Conceptos

Element Software

NetApp
November 18, 2025

Tabla de contenidos

Conceptos

Aprende conceptos básicos relacionados con el software Element.

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

Descripción general del producto

Un sistema de almacenamiento all-flash SolidFire se compone de componentes de hardware discretos (unidades y nodos) que se combinan en un único conjunto de recursos de almacenamiento. Este clúster unificado se presenta como un único sistema de almacenamiento para uso de clientes externos y se gestiona con el software NetApp Element .

Utilizando la interfaz Element, la API u otras herramientas de administración, puede supervisar la capacidad y el rendimiento del almacenamiento del clúster SolidFire y administrar la actividad de almacenamiento en una infraestructura multiinquilino.

Características de SolidFire

Un sistema Solidfire ofrece las siguientes características:

- Ofrece almacenamiento de alto rendimiento para su infraestructura de nube privada a gran escala.
- Proporciona una escala flexible que le permite satisfacer las necesidades de almacenamiento cambiantes.
- Utiliza una interfaz de software Element para la gestión del almacenamiento basada en API.
- Garantiza el rendimiento mediante políticas de calidad de servicio.
- Incluye balanceo de carga automático en todos los nodos del clúster.
- Reequilibra los clústeres automáticamente cuando se añaden o se eliminan nodos.

Despliegue de SolidFire

Utilice nodos de almacenamiento proporcionados por NetApp e integrados con el software NetApp Element .

"Descripción general de la arquitectura de almacenamiento totalmente flash de SolidFire"

Encuentra más información

- "Plugin de NetApp Element para vCenter Server"

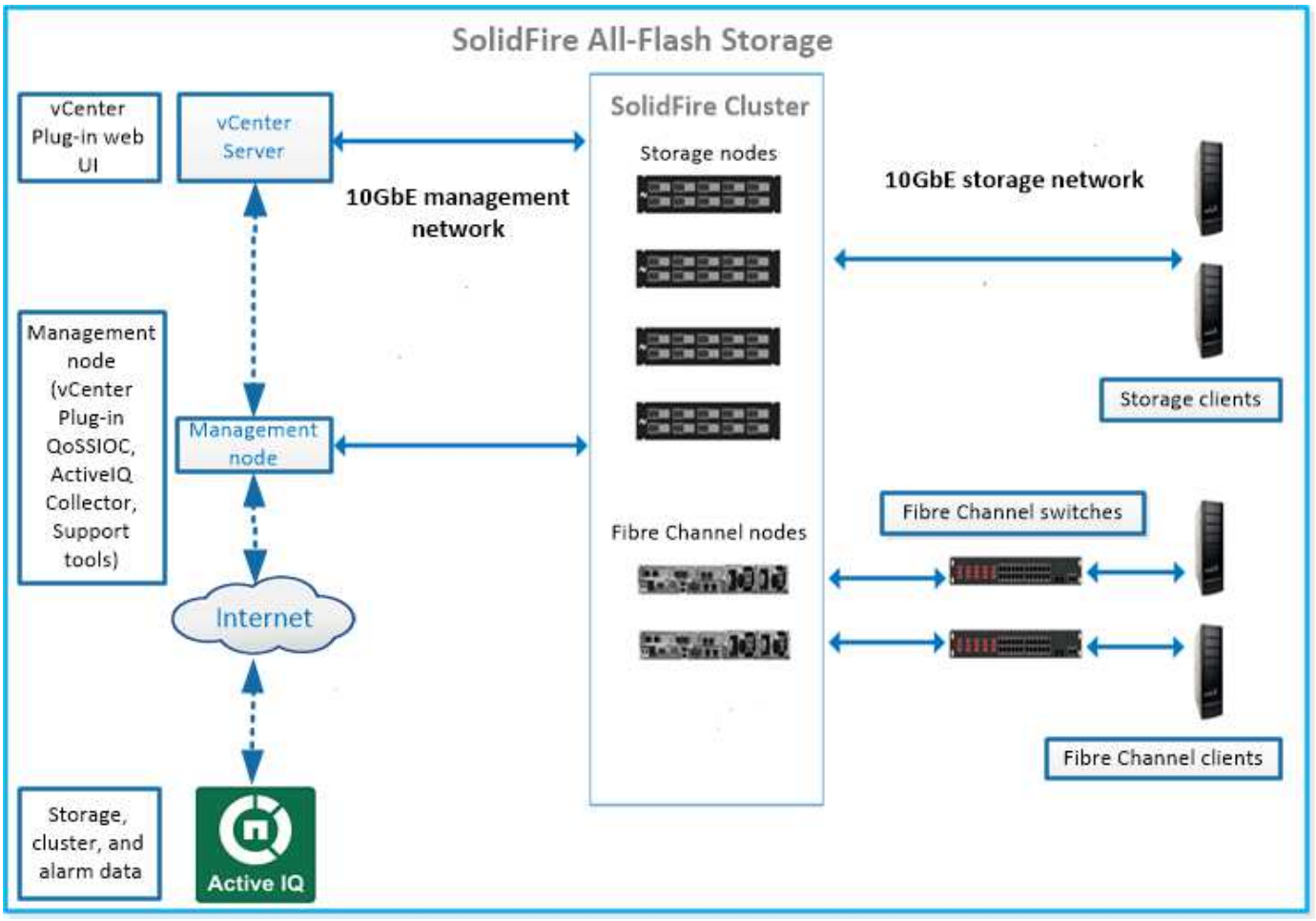
Arquitectura y componentes

Conozca la arquitectura de SolidFire

Un sistema de almacenamiento all-flash SolidFire se compone de componentes de hardware discretos (unidades y nodos) que se combinan en un conjunto de recursos de almacenamiento con el software NetApp Element ejecutándose de forma independiente en cada nodo. Este sistema de almacenamiento único se gestiona como una sola 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:

- **Clúster**: El núcleo del sistema de almacenamiento SolidFire que es una colección de nodos.
- **Nodos**: Los componentes de hardware agrupados en un clúster. 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
- **Unidades**: Se utilizan 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 volumen almacenan información que define los volúmenes y otros objetos dentro de un clúster.
  - Las unidades de bloque almacenan bloques de datos para volúmenes.



Puede administrar, supervisar y actualizar el sistema utilizando la interfaz web de Element y otras herramientas compatibles:

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

URL comunes

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

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 cualquier cuello de botella en el rendimiento o posibles problemas del sistema.
`https://[management node IP address]`	Acceda a NetApp Hybrid Cloud Control para actualizar su instalación de almacenamiento y los servicios de administración de actualizaciones.

