Conceitos

Element Software

NetApp
November 18, 2025

Índice

Conceitos

Aprenda os conceitos básicos relacionados ao software Element.

- "Visão geral do produto"
- Visão geral da arquitetura SolidFire
- Nós
- Aglomerados
- "Segurança"
- Contas e permissões
- "Volumes"
- Proteção de dados
- Desempenho e qualidade do serviço

Visão geral do produto

Um sistema de armazenamento all-flash SolidFire é composto por componentes de hardware discretos (unidades e nós) que são combinados em um único conjunto de recursos de armazenamento. Este cluster unificado se apresenta como um sistema de armazenamento único para uso por clientes externos e é gerenciado pelo software NetApp Element .

Utilizando a interface Element, a API ou outras ferramentas de gerenciamento, você pode monitorar a capacidade e o desempenho do armazenamento do cluster SolidFire e gerenciar a atividade de armazenamento em uma infraestrutura multi-inquilino.

O SolidFire apresenta funcionalidades.

Um sistema Solidfire oferece os seguintes recursos:

- Oferece armazenamento de alto desempenho para sua infraestrutura de nuvem privada em grande escala.
- Oferece uma escala flexível que permite atender às necessidades de armazenamento em constante mudança.
- Utiliza uma interface de software Element para gerenciamento de armazenamento orientada por API.
- Garante o desempenho através de políticas de Qualidade de Serviço.
- Inclui balanceamento de carga automático em todos os nós do cluster.
- Reequilibra os clusters automaticamente quando nós são adicionados ou removidos.

Implantação do SolidFire

Utilize nós de armazenamento fornecidos pela NetApp e integrados ao software NetApp Element .

"Visão geral da arquitetura de armazenamento all-flash SolidFire"

Encontre mais informações

- "Plug-in NetApp Element para vCenter Server"

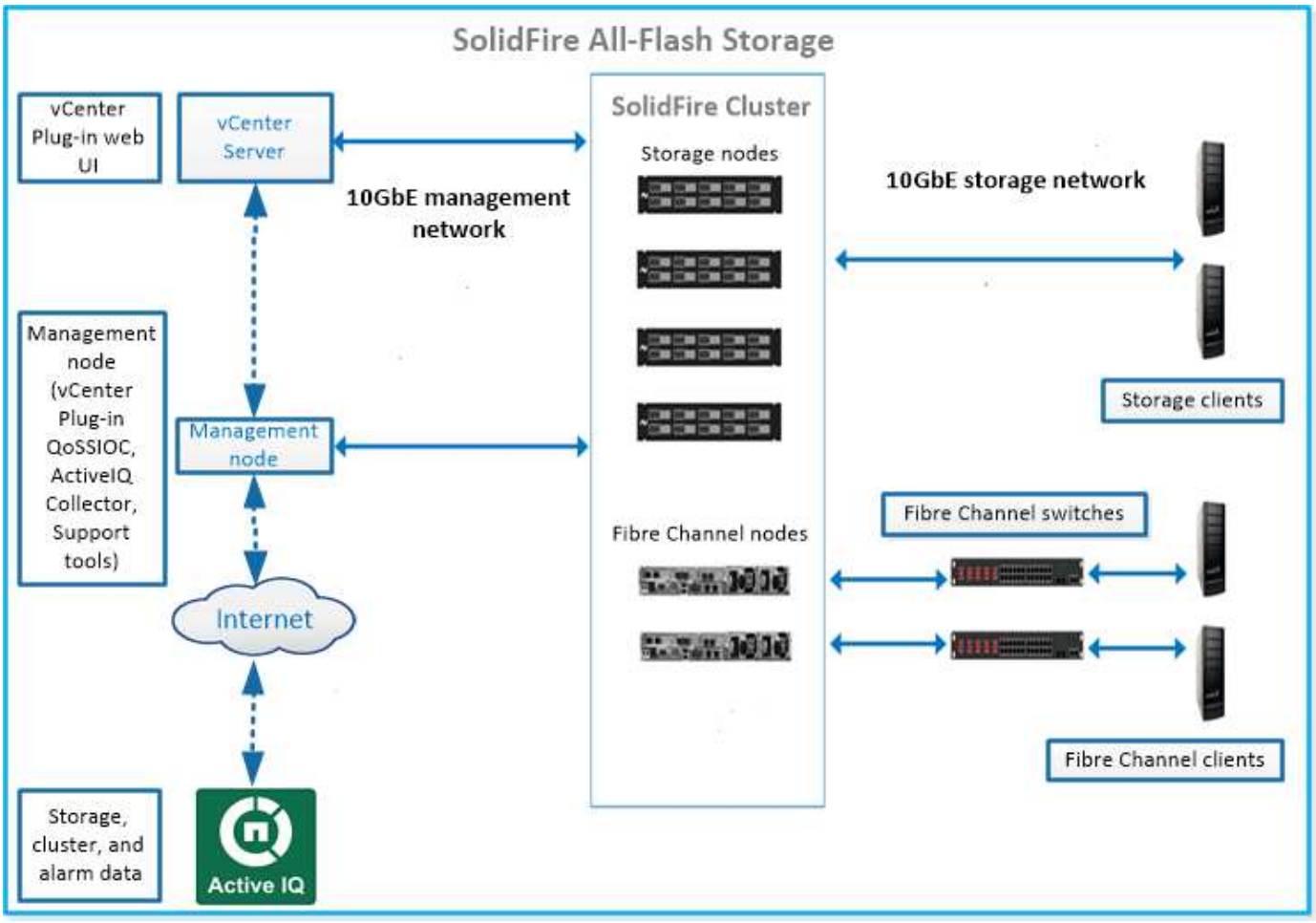
Arquitetura e componentes

Saiba mais sobre a arquitetura SolidFire .

Um sistema de armazenamento all-flash SolidFire é composto por componentes de hardware discretos (unidades e nós) que são combinados em um conjunto de recursos de armazenamento com o software NetApp Element executado independentemente em cada nó. Este sistema de armazenamento único é gerenciado como uma única entidade usando a interface de usuário do software Element, a API e outras ferramentas de gerenciamento.

Um sistema de armazenamento SolidFire inclui os seguintes componentes de hardware:

- **Cluster**: O núcleo do sistema de armazenamento SolidFire , que consiste em uma coleção de nós.
- **Nós**: Os componentes de hardware agrupados em um cluster. Existem dois tipos de nós:
  - Nós de armazenamento, que são servidores que contêm uma coleção de discos rígidos.
  - Nós Fibre Channel (FC), que você usa para se conectar a clientes FC.
- **Unidades de armazenamento**: Utilizadas nos nós de armazenamento para guardar dados do cluster. Um nó de armazenamento contém dois tipos de unidades:
  - Os metadados de volume fornecem informações de armazenamento que definem os volumes e outros objetos dentro de um cluster.
  - Unidades de bloco armazenam blocos de dados para volumes.



