarlos sin tener que interrumpir el servicio.

Nodo Fibre Channel

Los nodos Fibre Channel de SolidFire proporcionan conectividad a un switch Fibre Channel, que puede conectarse a clientes Fibre Channel. Los nodos Fibre Channel funcionan como un conversor de protocolo entre los protocolos de iSCSI y Fibre Channel. Esto permite añadir conectividad de Fibre Channel a un clúster de SolidFire nuevo o actual.

Los nodos Fibre Channel tienen las siguientes características:

- Los switches Fibre Channel gestionan el estado de la estructura para proporcionar interconexiones optimizadas.
- El tráfico entre dos puertos solo fluye por los switches; no se transmite a ningún otro puerto.
- Un error en un puerto es un hecho aislado y no afecta al funcionamiento de otros puertos.
- Varias parejas de puertos pueden comunicarse de forma simultánea en una estructura.

estados de funcionamiento del nodo

Un nodo se puede encontrar en alguno de varios estados en función del nivel de configuración.

- **Disponible**

  El nodo no tiene ningún nombre de clúster asociado y aún no forma parte de un clúster.

- **Pendiente**

  El nodo está configurado y se puede añadir a un clúster designado.

  No es necesario autenticarse para acceder al nodo.

- **Activo pendiente**

  El sistema está instalando el software Element compatible en el nodo. Cuando finalice, el nodo se moverá al estado Active.

- **Activo**

  El nodo participa en un clúster.

  Es necesario autenticarse para modificar el nodo.

En cada uno de estos estados, algunos campos son de solo lectura.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

De clúster

Un clúster es el concentrador de un sistema de almacenamiento SolidFire y se compone de una colección de nodos. Debe haber al menos cuatro nodos en un clúster para que se puedan aprovechar las eficiencias de almacenamiento de SolidFire. Un clúster aparece en la red como un grupo lógico y se puede acceder a él como almacenamiento basado en bloques.

La creación de un nuevo clúster inicializa un nodo como propietario de comunicaciones para un clúster y establece comunicaciones de red para cada nodo del clúster. Este proceso solo se realiza una vez por cada clúster nuevo. Un clúster se puede crear con la API o la interfaz de usuario de Element.

Un clúster se puede escalar horizontalmente si se añaden otros nodos. Cuando se añade un nodo nuevo, no se produce ninguna interrupción del servicio y el clúster utiliza automáticamente el rendimiento y la capacidad del nodo nuevo.

Los administradores y los hosts pueden acceder al clúster mediante las direcciones IP virtuales. Las direcciones IP virtuales se pueden alojar en cualquier nodo del clúster. La IP virtual de gestión (MVIP) permite administrar el clúster a través de una conexión de 1 GbE, mientras que la IP virtual de almacenamiento (SVIP) permite acceder al host para realizar tareas de almacenamiento a través de una conexión de 10 GbE. Estas direcciones IP virtuales permiten conexiones coherentes independientemente del tamaño o la composición de un clúster de SolidFire. Cuando un nodo que aloja una dirección IP virtual falla, otro nodo del clúster comienza a alojar la dirección IP virtual.

> A partir de la versión 11.0 de Element, los nodos se pueden configurar con IPv4, IPv6 o ambas direcciones para su red de gestión. Esto se aplica a los nodos de almacenamiento y de gestión, excepto el nodo de gestión 11.3 y una versión posterior que no admite IPv6. Cuando se crea un clúster, solo se puede usar una dirección IPv4 o IPv6 única para la dirección MVIP y el tipo de dirección correspondiente se debe configurar en todos los nodos.

Más sobre los clústeres

- Clústeres de almacenamiento autoritativos

- Regla de las terceras partes
- Capacidad desaprovechada
- Eficiencia del almacenamiento
- Quórum del clúster de 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 desde "Interfaz de usuario del software Element".

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.