URL	Descripción
`https://[IP address]:442`	Desde la interfaz de usuario de cada nodo, acceda a la configuración de red y clúster y utilice las pruebas y utilidades del sistema."Más información."
`https://[management node IP address]/mnode`	Utilice la API REST de servicios de gestión y otras funcionalidades del nodo de gestión."Más información."
`https://[management node IP address]:9443`	Registre el paquete de complementos de vCenter en el cliente web de vSphere."Más información."

Encuentra más información

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

interfaces de software SolidFire

Puede administrar un sistema de almacenamiento SolidFire utilizando diferentes interfaces de software y utilidades de integración de NetApp Element .

Opciones

- Interfaz de usuario del software NetApp Element
- API del software NetApp Element
- Plugin de NetApp Element para vCenter Server
- Control de nube híbrida de NetApp
- interfaces de usuario de nodos de administración
- Utilidades y herramientas de integración adicionales

Interfaz de usuario del software NetApp Element

Le permite configurar el almacenamiento de Element, supervisar la capacidad y el rendimiento del clúster y gestionar la actividad de almacenamiento en una infraestructura multiinquilino. Element es el sistema operativo de almacenamiento que constituye el núcleo de un clúster SolidFire . El software Element se ejecuta de forma independiente en todos los nodos del clúster y permite que los nodos del clúster combinen recursos que se presentan como un único sistema de almacenamiento a los clientes externos. El software Element es responsable de toda la coordinación del clúster, la escalabilidad y la gestión del sistema en su conjunto. La interfaz de software está construida sobre la API de Element.

"Gestiona el almacenamiento con el software Element."

API del software NetApp Element

Te permite utilizar un conjunto de objetos, métodos y rutinas para gestionar el almacenamiento de elementos. La API de Element se basa en el protocolo JSON-RPC sobre HTTPS. Puedes supervisar las operaciones de la API en la interfaz de usuario de Element habilitando el registro de la API; esto te permite ver los métodos que se están enviando al sistema. Puedes habilitar tanto las solicitudes como las respuestas para ver cómo responde el sistema a los métodos que se emiten.

"Gestiona el almacenamiento con la API de Element"

Plugin de NetApp Element para vCenter Server

Le permite configurar y administrar clústeres de almacenamiento que ejecutan el software Element utilizando una interfaz alternativa para la interfaz de usuario de Element dentro de VMware vSphere.

"Plugin de NetApp Element para vCenter Server"

Control de nube híbrida de NetApp

Le permite actualizar los servicios de almacenamiento y administración de Element y administrar los activos de almacenamiento utilizando la interfaz de NetApp Hybrid Cloud Control.

"Administre y supervise el almacenamiento con NetApp Hybrid Cloud Control."

interfaces de usuario de nodos de administración

El nodo de administración contiene dos interfaces de usuario: una interfaz para administrar servicios basados en REST y una interfaz por nodo para administrar la configuración de red y clúster, así como las pruebas y utilidades del sistema operativo. Desde la interfaz de usuario de la API REST, puede acceder a un menú de API relacionadas con el servicio que controlan la funcionalidad del sistema basado en servicios desde el nodo de administración.

Utilidades y herramientas de integración adicionales

Aunque normalmente se administra el almacenamiento con NetApp Element, NetApp Element API y NetApp Element Plug-in para vCenter Server, se pueden utilizar utilidades y herramientas de integración adicionales para acceder al almacenamiento.

CLI de Element

"CLI de Element"te permite controlar un sistema de almacenamiento SolidFire mediante una interfaz de línea de comandos sin necesidad de utilizar la API de Element.

Herramientas de PowerShell de Element

"Herramientas de PowerShell de Element"le permite utilizar una colección de funciones de Microsoft Windows PowerShell que utilizan la API de Element para administrar un sistema de almacenamiento SolidFire .

SDK de elementos

"SDK de elementos"le permiten administrar su clúster SolidFire utilizando estas 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 Element con el lenguaje de programación Python.

Suite de pruebas de la API Postman de SolidFire

Permite a los programadores utilizar una colección de"Cartero" funciones que prueban las llamadas a la 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 SolidFire replicados y ejecutar flujos de trabajo compatibles.

SolidFire vRO

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

Proveedor VSS de SolidFire

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

Encuentra más información

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

SolidFire Active IQ

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

En SolidFire Active IQ encontrará la siguiente información sobre su sistema:

- Número de nodos y estado de los nodos: sano, fuera de línea o con fallos.
- Representación gráfica del uso de CPU y memoria, y de la limitación de nodos.
- 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 de las máquinas virtuales

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

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"
- **Sitio de soporte de NetApp › Herramientas para Active IQ**

Nodo de gestión para el software Element

El"nodo de gestión (mNode)" es una máquina virtual que se ejecuta en paralelo con uno o más clústeres de almacenamiento basados en software Element. Se utiliza para

actualizar y proporcionar servicios del sistema, incluyendo monitoreo y telemetría, administrar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso al soporte de NetApp para la resolución de problemas.

El nodo de administración interactúa con un clúster de almacenamiento para realizar acciones de administración, pero no es miembro del clúster de almacenamiento. Los nodos de gestión recopilan periódicamente información sobre el clúster a través de llamadas a la API y envían esta información a Active IQ para la monitorización remota (si está habilitada). Los nodos de gestión también son responsables de coordinar las actualizaciones de software de los nodos del clúster.

A partir de la versión Element 11.3, el nodo de administración funciona como un host de microservicios, lo que permite actualizaciones más rápidas de servicios de software seleccionados fuera de las versiones principales. Estos microservicios o"servicios de administración" se actualizan con frecuencia como paquetes de servicios.

Servicios de gestión para almacenamiento all-flash SolidFire

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

Los servicios de gestión proporcionan funcionalidades de gestión centralizadas y extendidas para el almacenamiento all-flash SolidFire . Estos servicios incluyen"Control de nube híbrida de NetApp" , Telemetría, registro y actualizaciones de servicio del sistema Active IQ , así como el servicio QoSSIOC para el complemento Element para vCenter.

Obtenga más información sobre"Lanzamientos de servicios de gestión" .

Nodos

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

El software NetApp Element define diferentes roles de nodo para un clúster. Los tipos de roles de nodo son los siguientes:

- Nodo de gestión
- Nodo de almacenamiento
- Nodo de canal de fibra

Estados de los nodosvarían según la asociación del grupo.