Você pode gerenciar, monitorar e atualizar o sistema usando a interface web do Element e outras ferramentas compatíveis:

- "Interfaces de software SolidFire"
- "SolidFire Active IQ"
- "Nó de gerenciamento para o software Element"
- "Serviços de gestão"

URLs comuns

Estas são as URLs comuns que você usa com um sistema de armazenamento totalmente em flash SolidFire :

URL	Descrição
`https://[storage cluster MVIP address]`	Acesse a interface de usuário do software NetApp Element .
`https://activeiq.solidfire.com`	Monitore os dados e receba alertas sobre quaisquer gargalos de desempenho ou potenciais problemas do sistema.
`https://[management node IP address]`	Acesse o NetApp Hybrid Cloud Control para atualizar sua instalação de armazenamento e os serviços de gerenciamento.

URL	Descrição
`https://[IP address]:442`	A partir da interface de usuário de cada nó, acesse as configurações de rede e cluster e utilize os testes e utilitários do sistema."Saber mais."
`https://[management node IP address]/mnode`	Utilize a API REST dos serviços de gerenciamento e outras funcionalidades a partir do nó de gerenciamento."Saber mais."
`https://[management node IP address]:9443`	Registre o pacote de plug-in do vCenter no vSphere Web Client."Saber mais."

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Interfaces de software SolidFire

Você pode gerenciar um sistema de armazenamento SolidFire usando diferentes interfaces de software e utilitários de integração do NetApp Element .

Opções

- Interface do usuário do software NetApp Element
- API de software NetApp Element
- Plug-in NetApp Element para vCenter Server
- Controle de Nuvem Híbrida NetApp
- Interfaces de usuário de nós de gerenciamento
- Utilitários e ferramentas de integração adicionais

Interface do usuário do software NetApp Element

Permite configurar o armazenamento Element, monitorar a capacidade e o desempenho do cluster e gerenciar a atividade de armazenamento em uma infraestrutura multi-inquilino. O Element é o sistema operacional de armazenamento que está no coração de um cluster SolidFire . O software Element funciona de forma independente em todos os nós do cluster e permite que os nós do cluster combinem recursos que são apresentados como um único sistema de armazenamento para clientes externos. O software Element é responsável por toda a coordenação do cluster, dimensionamento e gerenciamento do sistema como um todo. A interface do software é construída com base na API Element.

"Gerencie o armazenamento com o software Element."

API de software NetApp Element

Permite usar um conjunto de objetos, métodos e rotinas para gerenciar o armazenamento de elementos. A API Element é baseada no protocolo JSON-RPC sobre HTTPS. Você pode monitorar as operações da API na interface do usuário do Element ativando o registro de API; isso permite visualizar os métodos que estão sendo enviados ao sistema. Você pode habilitar tanto as solicitações quanto as respostas para ver como o sistema responde aos métodos emitidos.

"Gerencie o armazenamento com a API Element."

Plug-in NetApp Element para vCenter Server

Permite configurar e gerenciar clusters de armazenamento que executam o software Element usando uma interface alternativa para a interface do usuário do Element no VMware vSphere.

"Plug-in NetApp Element para vCenter Server"

Controle de Nuvem Híbrida NetApp

Permite atualizar os serviços de armazenamento e gerenciamento do Element e gerenciar ativos de armazenamento usando a interface do NetApp Hybrid Cloud Control.

"Gerencie o armazenamento com o NetApp Hybrid Cloud Control."

Interfaces de usuário de nós de gerenciamento

O nó de gerenciamento contém duas interfaces de usuário: uma interface para gerenciar serviços baseados em REST e uma interface específica para cada nó, destinada a gerenciar configurações de rede e cluster, além de testes e utilitários do sistema operacional. A partir da interface de usuário da API REST, você pode acessar um menu de APIs relacionadas ao serviço que controlam a funcionalidade do sistema baseado em serviço a partir do nó de gerenciamento.

Utilitários e ferramentas de integração adicionais

Embora normalmente você gerencie seu armazenamento com o NetApp Element, a API do NetApp Element e o plug-in do NetApp Element para vCenter Server, você pode usar utilitários e ferramentas de integração adicionais para acessar o armazenamento.

CLI do Element

"CLI do Element"Permite controlar um sistema de armazenamento SolidFire usando uma interface de linha de comando, sem precisar usar a API do Element.

Ferramentas do PowerShell para Elementos

"Ferramentas do PowerShell para Elementos"Permite usar um conjunto de funções do Microsoft Windows PowerShell que utilizam a API Element para gerenciar um sistema de armazenamento SolidFire .

SDKs de elementos

"SDKs de elementos"Permitem que você gerencie seu cluster SolidFire usando estas ferramentas:

- SDK Java do Element: Permite que os programadores integrem a API do Element com a linguagem de programação Java.
- SDK Element .NET: Permite que os programadores integrem a API do Element com a plataforma de programação .NET.
- SDK Element para Python: Permite que programadores integrem a API do Element com a linguagem de programação Python.

Conjunto de testes de API Postman do SolidFire

Permite que os programadores usem uma coleção de"Carteiro" Funções que testam chamadas da API

Element.

Adaptador de replicação de armazenamento SolidFire

"Adaptador de replicação de armazenamento SolidFire"Integra-se com o VMware Site Recovery Manager (SRM) para permitir a comunicação com clusters de armazenamento SolidFire replicados e executar fluxos de trabalho compatíveis.

SolidFire vRO

"SolidFire vRO"Oferece uma maneira prática de usar a API Element para administrar seu sistema de armazenamento SolidFire com o VMware vRealize Orchestrator.

Provedor VSS do SolidFire

"Provedor VSS do SolidFire"Integra cópias de sombra VSS com snapshots e clones do Element.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

SolidFire Active IQ

"SolidFire Active IQ"É uma ferramenta online que fornece visualizações históricas continuamente atualizadas de dados de todo o cluster. Você pode configurar alertas para eventos, limites ou métricas específicos. O SolidFire Active IQ permite monitorar o desempenho e a capacidade do sistema, além de manter-se informado sobre a integridade do cluster.