Regla de las terceras partes

Cuando se mezclan los tipos de nodo de almacenamiento en un clúster de almacenamiento SolidFire de NetApp, ningún nodo de almacenamiento puede contener más del 33 % de la capacidad total de clúster de almacenamiento.

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.

Eficiencia del almacenamiento

Los clústeres de almacenamiento SolidFire de NetApp utilizan la deduplicación, la compresión y el thin provisioning para reducir la cantidad de almacenamiento físico necesario para almacenar un volumen.

- **Compresión**

  La compresión reduce la cantidad de almacenamiento físico necesario en un volumen al combinar bloques de datos en grupos de compresión, cada uno de los cuales se almacena como un único bloque.

- **Deduplicación**

  La deduplicación reduce la cantidad de almacenamiento físico necesario en un volumen al eliminar los bloques de datos duplicados.

- **Thin Provisioning**

  Un volumen o LUN con thin provisioning es uno para el cual no se reserva almacenamiento por adelantado. En su lugar, el almacenamiento se asigna de forma dinámica conforme se necesita. El espacio libre se libera de nuevo al sistema de almacenamiento cuando se eliminan datos en el volumen o LUN

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.

Seguridad

Al utilizar su sistema de almacenamiento all-flash SolidFire, sus datos están protegidos por protocolos de seguridad estándares del sector.

Cifrado en reposo (hardware)

Todas las unidades de los nodos de almacenamiento pueden cifrar 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 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. La contraseña se necesita para desbloquear la unidad y, a menos que se quite la alimentación de la unidad o que la unidad esté bloqueada.

"Habilitar la función de cifrado de hardware en reposo" no afecta al rendimiento o la eficiencia del clúster. Si un nodo o una unidad habilitados para el cifrado se quitan de la configuración del clúster con la API de Element o la interfaz de usuario de Element, se deshabilitará el cifrado en reposo en las unidades. Una vez que se quita la unidad, esta se puede borrar de forma segura mediante el `SecureEraseDrives` Método API. Si se elimina por la fuerza un nodo o una unidad física, los datos permanecen protegidos por la contraseña del clúster y las claves de cifrado individuales de la unidad.

Cifrado en reposo (software)

Otro tipo de cifrado en reposo, el cifrado por software en reposo permite cifrar todos los datos que se escriben en los SSD de un clúster de almacenamiento. "Si está habilitada", cifra todos los datos escritos y descifra todos los datos leídos automáticamente en el software. El cifrado por software en reposo refleja la implementación de la unidad de cifrado automático (SED) en el hardware para proporcionar seguridad de datos en ausencia de SED.

En los clústeres de almacenamiento all-flash de SolidFire, el cifrado del software en reposo debe habilitarse durante la creación del clúster y no se puede deshabilitar una vez que se ha creado el clúster.

Tanto el cifrado en reposo basado en software como en hardware pueden utilizarse de forma independiente o en combinación con uno al otro.

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 externas, consulte "la puesta en marcha con la gestión de claves externas" documentación.

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 "la activación de la autenticación multifactor" documentación.

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

Los clústeres de almacenamiento SolidFire de NetApp admiten el cifrado, conforme a los requisitos del 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 de 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 "Cree un clúster que admita unidades FIPS".

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

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cuentas y permisos

Para administrar y proporcionar acceso a los recursos de almacenamiento del sistema, debe configurar cuentas para los recursos del sistema.

El almacenamiento de Element se puede crear y gestionar los siguientes tipos de cuentas:

- Cuentas de usuario de administrador para el clúster de almacenamiento de
- Las cuentas de usuario para acceder al volumen de almacenamiento
- Cuentas de usuario de clúster autorizadas sobre Hybrid Cloud Control de NetApp

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.

Puede hacerlo "gestione cuentas de administrador de clúster" Para crear, eliminar y editar cuentas de administrador de clúster, cambiar la contraseña de administrador de clúster y configurar los ajustes de LDAP para gestionar el acceso al sistema de los usuarios.

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.

Cuentas de usuario de clúster autoritativas

Las cuentas de usuario de clúster autorizadas 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.