Nodo de gestión

Un nodo de administración es una máquina virtual que se utiliza para actualizar y proporcionar servicios del sistema, incluidos el monitoreo y la telemetría, administrar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema y habilitar el acceso del soporte de NetApp para la resolución de problemas."Más información"

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 del nodo contienen espacio de bloques y metadatos para el almacenamiento y la gestión de datos. Cada nodo contiene una imagen de fábrica del 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 utilizará por defecto SF-XXXX, donde XXXX son cuatro caracteres aleatorios generados por el sistema.
- Cada nodo tiene su propia memoria caché de escritura de memoria de acceso aleatorio no volátil (NVRAM) de alto rendimiento para mejorar el rendimiento general del sistema y reducir la latencia de escritura.
- Cada nodo está conectado a dos redes, una de almacenamiento y otra de gestión, cada una con dos enlaces independientes para redundancia y rendimiento. Cada nodo requiere una dirección IP en cada red.
- Puede crear un clúster con nuevos nodos de almacenamiento o agregar nodos de almacenamiento a un clúster existente para aumentar la capacidad y el rendimiento del almacenamiento.
- Puede agregar o eliminar nodos del clúster en cualquier momento sin interrumpir el servicio.

Nodo de canal de fibra

Los nodos Fibre Channel de SolidFire proporcionan conectividad a un conmutador Fibre Channel, al que puede conectar clientes Fibre Channel. Los nodos Fibre Channel actúan como un convertidor de protocolo entre los protocolos Fibre Channel e iSCSI; esto le permite agregar conectividad Fibre Channel a cualquier clúster SolidFire nuevo o existente.

Los nodos Fibre Channel tienen las siguientes características:

- Los conmutadores Fibre Channel gestionan el estado de la estructura, proporcionando interconexiones optimizadas.
- El tráfico entre dos puertos fluye únicamente a través de los conmutadores; no se transmite a ningún otro puerto.
- El fallo de un puerto es aislado y no afecta al funcionamiento de los demás puertos.
- En una estructura, varios pares de puertos pueden comunicarse simultáneamente.

Estados de operación de los nodos

Un nodo puede estar en uno de varios estados dependiendo del nivel de configuración.

- **Disponible**

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

- **Pendiente**

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

  No se requiere autenticación para acceder al nodo.

- **Activo pendiente**

  El sistema está en proceso de instalar el software Element compatible en el nodo. Una vez completado, el nodo pasará al estado Activo.

- **Activo**

  El nodo participa en un clúster.

  Se requiere autenticación para modificar el nodo.

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

Encuentra más información

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

Clústeres

Un clúster es el centro de un sistema de almacenamiento SolidFire y está formado por una colección de nodos. Para aprovechar al máximo la eficiencia del almacenamiento de SolidFire , debe tener al menos cuatro nodos en un clúster. Un clúster aparece en la red como un único grupo lógico y, por lo tanto, se puede acceder a él como almacenamiento en bloque.

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

Puedes escalar horizontalmente un clúster añadiendo nodos adicionales. Al agregar un nuevo nodo, no se interrumpe el servicio y el clúster utiliza automáticamente el rendimiento y la capacidad del nuevo nodo.

Los administradores y los anfitriones pueden acceder al clúster utilizando direcciones IP virtuales. Cualquier nodo del clúster puede alojar las direcciones IP virtuales. La IP virtual de gestión (MVIP) permite la gestión del clúster a través de una conexión de 1 GbE, mientras que la IP virtual de almacenamiento (SVIP) permite el acceso del host al almacenamiento a través de una conexión de 10 GbE. Estas direcciones IP virtuales permiten conexiones consistentes independientemente del tamaño o la composición de un clúster SolidFire . Si falla un nodo que aloja una dirección IP virtual, 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 direcciones IPv4, IPv6 o ambas para su red de administración. Esto se aplica tanto a los nodos de almacenamiento como a los nodos de administración, excepto al nodo de administración 11.3 y posteriores, que no admiten IPv6. Al crear un clúster, solo se puede usar una única dirección IPv4 o IPv6 para MVIP y el tipo de dirección correspondiente debe configurarse en todos los nodos.

Más sobre clústeres

- clústeres de almacenamiento autorizados

- Regla de los tercios
- capacidad varada
- Eficiencia de almacenamiento
- quórum del clúster de almacenamiento

clústeres de almacenamiento autorizados

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

Si su nodo de administración solo tiene un clúster de almacenamiento, entonces ese es el clúster autoritativo. Si su nodo de administración tiene dos o más clústeres de almacenamiento, uno de esos clústeres se asigna como clúster autorizado y solo los usuarios de ese clúster pueden iniciar sesión en NetApp Hybrid Cloud Control. Para averiguar qué clúster es el clúster autorizado, puede utilizar el `GET /mnode/about` API. En la respuesta, la dirección IP en el `token_url` El campo es la dirección IP virtual de gestión (MVIP) del clúster de almacenamiento autoritativo. Si intenta iniciar sesión en NetApp Hybrid Cloud Control como un usuario que no pertenece al clúster autorizado, el intento de inicio de sesión fallará.

Muchas funciones de NetApp Hybrid Cloud Control están diseñadas para funcionar con múltiples clústeres de almacenamiento, pero la autenticación y la autorización tienen limitaciones. La limitación en torno a la autenticación y autorización es que el usuario del clúster autoritativo puede ejecutar acciones en otros clústeres vinculados a NetApp Hybrid Cloud Control incluso si no es usuario en los otros clústeres de almacenamiento.

Antes de proceder a administrar varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados estén definidos en todos los demás clústeres de almacenamiento con los mismos permisos. Puedes gestionar los usuarios desde el"Interfaz de usuario del software Element" .

Ver"crear y administrar activos de clúster de almacenamiento" Para obtener más información sobre cómo trabajar con los recursos del clúster de almacenamiento del nodo de administración.

Regla de los tercios

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

capacidad varada

Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esta situación se mantendrá hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto suceda. Cuando un nodo queda aislado, se genera un fallo de clúster apropiado.

Eficiencia de almacenamiento

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

- **Compresión**

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

- **Desduplicación**

  La deduplicación reduce la cantidad de almacenamiento físico necesario para un volumen al descartar bloques de datos duplicados.

- **Aprovisionamiento ligero**

  Un volumen de aprovisionamiento ligero o LUN es aquel para el cual no se reserva almacenamiento por adelantado. En cambio, el almacenamiento se asigna dinámicamente, según se necesite. Cuando se eliminan datos del volumen o LUN, el espacio libre se devuelve al sistema de almacenamiento.

quórum del clúster de almacenamiento

El software Element crea un clúster de almacenamiento a partir de nodos seleccionados, que mantiene una base de datos replicada de la configuración del clúster. Se requiere un mínimo de tres nodos para participar en el conjunto de clústeres para mantener el quórum y garantizar la resiliencia del clúster.