Você pode encontrar as seguintes informações sobre o seu sistema no SolidFire Active IQ:

- Número de nós e estado dos nós: íntegros, offline ou com falha
- Representação gráfica do uso de CPU, memória e limitação de nós.
- Detalhes sobre o nó, como número de série, localização do slot no chassi, modelo e versão do software NetApp Element em execução no nó de armazenamento.
- Informações sobre CPU e armazenamento das máquinas virtuais

Para saber mais sobre o SolidFire Active IQ, consulte o "Documentação do SolidFire Active IQ" .

Para maiores informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"
- **Site de suporte da NetApp › Ferramentas para Active IQ**

Nó de gerenciamento para o software Element

O"nó de gerenciamento (mNode)" É uma máquina virtual que funciona em paralelo com um ou mais clusters de armazenamento baseados no software Element. É utilizado para

atualizar e fornecer serviços de sistema, incluindo monitoramento e telemetria, gerenciar ativos e configurações de cluster, executar testes e utilitários de sistema e habilitar o acesso do Suporte da NetApp para solução de problemas.

O nó de gerenciamento interage com um cluster de armazenamento para executar ações de gerenciamento, mas não é membro do cluster de armazenamento. Os nós de gerenciamento coletam periodicamente informações sobre o cluster por meio de chamadas de API e reportam essas informações ao Active IQ para monitoramento remoto (se habilitado). Os nós de gerenciamento também são responsáveis por coordenar as atualizações de software dos nós do cluster.

A partir da versão 11.3 do Element, o nó de gerenciamento funciona como um host de microsserviços, permitindo atualizações mais rápidas de serviços de software selecionados fora das versões principais. Esses microsserviços ou"serviços de gestão" são atualizados frequentemente como pacotes de serviços.

Serviços de gerenciamento para armazenamento all-flash SolidFire

A partir da versão 11.3 do Element, os **serviços de gerenciamento** estão hospedados no"nó de gerenciamento" , permitindo atualizações mais rápidas de serviços de software selecionados fora das versões principais.

Os serviços de gerenciamento fornecem funcionalidades de gerenciamento centralizadas e ampliadas para o armazenamento all-flash SolidFire . Esses serviços incluem"Controle de Nuvem Híbrida NetApp" , Telemetria do sistema Active IQ , registro de logs e atualizações de serviço, bem como o serviço QoSSIOC para o plug-in Element para vCenter.

Saiba mais sobre"liberações de serviços de gerenciamento" .

Nós

Os nós são recursos de hardware ou virtuais agrupados em um cluster para fornecer armazenamento em bloco e capacidade de computação.

O software NetApp Element define várias funções de nó para um cluster. Os tipos de funções de nó são os seguintes:

- Nó de gerenciamento
- Nó de armazenamento
- Nó Fibre Channel

Estados dos nósvariam dependendo da associação ao cluster.

Nó de gerenciamento

Um nó de gerenciamento é uma máquina virtual usada para atualizar e fornecer serviços de sistema, incluindo monitoramento e telemetria, gerenciar ativos e configurações do cluster, executar testes e utilitários do sistema e permitir o acesso do Suporte da NetApp para solução de problemas."Saber mais"

Nó de armazenamento

Um nó de armazenamento SolidFire é um servidor que contém uma coleção de unidades que se comunicam

entre si através da interface de rede Bond10G. As unidades no nó contêm espaço de bloco e de metadados para armazenamento e gerenciamento de dados. Cada nó contém uma imagem de fábrica do software NetApp Element .

Os nós de armazenamento possuem as seguintes características:

- Cada nó possui um nome único. Se um administrador não especificar um nome de nó, o padrão será SF-XXXX, onde XXXX são quatro caracteres aleatórios gerados pelo sistema.
- Cada nó possui seu próprio cache de escrita de memória de acesso aleatório não volátil (NVRAM) de alto desempenho para melhorar o desempenho geral do sistema e reduzir a latência de escrita.
- Cada nó está conectado a duas redes, uma de armazenamento e outra de gerenciamento, cada uma com dois links independentes para redundância e desempenho. Cada nó requer um endereço IP em cada rede.
- Você pode criar um cluster com novos nós de armazenamento ou adicionar nós de armazenamento a um cluster existente para aumentar a capacidade e o desempenho do armazenamento.
- Você pode adicionar ou remover nós do cluster a qualquer momento sem interromper o serviço.

Nó Fibre Channel

Os nós Fibre Channel da SolidFire fornecem conectividade a um switch Fibre Channel, que você pode conectar a clientes Fibre Channel. Os nós Fibre Channel atuam como conversores de protocolo entre os protocolos Fibre Channel e iSCSI; isso permite adicionar conectividade Fibre Channel a qualquer cluster SolidFire novo ou existente.

Os nós Fibre Channel possuem as seguintes características:

- Os switches Fibre Channel gerenciam o estado da estrutura, proporcionando interconexões otimizadas.
- O tráfego entre duas portas flui apenas através dos switches; ele não é transmitido para nenhuma outra porta.
- A falha de uma porta é isolada e não afeta o funcionamento das outras portas.
- Vários pares de portas podem se comunicar simultaneamente em uma malha.

Estados de operação dos nós

Um nó pode estar em um de vários estados, dependendo do nível de configuração.

- **Disponível**

  O nó não possui um nome de cluster associado e ainda não faz parte de um cluster.

- **Pendente**

  O nó está configurado e pode ser adicionado a um cluster designado.

  Não é necessário autenticar para acessar o nó.

- **Aguardando Ativação**

  O sistema está em processo de instalação do software Element compatível no nó. Ao concluir, o nó passará para o estado Ativo.

- **Ativo**

  O nó está participando de um cluster.

  É necessário autenticar-se para modificar o nó.

Em cada um desses estados, alguns campos são somente leitura.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Aglomerados

Um cluster é o núcleo de um sistema de armazenamento SolidFire e é composto por uma coleção de nós. Para que a eficiência de armazenamento do SolidFire seja alcançada, é necessário ter pelo menos quatro nós em um cluster. Um cluster aparece na rede como um único grupo lógico e pode então ser acessado como armazenamento em blocos.

A criação de um novo cluster inicializa um nó como proprietário das comunicações do cluster e estabelece as comunicações de rede para cada nó no cluster. Este processo é realizado apenas uma vez para cada novo cluster. Você pode criar um cluster usando a interface do usuário do Element ou a API.

Você pode expandir um cluster adicionando nós adicionais. Ao adicionar um novo nó, não há interrupção do serviço e o cluster utiliza automaticamente o desempenho e a capacidade do novo nó.