Reducida

Volúmenes

El sistema de almacenamiento NetApp Element 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.

El almacenamiento de Element 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.

Cuando se incluye una opción para habilitar volúmenes persistentes, se incluye en los scripts de instalación y actualización "implementar un nodo de gestión nuevo". 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. 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

Volúmenes virtuales (vVols)

Los volúmenes virtuales de vSphere son un paradigma de almacenamiento para VMware que mueve gran parte de la gestión de almacenamiento de vSphere del sistema de almacenamiento a VMware vCenter. Con Virtual Volumes (vVols), puede asignar almacenamiento de acuerdo con los requisitos de cada equipo virtual.

Vinculaciones

El clúster de NetApp Element elige un extremo de protocolo adecuado, crea una vinculación que asocia el host ESXi y el volumen virtual con el extremo del protocolo, y devuelve la vinculación al host ESXi. Una vez enlazados, el host ESXi puede llevar a cabo operaciones de I/o con el volumen virtual vinculado.

Extremos de protocolo

Los hosts ESXi de VMware utilizan proxies lógicos de I/o, que se conocen como extremos de protocolo, para comunicarse con los volúmenes virtuales. Los hosts ESXi enlazan volúmenes virtuales con extremos de

protocolo para realizar operaciones de I/O. Cuando una máquina virtual en el host realiza una operación de I/o, el extremo de protocolo asociado dirige el I/o al volumen virtual con el que está enlazado.

Los extremos de protocolo de un clúster de NetApp Element funcionan como unidades lógicas administrativas SCSI. El clúster crea automáticamente cada extremo de protocolo. Para cada nodo de un clúster, se crea un extremo de protocolo correspondiente. Por ejemplo, un clúster de cuatro nodos tendrá cuatro extremos de protocolo.

ISCSI es el único protocolo compatible con el software NetApp Element. No se admite el protocolo Fibre Channel. Los usuarios no pueden eliminar ni modificar los extremos de protocolo. Tampoco se pueden asociar con una cuenta ni se pueden añadir a un grupo de acceso de volúmenes.

Contenedores de almacenamiento

Los contenedores de almacenamiento son construcciones lógicas que se asignan a cuentas de NetApp Element y se usan para crear informes y asignar recursos. Estos aprovechan la capacidad de almacenamiento sin configurar o añaden capacidades de almacenamiento que el sistema de almacenamiento puede ofrecer a los volúmenes virtuales. Un almacén de datos VVol que se crea en vSphere se asigna a un contenedor de almacenamiento individual. De forma predeterminada, un único contenedor de almacenamiento contiene todos los recursos disponibles del clúster de NetApp Element. Sin embargo, si se precisa una gestión granular para el multi-tenancy, se pueden crear varios contenedores.

Los contenedores de almacenamiento funcionan como cuentas tradicionales, y pueden contener volúmenes virtuales y volúmenes tradicionales a la vez. Se permite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para habilitar la funcionalidad de VVol. Durante la creación de VVol, se pueden detectar contenedores de almacenamiento en vCenter.

Proveedor de VASA

Para que vSphere esté al tanto de la función VVol en el clúster de NetApp Element, el administrador de vSphere debe registrar el proveedor VASA de NetApp Element en vCenter. El proveedor de VASA es la ruta de control fuera de banda entre vSphere y el clúster de Element. Es responsable de ejecutar solicitudes en el clúster de Element en nombre de vSphere, como la creación de máquinas virtuales, la puesta a disposición de vSphere de máquinas virtuales y la publicidad de funcionalidades de almacenamiento para vSphere.

El proveedor de VASA se ejecuta como parte del maestro de clústeres en el software Element. El maestro de clústeres es un servicio de alta disponibilidad que se conmuta por error a cualquier nodo del clúster según sea necesario. Si el maestro del clúster se conmuta al nodo de respaldo, el proveedor de VASA se mueve con él, garantizando que el proveedor de VASA tiene una alta disponibilidad. Todas las tareas de aprovisionamiento y gestión de almacenamiento utilizan el proveedor VASA, que gestiona los cambios necesarios en el clúster de Element.