Seguridad

Cuando utiliza su sistema de almacenamiento totalmente flash SolidFire , sus datos están protegidos por protocolos de seguridad estándar del sector.

Cifrado en reposo (hardware)

Todas las unidades en los nodos de almacenamiento son capaces de utilizar el cifrado AES de 256 bits a nivel de unidad. Cada unidad tiene su propia clave de cifrado, que se crea cuando la unidad se inicializa por primera vez. Al habilitar la función de cifrado, se crea una contraseña para todo el clúster y, a continuación, se distribuyen fragmentos de la contraseña a todos los nodos del clúster. Ningún nodo individual almacena la contraseña completa. La contraseña se utiliza entonces para proteger con contraseña todo el acceso a las unidades. La contraseña es necesaria para desbloquear la unidad y luego no se necesita a menos que se desconecte la alimentación de la unidad o se bloquee la unidad.

"Habilitar la función de cifrado de hardware en reposo"No afecta al rendimiento ni a la eficiencia del clúster. Si se elimina una unidad o nodo con cifrado habilitado de la configuración del clúster mediante la API de Element o la interfaz de usuario de Element, se deshabilitará el cifrado en reposo en las unidades. Una vez extraída la unidad, se puede borrar de forma segura utilizando el método `SecureEraseDrives` Método API. Si se extrae por la fuerza una unidad o nodo físico, los datos permanecen protegidos por la contraseña de todo el clúster y las claves de cifrado individuales de la unidad.

Cifrado en reposo (software)

Otro tipo de cifrado en reposo, el cifrado en reposo por software, permite cifrar todos los datos escritos en las unidades SSD de un clúster de almacenamiento. "Cuando está habilitado" Encripta todos los datos escritos y desencripta todos los datos leídos automáticamente en el software. El cifrado de software en reposo reproduce la implementación de la unidad de autocifrado (SED) en el hardware para proporcionar seguridad de los datos en ausencia de SED.

Para los clústeres de almacenamiento all-flash SolidFire , el cifrado de software en reposo debe habilitarse durante la creación del clúster y no puede deshabilitarse después de que se haya creado el clúster.

Tanto el cifrado en reposo basado en software como el basado en hardware pueden utilizarse de forma independiente o en combinación entre sí.

Gestión de claves externas

Puede configurar el software Element para que utilice un servicio de administración de claves (KMS) de terceros compatible con KMIP para administrar las claves de cifrado del clúster de almacenamiento. Cuando habilita esta función, la clave de cifrado de la contraseña de acceso a la unidad de todo el clúster de almacenamiento es administrada por un KMS que usted especifica.

Element puede utilizar los siguientes servicios de gestión de claves:

- Gemalto SafeNet KeySecure
- SafeNet en KeySecure
- Control de teclas HyTrust
- Administrador de seguridad de datos de Vormetric
- Administrador del ciclo de vida de las claves de seguridad de IBM

Para obtener más información sobre la configuración de la administración de claves externas, consulte"Primeros pasos con la administración de claves externas" documentación.

Autenticación multifactor

La autenticación multifactor (MFA) le permite exigir a los usuarios que presenten varios tipos de evidencia para autenticarse con la interfaz de usuario web de NetApp Element o la interfaz de usuario del nodo de almacenamiento al iniciar sesión. Puede configurar Element para que acepte únicamente la autenticación multifactor para los inicios de sesión, integrándose con su sistema de gestión de usuarios y proveedor de identidad existentes. Puedes configurar Element para que se integre con un proveedor de identidad SAML 2.0 existente que puede aplicar múltiples esquemas de autenticación, como contraseña y mensaje de texto, contraseña y mensaje de correo electrónico u otros métodos.

Puede combinar la autenticación multifactor con proveedores de identidad (IdP) comunes compatibles con SAML 2.0, como Microsoft Active Directory Federation Services (ADFS) y Shibboleth.

Para configurar la autenticación multifactor (MFA), consulte "habilitar la autenticación multifactor" documentación.

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

Los clústeres de almacenamiento NetApp SolidFire admiten cifrado que cumple con los requisitos del Estándar Federal de Procesamiento de Información (FIPS) 140-2 para módulos criptográficos. Puede habilitar el cumplimiento de FIPS 140-2 en su clúster SolidFire tanto para las comunicaciones HTTPS como para el cifrado de unidades.

Cuando habilita el modo de funcionamiento FIPS 140-2 en su clúster, este activa el Módulo de Seguridad Criptográfica de NetApp (NCSM) y aprovecha el cifrado certificado FIPS 140-2 Nivel 1 para todas las comunicaciones a través de HTTPS con la interfaz de usuario y la API de NetApp Element . Usted usa el `EnableFeature` API de elementos con la `fips` Parámetro para habilitar el cifrado HTTPS FIPS 140-2. En

clústeres de almacenamiento con hardware compatible con FIPS, también puede habilitar el cifrado de unidad FIPS para datos en reposo mediante `EnableFeature` API de elementos con la `FipsDrives` parámetro.

Para obtener más información sobre cómo preparar un nuevo clúster de almacenamiento para el cifrado FIPS 140-2, 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"API de elementos EnableFeature" .

Para más información

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

Cuentas y permisos

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

Con el almacenamiento de Element, puede crear y administrar los siguientes tipos de cuentas:

- Cuentas de usuario administrador para el clúster de almacenamiento
- Cuentas de usuario para el acceso al volumen de almacenamiento
- Cuentas de usuario de clúster autorizadas para NetApp Hybrid Cloud Control

cuentas de administrador de clúster de almacenamiento

En un clúster de almacenamiento que ejecuta el software NetApp Element, pueden existir dos tipos de cuentas de administrador:

- **Cuenta de administrador principal del clúster**: Esta cuenta de administrador se crea cuando se crea el clúster. Esta cuenta es la cuenta administrativa principal con el nivel más alto de acceso al clúster. Esta cuenta es análoga a un usuario root en un sistema Linux. Puedes 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 asignadas a cada cuenta de administrador del clúster se utilizan para autenticar las solicitudes de API y de la interfaz de usuario de Element dentro del sistema de almacenamiento.

> Se requiere una cuenta de administrador de clúster local (no LDAP) para acceder a los nodos activos de un clúster a través de la interfaz de usuario por nodo. No se requieren credenciales de cuenta para acceder a un nodo que aún no forma parte de un clúster.

Puede"administrar cuentas de administrador de clúster" mediante la creación, eliminación y edición de cuentas de administrador de clúster, el cambio de la contraseña de administrador de clúster y la configuración de los ajustes LDAP para gestionar el acceso al sistema para 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 NetApp Element . Se requiere al menos una cuenta de usuario antes de poder crear un

volumen.