Administradores e hosts podem acessar o cluster usando endereços IP virtuais. Qualquer nó no cluster pode hospedar endereços IP virtuais. O endereço IP virtual de gerenciamento (MVIP) permite o gerenciamento do cluster por meio de uma conexão 1GbE, enquanto o endereço IP virtual de armazenamento (SVIP) permite o acesso do host ao armazenamento por meio de uma conexão 10GbE. Esses endereços IP virtuais permitem conexões consistentes, independentemente do tamanho ou da composição de um cluster SolidFire . Se um nó que hospeda um endereço IP virtual falhar, outro nó no cluster começará a hospedar o endereço IP virtual.

> A partir da versão 11.0 do Element, os nós podem ser configurados com endereços IPv4, IPv6 ou ambos para sua rede de gerenciamento. Isso se aplica tanto a nós de armazenamento quanto a nós de gerenciamento, exceto para o nó de gerenciamento 11.3 e versões posteriores, que não suportam IPv6. Ao criar um cluster, apenas um único endereço IPv4 ou IPv6 pode ser usado para o MVIP e o tipo de endereço correspondente deve ser configurado em todos os nós.

Mais sobre clusters

- Clusters de armazenamento autoritativos
- Regra dos terços
- Capacidade ociosa
- Eficiência de armazenamento
- Quórum do cluster de armazenamento

Clusters de armazenamento autoritativos

O cluster de armazenamento autorizado é o cluster de armazenamento que o NetApp Hybrid Cloud Control usa para autenticar usuários.

Se o seu nó de gerenciamento tiver apenas um cluster de armazenamento, então ele será o cluster autoritativo. Se o seu nó de gerenciamento tiver dois ou mais clusters de armazenamento, um desses clusters será designado como o cluster autoritativo e somente os usuários desse cluster poderão fazer login no NetApp Hybrid Cloud Control. Para descobrir qual cluster é o cluster autoritativo, você pode usar o `GET /mnode/about` API. Na resposta, o endereço IP no `token_url` O campo é o endereço IP virtual de gerenciamento (MVIP) do cluster de armazenamento autoritativo. Se você tentar fazer login no NetApp Hybrid Cloud Control como um usuário que não está no cluster autoritativo, a tentativa de login falhará.

Muitos recursos do NetApp Hybrid Cloud Control são projetados para funcionar com vários clusters de armazenamento, mas a autenticação e a autorização têm limitações. A limitação relacionada à autenticação e autorização é que o usuário do cluster autoritativo pode executar ações em outros clusters vinculados ao NetApp Hybrid Cloud Control, mesmo que não seja um usuário nesses outros clusters de armazenamento.

Antes de prosseguir com o gerenciamento de vários clusters de armazenamento, você deve garantir que os usuários definidos nos clusters autorizados estejam definidos em todos os outros clusters de armazenamento com as mesmas permissões. Você pode gerenciar usuários a partir do"Interface de usuário do software Element" .

Ver"Criar e gerenciar ativos de cluster de armazenamento" Para obter mais informações sobre como trabalhar com ativos de cluster de armazenamento de nós de gerenciamento.

Regra dos terços

Ao combinar tipos de nós de armazenamento em um cluster de armazenamento NetApp SolidFire , nenhum nó de armazenamento individual pode conter mais de 33% da capacidade total do cluster.

Capacidade ociosa

Se um nó recém-adicionado representar mais de 50% da capacidade total do cluster, parte da capacidade desse nó será tornada inutilizável ("isolada"), para que ele esteja em conformidade com a regra de capacidade. Essa situação permanece inalterada até que mais capacidade de armazenamento seja adicionada. Se um nó muito grande for adicionado e também desobedecer à regra de capacidade, o nó anteriormente isolado deixará de estar isolado, enquanto o nó recém-adicionado ficará isolado. A capacidade deve sempre ser adicionada em pares para evitar que isso aconteça. Quando um nó fica inativo, uma falha de cluster apropriada é lançada.

Eficiência de armazenamento

Os clusters de armazenamento NetApp SolidFire utilizam deduplicação, compressão e provisionamento dinâmico para reduzir a quantidade de armazenamento físico necessária para armazenar um volume.

- **Compressão**

  A compressão reduz a quantidade de armazenamento físico necessária para um volume, combinando blocos de dados em grupos de compressão, cada um dos quais é armazenado como um único bloco.

- **Desduplicação**

  A deduplicação reduz a quantidade de armazenamento físico necessária para um volume, descartando

blocos de dados duplicados.

- **Provisionamento dinâmico**

  Um volume ou LUN com provisionamento dinâmico é aquele para o qual o armazenamento não é reservado antecipadamente. Em vez disso, o armazenamento é alocado dinamicamente, conforme a necessidade. O espaço livre é liberado para o sistema de armazenamento quando os dados no volume ou LUN são excluídos.

Quórum do cluster de armazenamento

O software Element cria um cluster de armazenamento a partir de nós selecionados, que mantém um banco de dados replicado da configuração do cluster. Para manter o quórum e garantir a resiliência do cluster, é necessário que pelo menos três nós participem do conjunto de clusters.

Segurança

Ao utilizar o sistema de armazenamento all-flash SolidFire , seus dados são protegidos por protocolos de segurança padrão do setor.

Criptografia em repouso (hardware)

Todas as unidades nos nós de armazenamento são capazes de utilizar criptografia AES de 256 bits no nível da unidade. Cada unidade possui sua própria chave de criptografia, que é criada quando a unidade é inicializada pela primeira vez. Ao ativar o recurso de criptografia, uma senha válida para todo o cluster é criada e partes dessa senha são distribuídas para todos os nós do cluster. Nenhum nó individual armazena a senha completa. A senha é então usada para proteger todo o acesso às unidades. A senha é necessária para desbloquear a unidade e, em seguida, não é necessária a menos que a alimentação da unidade seja removida ou a unidade esteja bloqueada.

"Habilitar o recurso de criptografia de hardware em repouso"Não afeta o desempenho ou a eficiência do cluster. Se uma unidade ou nó com criptografia habilitada for removido da configuração do cluster usando a API do Element ou a interface do usuário do Element, a criptografia em repouso será desativada nessas unidades. Após a remoção da unidade, os dados podem ser apagados com segurança utilizando o seguinte método: `SecureEraseDrives` Método da API. Se uma unidade ou nó físico for removido à força, os dados permanecem protegidos pela senha global do cluster e pelas chaves de criptografia individuais da unidade.

Criptografia em repouso (software)

Outro tipo de criptografia em repouso, a criptografia em repouso por software, permite que todos os dados gravados em SSDs em um cluster de armazenamento sejam criptografados. "Quando ativado" Ele criptografa todos os dados gravados e descriptografa todos os dados lidos automaticamente no software. A criptografia de software em repouso espelha a implementação do Self-Encrypting Drive (SED) em hardware para fornecer segurança de dados na ausência do SED.