> No se deben registrar más de un proveedor de VASA de NetApp Element en una sola instancia de vCenter. Cuando se añade un segundo proveedor de VASA NetApp Element, esto hace que no se pueda acceder a todos los almacenes de datos DE VVOL.

> La compatibilidad CON VASA de hasta 10 vCenter está disponible como revisión de actualización si ya se registró un proveedor de VASA en el para vCenter. Para instalar, siga las instrucciones del manifiesto VASA39 y descargue el archivo .tar.gz desde el "Descargas de software de NetApp" sitio. El proveedor VASA de NetApp Element utiliza un certificado de NetApp. Con este parche, vCenter utiliza el certificado sin modificar para admitir varias instancias de vCenter para que usen VASA y VVol. No modifique el certificado. VASA no admite los certificados SSL personalizados.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Los grupos de acceso de volúmenes

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 del almacenamiento SolidFire de NetApp permiten que los IQN de iniciadores de iSCSI o WWPN de Fibre Channel accedan a una colección de volúmenes. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo sin utilizar 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.

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.
- Para los clústeres Fibre Channel, un solo volumen puede pertenecer a hasta cuatro grupos de acceso.

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.

Protección de datos

Las funcionalidades de protección de datos incluyen replicación remota, snapshots de volúmenes, clonado de volúmenes, Protection Domains y alta disponibilidad con la tecnología Double Helix.

La protección de datos de almacenamiento de Element incluye los siguientes conceptos:

- Tipos de replicación remota
- Snapshots de volumen para proteger los datos

- Clones de volúmenes
- Información general del proceso de backup y restauración para el almacenamiento Element
- Dominios de protección
- Dominios de protección personalizados
- 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

Para obtener más información, 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.

El software NetApp Element 10.1 y versiones posteriores admite la funcionalidad de SnapMirror para copiar y restaurar copias Snapshot con sistemas ONTAP.

Los sistemas que ejecutan Element 10.1 y versiones posteriores incluyen el código que puede comunicarse directamente con SnapMirror en sistemas ONTAP que ejecutan 9.3 o posterior. La API de Element proporciona métodos para habilitar la funcionalidad de SnapMirror en clústeres, volúmenes y copias de Snapshot. Además, la interfaz de usuario de Element incluye la funcionalidad para gestionar las relaciones de SnapMirror entre el software Element y los sistemas ONTAP.

A partir de los sistemas Element 10.3 y ONTAP 9.4, es posible replicar volúmenes originados por ONTAP en volúmenes de Element en casos de uso específicos con funcionalidad limitada.

Para obtener más información, consulte la documentación de ONTAP.

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 copias de Snapshot de un clúster de Element en un almacén de objetos externo o en otro clúster de Element. 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 del proceso de backup y restauración para el almacenamiento Element

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 fallen, al tiempo que se mantiene la disponibilidad de los datos. Los dominios de protección permiten que un clúster de almacenamiento se repare automáticamente de la pérdida de un chasis (afinidad de chasis) o de todo un dominio (grupo de chasis).

Es posible habilitar manualmente la supervisión de dominios de protección mediante el punto de extensión NetApp Element Configuration en el plugin de NetApp Element para vCenter Server. Puede seleccionar un umbral para Protection Domain a partir de dominios de nodo o de chasis. También es posible habilitar la supervisión de Protection Domain mediante la API o la interfaz de usuario web de Element.

Un diseño de Protection Domain asigna cada nodo a un dominio de protección específico.

Se admiten dos diseños diferentes de Protection Domain, denominados niveles de Protection Domain.

- 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.

Cuando crea un clúster nuevo, si utiliza nodos de almacenamiento que residen en un chasis compartido, puede que desee considerar diseñar la protección contra fallos en el nivel del chasis mediante la función Protection Domains.