Cuando se crea un volumen, este se asigna a una cuenta. Si ha creado un volumen virtual, la cuenta es el contenedor de almacenamiento.

Aquí hay algunas consideraciones adicionales:

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

cuentas de usuario de clúster autorizadas

Las cuentas de usuario autorizadas del clúster pueden autenticarse frente a cualquier recurso de almacenamiento asociado con la instancia de nodos y clústeres de NetApp Hybrid Cloud Control. Con esta cuenta, puede administrar volúmenes, cuentas, grupos de acceso y más en todos los clústeres.

Las cuentas de usuario autorizadas se gestionan desde la opción "Gestión de usuarios" del menú superior derecho en NetApp Hybrid Cloud Control.

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

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

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

Si bien muchas funciones de NetApp Hybrid Cloud Control funcionan con múltiples clústeres de almacenamiento, la autenticación y la autorización tienen limitaciones necesarias. La limitación en torno a la autenticación y autorización es que los usuarios del clúster autoritativo pueden ejecutar acciones en otros clústeres vinculados a NetApp Hybrid Cloud Control incluso si no son usuarios de los otros clústeres de almacenamiento. Antes de proceder a administrar varios clústeres de almacenamiento, debe asegurarse de que los usuarios definidos en los clústeres autorizados estén definidos en todos los demás clústeres de almacenamiento con los mismos permisos. Puede administrar los usuarios desde NetApp Hybrid Cloud Control.

Cuentas de volumen

Las cuentas específicas de volumen son específicas únicamente del clúster de almacenamiento en el que se crearon. Estas cuentas permiten establecer permisos en volúmenes específicos de la red, pero no tienen efecto fuera de esos volúmenes.

Las cuentas de volumen se gestionan dentro de la tabla de volúmenes de control de la nube híbrida de NetApp .

Almacenamiento

Volúmenes

El sistema de almacenamiento NetApp Element aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que acceden a través de la red los clientes iSCSI o Fibre Channel.

El almacenamiento de elementos le permite crear, ver, editar, eliminar, clonar, realizar copias de seguridad o restaurar volúmenes para cuentas de usuario. También puede administrar cada volumen en un clúster y agregar o eliminar volúmenes en grupos de acceso a volúmenes.

Volúmenes persistentes

Los volúmenes persistentes permiten almacenar los datos de configuración del nodo de administración en un clúster de almacenamiento específico, 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 administración. Los volúmenes persistentes son una configuración de nodo de administración opcional, pero recomendada.

En los scripts de instalación y actualización se incluye una opción para habilitar volúmenes persistentes cuando"despliegue de 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 administración para la máquina virtual del nodo de administración del host, la cual persiste más allá de la vida útil de la máquina virtual. Si se pierde el nodo de administración, una máquina virtual de nodo de administración de reemplazo puede reconectarse y recuperar los datos de configuración de la máquina virtual perdida.

La funcionalidad de volúmenes persistentes, si está habilitada durante la instalación o actualización, crea automáticamente varios volúmenes. Estos volúmenes, al igual que cualquier volumen basado en software Element, se pueden visualizar mediante la interfaz web del software Element, el complemento NetApp Element para vCenter Server o la API, según sus preferencias e instalación. Los volúmenes persistentes deben estar activos y funcionando con una conexión iSCSI al nodo de administración para mantener los datos de configuración actuales que se pueden utilizar para la recuperación.

> Los volúmenes persistentes asociados a los servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine los volúmenes ni sus cuentas asociadas.

Volúmenes virtuales (vVols)

vSphere Virtual Volumes es un paradigma de almacenamiento para VMware que traslada gran parte de la gestión del almacenamiento de vSphere desde el sistema de almacenamiento a VMware vCenter. Con los volúmenes virtuales (vVols), puede asignar almacenamiento de acuerdo con los requisitos de cada máquina virtual.

Fijaciones

El clúster NetApp Element elige un punto de conexión de protocolo óptimo, crea un enlace que asocia el host ESXi y el volumen virtual con el punto de conexión de protocolo y devuelve el enlace al host ESXi. Una vez enlazado, el host ESXi puede realizar operaciones de E/S con el volumen virtual enlazado.

puntos finales del protocolo

Los hosts VMware ESXi utilizan proxies de E/S lógicos conocidos como puntos finales de protocolo para comunicarse con volúmenes virtuales. Los hosts ESXi enlazan volúmenes virtuales a puntos finales de protocolo para realizar operaciones de E/S. Cuando una máquina virtual en el host realiza una operación de E/S, el punto final del protocolo asociado dirige la E/S al volumen virtual con el que está emparejado.

Los puntos finales del protocolo en un clúster NetApp Element funcionan como unidades lógicas administrativas SCSI. El clúster crea automáticamente cada punto final del protocolo. Para cada nodo de un clúster, se crea un punto final de protocolo correspondiente. Por ejemplo, un clúster de cuatro nodos tendrá cuatro puntos finales de protocolo.

iSCSI es el único protocolo compatible con el software NetApp Element . El protocolo Fibre Channel no es compatible. Los puntos de conexión del protocolo no pueden ser eliminados ni modificados por un usuario, no están asociados a una cuenta y no pueden agregarse a un grupo de acceso por volumen.

contenedores de almacenamiento

Los contenedores de almacenamiento son construcciones lógicas que se asignan a cuentas de NetApp Element y se utilizan para la generación de informes y la asignación de recursos. Agrupan la capacidad de almacenamiento en bruto o agregan las capacidades de almacenamiento que el sistema de almacenamiento puede proporcionar a los volúmenes virtuales. Un almacén de datos VVol que se crea en vSphere se asigna a un contenedor de almacenamiento individual. Un único contenedor de almacenamiento dispone de forma predeterminada de todos los recursos disponibles del clúster NetApp Element . Si se requiere una gobernanza más granular para la multitenencia, se pueden crear múltiples contenedores de almacenamiento.

Los contenedores de almacenamiento funcionan como las cuentas tradicionales y pueden contener tanto volúmenes virtuales como volúmenes tradicionales. Se admite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para utilizar la funcionalidad VVols. Puede descubrir contenedores de almacenamiento en vCenter durante la creación de VVols.

Proveedor de VASA

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

El proveedor VASA se ejecuta como parte del maestro del clúster en el software Element. El maestro del clúster es un servicio de alta disponibilidad que realiza la conmutación por error a cualquier nodo del clúster según sea necesario. Si el maestro del clúster falla, el proveedor VASA se mueve con él, lo que garantiza una alta disponibilidad para el proveedor VASA. Todas las tareas de aprovisionamiento y gestión de almacenamiento utilizan el proveedor VASA, que se encarga de cualquier cambio necesario en el clúster Element.