Para clusters de armazenamento all-flash SolidFire , a criptografia de software em repouso deve ser ativada durante a criação do cluster e não pode ser desativada após a sua criação.

A criptografia em repouso baseada em software e em hardware pode ser usada de forma independente ou em combinação.

Gestão de chaves externas

Você pode configurar o software Element para usar um serviço de gerenciamento de chaves (KMS) de terceiros compatível com KMIP para gerenciar as chaves de criptografia do cluster de armazenamento. Ao ativar esse recurso, a chave de criptografia da senha de acesso à unidade em todo o cluster de armazenamento é gerenciada por um KMS especificado por você.

O Element pode utilizar os seguintes serviços de gerenciamento de chaves:

- Gemalto SafeNet KeySecure
- SafeNet AT KeySecure
- Controle de chave HyTrust
- Gerente de Segurança de Dados Vormetric
- IBM Security Key Lifecycle Manager

Para obter mais informações sobre como configurar o gerenciamento de chaves externas, consulte"Introdução ao gerenciamento de chaves externas" documentação.

Autenticação multifator

A autenticação multifator (MFA) permite exigir que os usuários apresentem vários tipos de evidências para autenticar-se na interface web do NetApp Element ou na interface do nó de armazenamento ao fazer login. Você pode configurar o Element para aceitar somente autenticação multifator para logins, integrando-o ao seu sistema de gerenciamento de usuários e provedor de identidade existentes. Você pode configurar o Element para integrar-se a um provedor de identidade SAML 2.0 existente, que pode impor vários esquemas de autenticação, como senha e mensagem de texto, senha e mensagem de e-mail ou outros métodos.

Você pode combinar a autenticação multifator com provedores de identidade (IdPs) comuns compatíveis com SAML 2.0, como o Microsoft Active Directory Federation Services (ADFS) e o Shibboleth.

Para configurar a MFA, consulte "habilitar autenticação multifator" documentação.

FIPS 140-2 para HTTPS e criptografia de dados em repouso

Os clusters de armazenamento NetApp SolidFire suportam criptografia em conformidade com os requisitos do padrão Federal Information Processing Standard (FIPS) 140-2 para módulos criptográficos. Você pode habilitar a conformidade com o padrão FIPS 140-2 em seu cluster SolidFire para comunicações HTTPS e criptografia de unidade.

Ao ativar o modo de operação FIPS 140-2 no seu cluster, o módulo de segurança criptográfica da NetApp (NCSM) é ativado e utiliza criptografia certificada FIPS 140-2 Nível 1 para toda a comunicação via HTTPS com a interface do usuário e a API do NetApp Element . Você usa o `EnableFeature` API de elementos com o `fips` parâmetro para habilitar a criptografia HTTPS FIPS 140-2. Em clusters de armazenamento com hardware compatível com FIPS, você também pode habilitar a criptografia de unidade FIPS para dados em repouso usando o `EnableFeature` API de elementos com o `FipsDrives` parâmetro.

Para obter mais informações sobre como preparar um novo cluster de armazenamento para criptografia FIPS 140-2, consulte"Crie um cluster que suporte unidades FIPS." .

Para obter mais informações sobre como habilitar o FIPS 140-2 em um cluster existente e preparado, consulte"API EnableFeatureElement" .

Para maiores informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Contas e permissões

Para administrar e fornecer acesso aos recursos de armazenamento do seu sistema, você precisará configurar contas para esses recursos.

Utilizando o armazenamento Element, você pode criar e gerenciar os seguintes tipos de contas:

- Contas de usuário administrador para o cluster de armazenamento
- Contas de usuário para acesso ao volume de armazenamento
- Contas de usuário autorizadas para o cluster do NetApp Hybrid Cloud Control.

Contas de administrador de cluster de armazenamento

Existem dois tipos de contas de administrador que podem existir em um cluster de armazenamento executando o software NetApp Element :

- **Conta de administrador do cluster principal**: Esta conta de administrador é criada quando o cluster é criado. Esta conta é a conta administrativa principal com o nível mais alto de acesso ao cluster. Essa conta é análoga a um usuário root em um sistema Linux. Você pode alterar a senha desta conta de administrador.
- **Conta de administrador do cluster**: Você pode conceder a uma conta de administrador do cluster um acesso administrativo limitado para executar tarefas específicas dentro de um cluster. As credenciais atribuídas a cada conta de administrador de cluster são usadas para autenticar solicitações de API e da interface do usuário do Element dentro do sistema de armazenamento.

> É necessária uma conta de administrador de cluster local (não LDAP) para acessar os nós ativos em um cluster por meio da interface de usuário de cada nó. Não são necessárias credenciais de conta para acessar um nó que ainda não faz parte de um cluster.

Você pode"gerenciar contas de administrador de cluster" através da criação, exclusão e edição de contas de administrador de cluster, alteração da senha do administrador de cluster e configuração das definições de LDAP para gerir o acesso dos utilizadores ao sistema.

Contas de usuário

As contas de usuário são utilizadas para controlar o acesso aos recursos de armazenamento em uma rede baseada no software NetApp Element . É necessário ter pelo menos uma conta de usuário para que um volume possa ser criado.

Ao criar um volume, ele é atribuído a uma conta. Se você criou um volume virtual, a conta é o contêiner de armazenamento.

Aqui estão algumas considerações adicionais:

- A conta contém a autenticação CHAP necessária para acessar os volumes a ela atribuídos.

- Uma conta pode ter até 2000 volumes atribuídos a ela, mas um volume só pode pertencer a uma conta.
- As contas de usuário podem ser gerenciadas a partir do ponto de extensão NetApp Element Management.

Contas de usuário autorizadas do cluster

As contas de usuário autorizadas do cluster podem se autenticar em qualquer recurso de armazenamento associado à instância de nós e clusters do NetApp Hybrid Cloud Control. Com esta conta, você pode gerenciar volumes, contas, grupos de acesso e muito mais em todos os clusters.

As contas de usuário autorizadas são gerenciadas na opção Gerenciamento de Usuários, no menu superior direito do NetApp Hybrid Cloud Control.

O"cluster de armazenamento autoritativo" é o cluster de armazenamento que o NetApp Hybrid Cloud Control usa para autenticar usuários.

Todos os usuários criados no cluster de armazenamento autoritativo podem fazer login no NetApp Hybrid Cloud Control. Usuários criados em outros clusters de armazenamento *não podem* fazer login no Hybrid Cloud Control.

- Se o seu nó de gerenciamento tiver apenas um cluster de armazenamento, então ele será o cluster autoritativo.
- Se o seu nó de gerenciamento tiver dois ou mais clusters de armazenamento, um desses clusters será designado como o cluster autoritativo e somente os usuários desse cluster poderão fazer login no NetApp Hybrid Cloud Control.