Dominios de protección personalizados

Puede definir un diseño personalizado de Protection Domain que coincida con el diseño de nodo y chasis específicos, y donde cada nodo está asociado a un y solo un 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.

Cuando se configuran los dominios de protección personalizados de un clúster, se pueden ver tres niveles posibles de protección en la consola de la interfaz de usuario web de Element:

- No protegido: El clúster de almacenamiento no está protegido ante el fallo de uno de sus dominios de protección personalizados. Para solucionarlo, añada más capacidad de almacenamiento al clúster o vuelva a configurar los dominios de protección personalizados del clúster para proteger el clúster de una posible pérdida de datos.
- Tolerancia a fallos: El clúster de almacenamiento tiene suficiente capacidad libre para evitar la pérdida de datos tras el fallo de uno de sus dominios de protección personalizados.
- Fault resiliente: El clúster de almacenamiento tiene suficiente capacidad libre para recuperarse tras el fallo de uno de sus dominios de protección personalizados. Una vez completado el proceso de reparación, el clúster se protegerá de la pérdida de datos si otros dominios fallan.

Si se asigna más de un dominio de protección personalizado, cada subsistema asignará duplicados a dominios de protección personalizados separados. 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.

Puede configurar dominios de protección personalizados mediante los siguientes métodos API:

- "GetProtectionDomainLayout" - Muestra en qué chasis y en qué dominio de protección personalizado se encuentra cada nodo.
- "SetProtectionDomainLayout" - Permite asignar un dominio de protección personalizado a cada nodo.

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.

Rendimiento y calidad del 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.

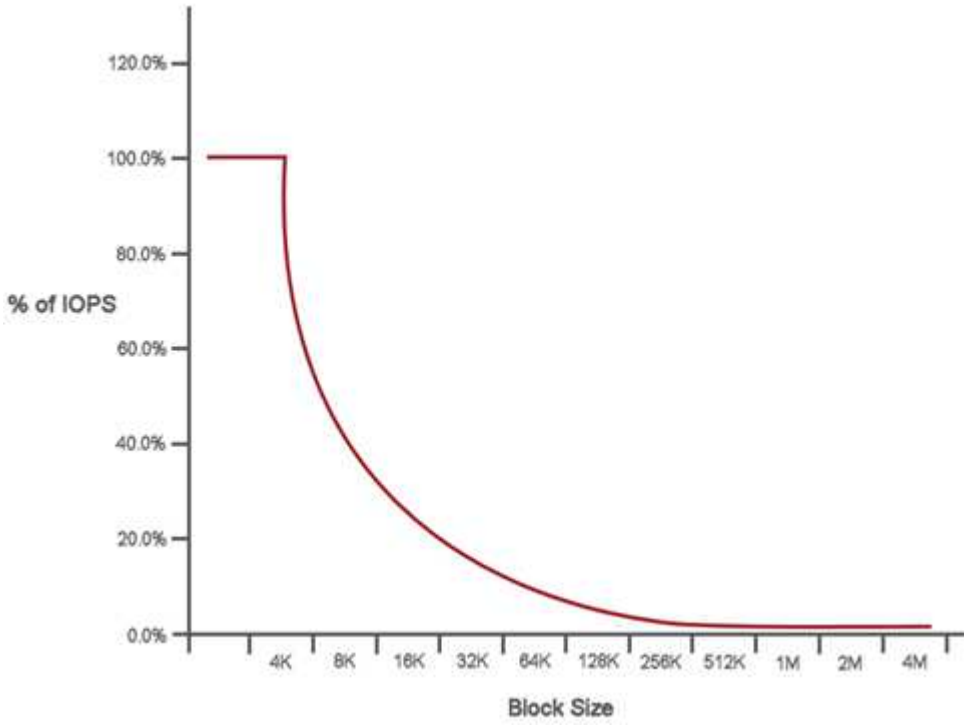
Rendimiento de la calidad de servicio

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

- "Documentación de SolidFire y el software Element"

Información de copyright

Información de la marca comercial