Para Element 12.5 y versiones anteriores, no registre más de un proveedor NetApp Element VASA en una sola instancia de vCenter. Cuando se agrega un segundo proveedor NetApp Element VASA, todos los almacenes de datos VVOL quedan inaccesibles.

La compatibilidad con VASA para hasta 10 vCenters está disponible como parche de actualización si ya ha registrado un proveedor de VASA con su vCenter. Para instalarlo, siga las instrucciones del manifiesto VASA39 y descargue el archivo .tar.gz desde el"Descargas de software de NetApp" sitio. El proveedor NetApp Element VASA utiliza un certificado NetApp . Con este parche, vCenter utiliza el certificado sin modificaciones para admitir múltiples vCenters para el uso de VASA y VVols. No modifique el certificado. VASA no admite certificados SSL personalizados.

Encuentra más información

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

Grupos de acceso por volumen

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

Los grupos de acceso a volúmenes en el almacenamiento NetApp SolidFire permiten que los IQN iniciadores iSCSI o los WWPN de Fibre Channel accedan a una colección de volúmenes. Cada IQN que agregue a un grupo de acceso puede acceder a cada volumen del grupo sin utilizar la autenticación CHAP. Cada WWPN que agregue a un grupo de acceso habilita el acceso a la red Fibre Channel a los volúmenes del grupo de acceso.

Los grupos de acceso por volumen tienen los siguientes límites:

- Un máximo de 128 iniciadores por grupo de acceso por volumen.
- Un máximo de 64 grupos de acceso por volumen.
- Un grupo de acceso puede estar compuesto por un máximo de 2000 volúmenes.
- Un IQN o WWPN solo puede pertenecer a un grupo de acceso a volumen.
- Para los clústeres Fibre Channel, un único volumen puede pertenecer a un máximo de cuatro grupos de acceso.

Iniciadores

Los iniciadores permiten que los clientes externos accedan a los volúmenes de un clúster, sirviendo como punto de entrada para la comunicación entre clientes y volúmenes. Puede utilizar iniciadores para el acceso basado en CHAP en lugar del acceso basado en cuentas a los volúmenes de almacenamiento. Un único iniciador, cuando se agrega a un grupo de acceso a volúmenes, permite a los miembros del grupo de acceso a volúmenes acceder a todos los volúmenes de almacenamiento agregados al grupo sin necesidad de autenticación. Un iniciador solo puede pertenecer a un grupo de acceso.

Protección de datos

Las funciones de protección de datos incluyen replicación remota, instantáneas de volumen, clonación de volumen, dominios de protección y alta disponibilidad con tecnología de doble hélice.

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

- Tipos de replicación remota
- Instantáneas de volumen para la protección de datos
- clones de volumen
- Descripción general del proceso de copia de seguridad y restauración para el almacenamiento de 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 instantáneas
- Replicación entre clústeres Element y ONTAP mediante SnapMirror

Para obtener más información, consulte "TR-4741: Replicación remota de software NetApp Element" .

Replicación síncrona y asíncrona entre clústeres

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

Puedes emparejar un clúster de almacenamiento con hasta cuatro clústeres de almacenamiento adicionales. Puede replicar datos de volumen de forma síncrona o asíncrona desde cualquiera de los clústeres de un par de clústeres para escenarios de conmutación por error y recuperación ante fallos.

Replicación sincrónica

La replicación síncrona replica continuamente los 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 apropiada para las siguientes situaciones:

- Replicación de varios sistemas a corta distancia
- Un sitio de recuperación ante desastres que se encuentra geográficamente cerca de la fuente.
- Aplicaciones sensibles al tiempo y la protección de bases de datos
- Aplicaciones de continuidad de negocio que requieren que el sitio secundario actúe como sitio principal cuando este último esté inactivo.

Replicación asíncrona

La replicación asíncrona replica continuamente los datos de un clúster de origen a un clúster de destino sin esperar las confirmaciones del clúster de destino. Durante la replicación asíncrona, las escrituras se confirman al cliente (aplicación) después de que se hayan confirmado en el clúster de origen.

La replicación asíncrona es apropiada para las siguientes situaciones:

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

Replicación solo de instantáneas

La protección de datos de solo instantáneas replica los datos modificados en momentos específicos en un clúster remoto. Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no lo son.

Puedes configurar la frecuencia de las replicaciones de instantáneas.

La replicación de instantáneas no afecta a la replicación asíncrona ni a la síncrona.

Replicación entre clústeres Element y ONTAP mediante SnapMirror

Con la tecnología NetApp SnapMirror , puede replicar instantáneas tomadas con el software NetApp Element en ONTAP para fines de recuperación ante desastres. En una relación SnapMirror , Element es un punto final y ONTAP es el otro.

SnapMirror es una tecnología de replicación de instantáneas de NetApp que facilita la recuperación ante desastres, diseñada para la conmutación por error desde el almacenamiento primario al almacenamiento secundario en un sitio geográficamente remoto. La tecnología SnapMirror crea una réplica, o espejo, de los datos de trabajo en un almacenamiento secundario desde el cual se puede seguir proporcionando datos si se produce una interrupción en el sitio principal. Los datos se reflejan a 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 puntos finales en los que residen los volúmenes y los volúmenes que contienen los datos replicados deben estar interconectados. Una relación entre pares permite que los clústeres y volúmenes intercambien datos de forma segura.

SnapMirror se ejecuta de forma nativa en los controladores NetApp ONTAP y está integrado en Element, que se ejecuta en clústeres NetApp HCI y SolidFire . La lógica para controlar SnapMirror reside en el software ONTAP ; por lo tanto, todas las relaciones de SnapMirror deben involucrar al menos un sistema ONTAP para realizar el trabajo de coordinación. Los usuarios gestionan las relaciones entre los clústeres Element y ONTAP principalmente a través de la interfaz de usuario de Element; sin embargo, algunas tareas de gestión residen en NetApp ONTAP System Manager. Los usuarios también pueden administrar SnapMirror a través de la CLI y la API, ambas disponibles en ONTAP y Element.

Ver "TR-4651: Arquitectura y configuración de NetApp SolidFire SnapMirror" (Se requiere iniciar sesión)

Debe habilitar manualmente la funcionalidad SnapMirror a nivel de clúster utilizando el software Element. La funcionalidad SnapMirror está desactivada por defecto y no se activa automáticamente como parte de una nueva instalación o actualización.