Embora muitos recursos do NetApp Hybrid Cloud Control funcionem com vários clusters de armazenamento, a autenticação e a autorização têm limitações inerentes. A limitação relacionada à autenticação e autorização é que os usuários do cluster autoritativo podem executar ações em outros clusters vinculados ao NetApp Hybrid Cloud Control, mesmo que não sejam usuários nesses outros clusters de armazenamento. Antes de prosseguir com o gerenciamento de vários clusters de armazenamento, você deve garantir que os usuários definidos nos clusters autorizados estejam definidos em todos os outros clusters de armazenamento com as mesmas permissões. Você pode gerenciar usuários a partir do NetApp Hybrid Cloud Control.

Contas de volume

As contas específicas de volume são exclusivas do cluster de armazenamento no qual foram criadas. Essas contas permitem definir permissões em volumes específicos na rede, mas não têm efeito fora desses volumes.

As contas de volume são gerenciadas na tabela de Volumes de Controle do NetApp Hybrid Cloud.

Armazenar

Volumes

O sistema de armazenamento NetApp Element provisiona armazenamento usando volumes. Os volumes são dispositivos de bloco acessados pela rede por clientes iSCSI ou Fibre Channel.

O armazenamento de elementos permite criar, visualizar, editar, excluir, clonar, fazer backup ou restaurar volumes para contas de usuário. Você também pode gerenciar cada volume em um cluster e adicionar ou remover volumes em grupos de acesso a volumes.

Volumes persistentes

Os volumes persistentes permitem que os dados de configuração do nó de gerenciamento sejam armazenados em um cluster de armazenamento específico, em vez de localmente em uma máquina virtual, para que os dados possam ser preservados em caso de perda ou remoção do nó de gerenciamento. Os volumes persistentes são uma configuração opcional, porém recomendada, do nó de gerenciamento.

Uma opção para habilitar volumes persistentes está incluída nos scripts de instalação e atualização quando… "implantando um novo nó de gerenciamento" . Volumes persistentes são volumes em um cluster de armazenamento baseado em software Element que contêm informações de configuração do nó de gerenciamento para a máquina virtual (VM) do nó de gerenciamento do host, e que persistem além do ciclo de vida da VM. Caso o nó de gerenciamento seja perdido, uma máquina virtual de nó de gerenciamento substituta pode se reconectar e recuperar os dados de configuração da máquina virtual perdida.

A funcionalidade de volumes persistentes, se ativada durante a instalação ou atualização, cria automaticamente vários volumes. Esses volumes, assim como qualquer volume baseado no software Element, podem ser visualizados usando a interface web do software Element, o plug-in NetApp Element para vCenter Server ou a API, dependendo da sua preferência e instalação. Os volumes persistentes devem estar ativos e em funcionamento, com uma conexão iSCSI ao nó de gerenciamento, para manter os dados de configuração atuais que podem ser usados para recuperação.

> Os volumes persistentes associados aos serviços de gerenciamento são criados e atribuídos a uma nova conta durante a instalação ou atualização. Se você estiver usando volumes persistentes, não modifique nem exclua os volumes ou a conta associada a eles.

Volumes virtuais (vVols)

O vSphere Virtual Volumes é um paradigma de armazenamento para VMware que transfere grande parte do gerenciamento de armazenamento do vSphere do sistema de armazenamento para o VMware vCenter. Com os Volumes Virtuais (vVols), você pode alocar armazenamento de acordo com os requisitos de máquinas virtuais individuais.

Encadernações

O cluster NetApp Element escolhe um endpoint de protocolo ideal, cria uma associação que vincula o host ESXi e o volume virtual ao endpoint do protocolo e retorna a associação para o host ESXi. Após a vinculação, o host ESXi pode executar operações de E/S com o volume virtual vinculado.

Pontos finais do protocolo

Os hosts VMware ESXi usam proxies de E/S lógicos, conhecidos como endpoints de protocolo, para se comunicar com volumes virtuais. Os hosts ESXi vinculam volumes virtuais a endpoints de protocolo para executar operações de E/S. Quando uma máquina virtual no host executa uma operação de E/S, o endpoint do protocolo associado direciona a E/S para o volume virtual com o qual está emparelhada.

Os endpoints de protocolo em um cluster NetApp Element funcionam como unidades lógicas administrativas SCSI. Cada ponto de extremidade do protocolo é criado automaticamente pelo cluster. Para cada nó em um cluster, é criado um ponto de extremidade de protocolo correspondente. Por exemplo, um cluster de quatro nós terá quatro pontos de extremidade de protocolo.

O iSCSI é o único protocolo compatível com o software NetApp Element . O protocolo Fibre Channel não é suportado. Os endpoints do protocolo não podem ser excluídos ou modificados por um usuário, não estão associados a uma conta e não podem ser adicionados a um grupo de acesso a volume.

Recipientes de armazenamento

Os contêineres de armazenamento são construções lógicas que correspondem a contas do NetApp Element e são usadas para geração de relatórios e alocação de recursos. Eles agrupam a capacidade de armazenamento bruto ou as capacidades de armazenamento agregadas que o sistema de armazenamento pode fornecer aos volumes virtuais. Um armazenamento de dados VVol criado no vSphere é mapeado para um contêiner de armazenamento individual. Por padrão, um único contêiner de armazenamento possui todos os recursos disponíveis do cluster NetApp Element . Caso seja necessário um controle mais granular para multilocação, vários contêineres de armazenamento podem ser criados.

Os contêineres de armazenamento funcionam como contas tradicionais e podem conter tanto volumes virtuais quanto volumes tradicionais. É suportado um máximo de quatro contêineres de armazenamento por cluster. É necessário, no mínimo, um contêiner de armazenamento para usar a funcionalidade VVols. É possível descobrir contêineres de armazenamento no vCenter durante a criação de VVols.

provedor VASA

Para que o vSphere reconheça o recurso vVol no cluster NetApp Element , o administrador do vSphere deve registrar o provedor VASA do NetApp Element no vCenter. O provedor VASA é o caminho de controle fora de banda entre o vSphere e o cluster Element. É responsável por executar solicitações no cluster Element em nome do vSphere, como criar VMs, disponibilizar VMs para o vSphere e anunciar recursos de armazenamento para o vSphere.

O provedor VASA é executado como parte do nó mestre do cluster no software Element. O nó mestre do cluster é um serviço de alta disponibilidade que, em caso de falha, alterna para qualquer nó do cluster conforme necessário. Se o nó mestre do cluster falhar, o provedor VASA migrará juntamente com ele, garantindo alta disponibilidade para o provedor VASA. Todas as tarefas de provisionamento e gerenciamento de armazenamento utilizam o provedor VASA, que lida com quaisquer alterações necessárias no cluster Element.

> Para o Element 12.5 e versões anteriores, não registre mais de um provedor NetApp Element VASA em uma única instância do vCenter. Quando um segundo provedor NetApp Element VASA é adicionado, todos os datastores VVOL ficam inacessíveis.

> O suporte ao VASA para até 10 vCenters está disponível como um patch de atualização caso você já tenha registrado um provedor VASA em seu vCenter. Para instalar, siga as instruções no manifesto VASA39 e baixe o arquivo .tar.gz do site."Downloads de software da NetApp" site. O provedor NetApp Element VASA utiliza um certificado NetApp . Com essa correção, o certificado é usado sem modificações pelo vCenter para oferecer suporte a vários vCenters para uso com VASA e VVols. Não modifique o certificado. A VASA não oferece suporte a certificados SSL personalizados.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Grupos de acesso a volume

Ao criar e usar grupos de acesso a volumes, você pode controlar o acesso a um conjunto de volumes. Ao associar um conjunto de volumes e um conjunto de iniciadores a um grupo de acesso a volumes, o grupo de acesso concede a esses iniciadores

acesso a esse conjunto de volumes.

Os grupos de acesso a volumes no armazenamento NetApp SolidFire permitem que os IQNs de iniciadores iSCSI ou os WWPNs Fibre Channel acessem uma coleção de volumes. Cada IQN adicionado a um grupo de acesso pode acessar todos os volumes do grupo sem usar a autenticação CHAP. Cada WWPN adicionado a um grupo de acesso habilita o acesso à rede Fibre Channel aos volumes presentes no grupo.

Os grupos de acesso por volume têm as seguintes limitações:

- Um máximo de 128 iniciadores por grupo de acesso por volume.
- Um máximo de 64 grupos de acesso por volume.
- Um grupo de acesso pode ser composto por, no máximo, 2000 volumes.
- Um IQN ou WWPN pode pertencer a apenas um grupo de acesso a volume.
- Para clusters Fibre Channel, um único volume pode pertencer a, no máximo, quatro grupos de acesso.

Iniciadores

Os iniciadores permitem que clientes externos acessem volumes em um cluster, servindo como ponto de entrada para a comunicação entre clientes e volumes. Você pode usar iniciadores para acesso a volumes de armazenamento baseado em CHAP, em vez de acesso baseado em conta. Um único iniciador, quando adicionado a um grupo de acesso a volumes, permite que os membros do grupo acessem todos os volumes de armazenamento adicionados ao grupo sem a necessidade de autenticação. Um iniciador pode pertencer a apenas um grupo de acesso.

Proteção de dados

Os recursos de proteção de dados incluem replicação remota, snapshots de volume, clonagem de volume, Domínios de Proteção e alta disponibilidade com a tecnologia Double Helix.

A proteção de dados de armazenamento de elementos inclui os seguintes conceitos:

- Tipos de replicação remota
- Instantâneos de volume para proteção de dados
- Clones de volume
- Visão geral do processo de backup e restauração para o armazenamento Element.
- Domínios de proteção
- Domínios de proteção personalizados
- Alta disponibilidade da dupla hélice

Tipos de replicação remota

A replicação remota de dados pode assumir as seguintes formas:

- Replicação síncrona e assíncrona entre clusters

- Replicação somente de instantâneo
- Replicação entre clusters Element e ONTAP usando SnapMirror

Para obter mais informações, consulte "TR-4741: Replicação Remota do Software NetApp Element" .

Replicação síncrona e assíncrona entre clusters

Para clusters que executam o software NetApp Element , a replicação em tempo real permite a criação rápida de cópias remotas de dados de volume.

Você pode emparelhar um cluster de armazenamento com até quatro outros clusters de armazenamento. Você pode replicar dados de volume de forma síncrona ou assíncrona de qualquer um dos clusters em um par de clusters para cenários de failover e failback.

Replicação síncrona

A replicação síncrona replica continuamente os dados do cluster de origem para o cluster de destino e é afetada por latência, perda de pacotes, jitter e largura de banda.

A replicação síncrona é apropriada para as seguintes situações:

- Replicação de vários sistemas em uma curta distância.
- Um local de recuperação de desastres que esteja geograficamente próximo da fonte.
- Aplicações sensíveis ao tempo e a proteção de bancos de dados
- Aplicações de continuidade de negócios que exigem que o site secundário atue como site primário quando o site primário estiver inativo.

Replicação assíncrona

A replicação assíncrona replica continuamente os dados de um cluster de origem para um cluster de destino sem esperar pelas confirmações do cluster de destino. Durante a replicação assíncrona, as gravações são confirmadas ao cliente (aplicação) após serem confirmadas no cluster de origem.

A replicação assíncrona é apropriada para as seguintes situações:

- O local de recuperação de desastres fica longe da origem do problema e o aplicativo não tolera latências induzidas pela rede.
- Existem limitações de largura de banda na rede que conecta os clusters de origem e destino.

Replicação somente de instantâneo

A proteção de dados somente com snapshots replica os dados alterados em pontos específicos no tempo para um cluster remoto. Somente os snapshots criados no cluster de origem são replicados. As gravações ativas do volume de origem não são.

Você pode definir a frequência das replicações de snapshots.

A replicação de instantâneos não afeta a replicação assíncrona ou síncrona.

Replicação entre clusters Element e ONTAP usando SnapMirror

Com a tecnologia NetApp SnapMirror , você pode replicar snapshots criados com o software NetApp Element para o ONTAP para fins de recuperação de desastres. Em um relacionamento SnapMirror , o Element é um

endpoint e o ONTAP é o outro.

O SnapMirror é uma tecnologia de replicação de snapshots da NetApp que facilita a recuperação de desastres, projetada para failover do armazenamento primário para o armazenamento secundário em um local geograficamente remoto. A tecnologia SnapMirror cria uma réplica, ou espelho, dos dados em funcionamento em um armazenamento secundário, a partir do qual você pode continuar a fornecer dados caso ocorra uma interrupção no site principal. Os dados são replicados no nível de volume.

A relação entre o volume de origem no armazenamento primário e o volume de destino no armazenamento secundário é chamada de relação de proteção de dados. Os clusters são chamados de endpoints, nos quais os volumes residem, e os volumes que contêm os dados replicados devem ser interconectados. Uma relação ponto a ponto permite que clusters e volumes troquem dados com segurança.