Tras habilitar SnapMirror, puede crear relaciones de SnapMirror desde la pestaña Protección de datos en el

software Element.

El software NetApp Element 10.1 y versiones posteriores admiten la funcionalidad SnapMirror para copiar y restaurar instantáneas con sistemas ONTAP .

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

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

Para obtener más información, consulte "Replicación entre NetApp Element Software y ONTAP (CLI de ONTAP)".

Instantáneas de volumen para la protección de datos

Una instantánea de volumen es una copia de un volumen en un momento dado que posteriormente se puede usar para restaurar un volumen a ese momento específico.

Aunque las instantáneas son similares a los clones de volumen, las instantáneas son simplemente réplicas de los metadatos del volumen, por lo que no se pueden montar ni escribir en ellas. La creación de una instantánea de volumen también requiere una cantidad mínima de recursos del sistema y espacio, lo que hace que la creación de instantáneas sea más rápida que la clonación.

Puede replicar instantáneas en un clúster remoto y utilizarlas como copia de seguridad del volumen. Esto le permite revertir un volumen a un punto específico en el tiempo mediante el uso de la instantánea replicada; también puede crear un clon de un volumen a partir de una instantánea replicada.

Puede realizar copias de seguridad de instantáneas desde un clúster de Element a un almacenamiento de objetos externo o a otro clúster de Element. Cuando se realiza una copia de seguridad de una instantánea en un almacenamiento de objetos externo, es necesario disponer de una conexión con dicho almacenamiento que permita operaciones de lectura/escritura.

Puede tomar una instantánea de un volumen individual o de varios para la protección de datos.

clones de volumen

Un clon de un único volumen o de varios volúmenes es una copia de los datos en un momento dado. Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea una copia de los datos a los que hace referencia la instantánea.

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

El clúster admite hasta dos solicitudes de clonación en ejecución por volumen a la vez y hasta ocho operaciones de clonación de volumen activas a la vez. Las solicitudes que superen estos límites se pondrán en cola para su posterior procesamiento.

Descripción general del proceso de copia de seguridad y restauración para el almacenamiento de Element

Puede realizar copias de seguridad y restaurar volúmenes en otros almacenamientos SolidFire , así como en almacenes de objetos secundarios compatibles con Amazon S3 u OpenStack Swift.

Puedes realizar una copia de seguridad de un volumen en lo siguiente:

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

Al restaurar volúmenes desde OpenStack Swift o Amazon S3, se necesita la información del manifiesto del proceso de copia de seguridad original. Si está restaurando un volumen del que se realizó una copia de seguridad en un sistema de almacenamiento SolidFire , no se requiere información de manifiesto.

Dominios de protección

Un dominio de protección es un nodo o un conjunto de nodos agrupados de tal manera que cualquier parte o incluso la totalidad del mismo podría fallar, manteniendo al mismo tiempo la disponibilidad de los datos. Los dominios de protección permiten que un clúster de almacenamiento se recupere automáticamente de la pérdida de un chasis (afinidad de chasis) o de todo un dominio (grupo de chasis).

Puede habilitar manualmente la supervisión del dominio de protección mediante el punto de extensión de configuración de NetApp Element en el complemento NetApp Element para vCenter Server. Puede seleccionar un umbral de dominio de protección basado en dominios de nodo o chasis. También puede habilitar la supervisión del dominio de protección mediante la API de Element o la interfaz web.

Un diseño de Dominio de Protección asigna cada nodo a un Dominio de Protección específico.

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

- A nivel de nodo, cada nodo se encuentra en su propio Dominio de Protección.
- A nivel de chasis, solo los nodos que comparten un chasis están en el mismo Dominio de Protección.
    - La disposición a nivel de chasis se determina automáticamente a partir del hardware cuando se agrega el nodo al clúster.
    - En un clúster donde cada nodo se encuentra en un chasis separado, estos dos niveles son funcionalmente idénticos.

Al crear un nuevo clúster, si utiliza nodos de almacenamiento que residen en un chasis compartido, es posible que desee considerar el diseño de una protección contra fallos a nivel de chasis mediante la función Dominios de protección.

Dominios de protección personalizados

Puede definir una disposición de dominio de protección personalizada que se ajuste a la disposición específica de su chasis y nodos, donde cada nodo esté asociado con un único dominio de protección personalizado. Por defecto, a cada nodo se le asigna el mismo dominio de protección personalizado predeterminado.

Si no se han asignado dominios de protección personalizados:

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

Cuando configura dominios de protección personalizados para un clúster, existen tres niveles de protección posibles, que puede ver en el panel de la interfaz web de Element:

- No protegido: El clúster de almacenamiento no está protegido contra el fallo de uno de sus dominios de protección personalizados. Para solucionar esto, agregue capacidad de almacenamiento adicional al clúster o reconfigure los dominios de protección personalizados del clúster para protegerlo de posibles pérdidas 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.
- Resistente a fallos: El clúster de almacenamiento tiene suficiente capacidad libre para autorrepararse tras el fallo de uno de sus dominios de protección personalizados. Una vez finalizado el proceso de recuperación, el clúster estará protegido contra la pérdida de datos en caso de que fallen dominios adicionales.

Si se asigna más de un dominio de protección personalizado, cada subsistema asignará los duplicados a dominios de protección personalizados separados. Si esto no es posible, recurre a asignar los duplicados a nodos separados. Cada subsistema (por ejemplo, contenedores, segmentos, proveedores de puntos finales de protocolo y conjunto) realiza esto de forma independiente.

Puedes usar la interfaz de usuario de Element para"Configurar dominios de protección personalizados" o bien puede utilizar los siguientes métodos de la API:

- "ObtenerDiseñoDeDominioDeProtección"- muestra en qué chasis y en qué dominio de protección personalizado se encuentra cada nodo.
- "Establecer diseño de dominio de protección"- Permite asignar un dominio de protección personalizado a cada nodo.

Alta disponibilidad de Double Helix

La protección de datos Double Helix es un método de replicación que distribuye al menos dos copias redundantes de los datos 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 se repare rápidamente.

Rendimiento y calidad del servicio

Un clúster de almacenamiento SolidFire tiene la capacidad de 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 QoS: IOPS mínimas, IOPS máximas e IOPS de ráfaga.

SolidFire Active IQ cuenta con una página de recomendaciones de QoS que ofrece consejos sobre la configuración óptima y la puesta en marcha de los ajustes de QoS.

Parámetros de calidad del servicio

Los parámetros IOPS se definen de las siguientes maneras:

- **IOPS mínimo** - El número mínimo de entradas y salidas sostenidas por segundo (IOPS) que el clúster de almacenamiento proporciona a un volumen. El valor de IOPS mínimo configurado para un volumen es el nivel de rendimiento garantizado para dicho volumen. El rendimiento no baja de este nivel.
- **IOPS máximo** - El número máximo de IOPS sostenidas que el clúster de almacenamiento proporciona a un volumen. Cuando los niveles de IOPS del clúster son críticamente altos, este nivel de rendimiento de IOPS no se supera.
- **IOPS de ráfaga** - El número máximo de IOPS permitido en un escenario de ráfaga corta. Si un volumen ha estado funcionando por debajo del IOPS máximo, se acumulan créditos de ráfaga. Cuando los niveles de rendimiento se vuelven muy altos y se llevan a niveles máximos, se permiten ráfagas cortas de IOPS en el volumen.

  El software Element utiliza Burst IOPS cuando un clúster se encuentra en un estado de baja utilización de IOPS del clúster.

  Un único volumen puede acumular IOPS de ráfaga y usar los créditos para realizar ráfagas por encima de sus IOPS máximas hasta su nivel de IOPS de ráfaga durante un "período de ráfaga" determinado. Un volumen puede generar ráfagas de hasta 60 segundos si el clúster tiene la capacidad para acomodarlas. Un volumen acumula un segundo de crédito de ráfaga (hasta un máximo de 60 segundos) por cada segundo que el volumen funcione por debajo de su límite de IOPS máximo.

  Las IOPS de ráfaga están limitadas de dos maneras:

  - Un volumen puede superar su IOPS máxima durante un número de segundos igual al número de créditos de ráfaga que haya acumulado el volumen.
  - Cuando un volumen supera su configuración de IOPS máximas, queda limitado por su configuración de IOPS de ráfaga. Por lo tanto, las IOPS de ráfaga nunca superan la configuración de IOPS de ráfaga para el volumen.
- **Ancho de banda máximo efectivo** - El ancho de banda máximo se calcula multiplicando el número de IOPS (según la curva QoS) por el tamaño de E/S.

  Ejemplo: La configuración de parámetros QoS de 100 IOPS mínimas, 1000 IOPS máximas y 1500 IOPS de ráfaga tiene los siguientes efectos en la calidad del rendimiento:

  - Las cargas de trabajo pueden alcanzar y mantener un máximo de 1000 IOPS hasta que la condición de contención de carga de trabajo por IOPS se haga evidente en el clúster. A continuación, las IOPS se reducen de forma incremental hasta que las IOPS en todos los volúmenes se encuentran dentro de los rangos QoS designados y se alivia la contención por el rendimiento.
  - El rendimiento en todos los volúmenes se está llevando hacia el IOPS mínimo de 100. Los niveles no bajan del valor de IOPS mínimo establecido, pero podrían mantenerse por encima de 100 IOPS cuando se alivia la contención de la carga de trabajo.
  - El rendimiento nunca es superior a 1000 IOPS, ni inferior a 100 IOPS durante un período prolongado. Se permite un rendimiento de 1500 IOPS (IOPS de ráfaga), pero solo para aquellos volúmenes que hayan acumulado créditos de ráfaga al funcionar por debajo de las IOPS máximas y solo durante períodos cortos de tiempo. Los niveles de ráfaga nunca se mantienen.

límites de valor de QoS

Aquí están los posibles valores mínimos y máximos para QoS.

Parámetros	Valor mínimo	Por defecto	4 KB	5 8KB	6 16 KB	262 KB
IOPS mínimas	50	50	15.000	9.375*	5556*	385*

Parámetros	Valor mínimo	Por defecto	4 KB	5 8KB	6 16 KB	262 KB
IOPS máximas	100	15.000	200.000**	125.000	74.074	5128
Burst IOPS	100	15.000	200.000**	125.000	74,074	5128

*Estas estimaciones son aproximadas. **Los valores de IOPS máximos e IOPS de ráfaga se pueden configurar hasta en 200.000; sin embargo, esta configuración solo se permite para desbloquear efectivamente el rendimiento de un volumen. El rendimiento máximo real de un volumen está limitado por el uso del clúster y el rendimiento por nodo.

Rendimiento de QoS

La curva de rendimiento QoS muestra la relación entre el tamaño del bloque y el porcentaje de IOPS.

El tamaño de bloque y el ancho de banda tienen un impacto directo en la cantidad de IOPS que una aplicación puede obtener. El software Element tiene en cuenta los tamaños de bloque que recibe normalizando los tamaños de bloque a 4k. En función de la carga de trabajo, el sistema podría aumentar el tamaño de los bloques. A medida que aumenta el tamaño de los bloques, el sistema incrementa el ancho de banda hasta el nivel necesario para procesar los bloques de mayor tamaño. A medida que aumenta el ancho de banda, disminuye el número de IOPS que el sistema puede alcanzar.

La curva de rendimiento QoS muestra la relación entre el aumento del tamaño de los bloques y la disminución del porcentaje de IOPS:

Por ejemplo, si los tamaños de bloque son de 4k y el ancho de banda es de 4000 KBps, las IOPS son 1000. Si el tamaño de los bloques aumenta a 8k, el ancho de banda aumenta a 5000 KBps y las IOPS disminuyen a 625. Al tener en cuenta el tamaño del bloque, el sistema garantiza que las cargas de trabajo de menor prioridad que utilizan tamaños de bloque más grandes, como las copias de seguridad y las actividades del hipervisor, no consuman demasiado rendimiento del tráfico de mayor prioridad que utiliza tamaños de bloque más pequeños.

Políticas de QoS

Una política de QoS le permite crear y guardar una configuración de calidad de servicio estandarizada que se puede aplicar a muchos volúmenes.

Las políticas de QoS son las más adecuadas para entornos de servicio, por ejemplo, con servidores de bases de datos, aplicaciones o infraestructura que rara vez se reinician y necesitan un acceso constante y equitativo al almacenamiento. La QoS de volumen individual es la mejor opción para máquinas virtuales de uso ligero, como escritorios virtuales o máquinas virtuales especializadas tipo quiosco, que pueden reiniciarse, encenderse o apagarse diariamente o varias veces al día.

No se deben utilizar juntas las políticas de QoS y QoS. Si está utilizando políticas de QoS, no utilice QoS personalizada en un volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.

El clúster seleccionado debe ser Element 10.0 o posterior para utilizar las políticas de QoS; de lo contrario, las funciones de política de QoS no estarán disponibles.

Encuentra más información

- "Documentación del software SolidFire y Element"

Información de copyright

Información de la marca comercial