O SnapMirror é executado nativamente nos controladores NetApp ONTAP e está integrado ao Element, que é executado em clusters NetApp HCI e SolidFire . A lógica para controlar o SnapMirror reside no software ONTAP ; portanto, todos os relacionamentos do SnapMirror devem envolver pelo menos um sistema ONTAP para realizar o trabalho de coordenação. Os usuários gerenciam os relacionamentos entre os clusters Element e ONTAP principalmente por meio da interface do usuário do Element; no entanto, algumas tarefas de gerenciamento residem no NetApp ONTAP System Manager. Os usuários também podem gerenciar o SnapMirror por meio da CLI e da API, ambas disponíveis no ONTAP e no Element.

Ver "TR-4651: Arquitetura e configuração do NetApp SolidFire SnapMirror" (login necessário)

Você deve habilitar manualmente a funcionalidade SnapMirror no nível do cluster usando o software Element. A funcionalidade SnapMirror está desativada por padrão e não é ativada automaticamente como parte de uma nova instalação ou atualização.

Após ativar o SnapMirror, você pode criar relacionamentos SnapMirror na guia Proteção de Dados do software Element.

O software NetApp Element versão 10.1 e superior suporta a funcionalidade SnapMirror para copiar e restaurar snapshots com sistemas ONTAP .

Sistemas que executam o Element 10.1 e versões superiores incluem código que pode se comunicar diretamente com o SnapMirror em sistemas ONTAP que executam a versão 9.3 ou superior. A API Element fornece métodos para habilitar a funcionalidade SnapMirror em clusters, volumes e snapshots. Além disso, a interface do usuário do Element inclui funcionalidades para gerenciar relacionamentos SnapMirror entre o software Element e os sistemas ONTAP .

A partir dos sistemas Element 10.3 e ONTAP 9.4, é possível replicar volumes originados no ONTAP para volumes do Element em casos de uso específicos, com funcionalidade limitada.

Para mais informações, consulte "Replicação entre o software NetApp Element e o ONTAP (CLI do ONTAP)".

Instantâneos de volume para proteção de dados

Um instantâneo de volume é uma cópia de um volume em um determinado momento, que você pode usar posteriormente para restaurar o volume para aquele momento específico.

Embora os snapshots sejam semelhantes aos clones de volume, eles são simplesmente réplicas dos metadados do volume, portanto, você não pode montá-los ou gravar neles. A criação de um snapshot de volume também requer apenas uma pequena quantidade de recursos e espaço do sistema, o que torna a criação de snapshots mais rápida do que a clonagem.

Você pode replicar snapshots para um cluster remoto e usá-los como uma cópia de backup do volume. Isso

permite reverter um volume para um ponto específico no tempo usando o snapshot replicado; você também pode criar um clone de um volume a partir de um snapshot replicado.

Você pode fazer backup de snapshots de um cluster Element para um armazenamento de objetos externo ou para outro cluster Element. Ao fazer backup de um snapshot para um armazenamento de objetos externo, você precisa ter uma conexão com esse armazenamento que permita operações de leitura/gravação.

Você pode tirar um instantâneo de um volume individual ou de vários volumes para proteção de dados.

Clones de volume

Um clone de um único volume ou de múltiplos volumes é uma cópia dos dados em um determinado momento. Ao clonar um volume, o sistema cria um instantâneo do volume e, em seguida, cria uma cópia dos dados referenciados por esse instantâneo.

Este é um processo assíncrono, e o tempo necessário para sua conclusão depende do tamanho do volume que você está clonando e da carga atual do cluster.

O cluster suporta até duas solicitações de clonagem em execução por volume simultaneamente e até oito operações de clonagem de volume ativas ao mesmo tempo. Solicitações que excedam esses limites são enfileiradas para processamento posterior.

Visão geral do processo de backup e restauração para o armazenamento Element.

Você pode fazer backup e restaurar volumes em outros armazenamentos SolidFire , bem como em armazenamentos de objetos secundários compatíveis com Amazon S3 ou OpenStack Swift.

Você pode fazer backup de um volume nos seguintes locais:

- Um cluster de armazenamento SolidFire
- Um armazenamento de objetos Amazon S3
- Um armazenamento de objetos OpenStack Swift

Ao restaurar volumes do OpenStack Swift ou do Amazon S3, você precisa das informações do manifesto do processo de backup original. Se você estiver restaurando um volume que foi salvo em um sistema de armazenamento SolidFire , nenhuma informação de manifesto será necessária.

Domínios de proteção

Um Domínio de Proteção é um nó ou um conjunto de nós agrupados de forma que qualquer parte dele, ou mesmo a sua totalidade, possa falhar, mantendo a disponibilidade dos dados. Os Domínios de Proteção permitem que um cluster de armazenamento se recupere automaticamente da perda de um chassi (afinidade de chassi) ou de um domínio inteiro (grupo de chassis).

Você pode habilitar manualmente o monitoramento do Domínio de Proteção usando o ponto de extensão de Configuração de NetApp Element no plug-in de NetApp Element para vCenter Server. Você pode selecionar um limite de Domínio de Proteção com base em domínios de nó ou chassi. Você também pode ativar o monitoramento do Domínio de Proteção usando a API do Element ou a interface web.

Um layout de Domínio de Proteção atribui cada nó a um Domínio de Proteção específico.

São suportados dois layouts diferentes de Domínio de Proteção, chamados níveis de Domínio de Proteção.

- No nível do nó, cada nó está em seu próprio Domínio de Proteção.
- No nível do chassi, apenas os nós que compartilham um chassi estão no mesmo Domínio de Proteção.
  - O layout em nível de chassi é determinado automaticamente a partir do hardware quando o nó é adicionado ao cluster.
  - Em um cluster onde cada nó está em um chassi separado, esses dois níveis são funcionalmente idênticos.

Ao criar um novo cluster, se você estiver usando nós de armazenamento que residem em um chassi compartilhado, considere projetar a proteção contra falhas em nível de chassi usando o recurso Domínios de Proteção.

Domínios de Proteção Personalizados

Você pode definir um layout de Domínio de Proteção personalizado que corresponda ao layout específico do seu chassi e nó, e onde cada nó esteja associado a um e apenas um Domínio de Proteção personalizado. Por padrão, cada nó é atribuído ao mesmo Domínio de Proteção personalizado padrão.

Caso não haja domínios de proteção personalizados atribuídos:

- O funcionamento do cluster não é afetado.
- O nível personalizado não é tolerante nem resiliente.

Ao configurar Domínios de Proteção personalizados para um cluster, existem três níveis de proteção possíveis, que podem ser visualizados no painel da interface web do Element:

- Sem proteção: O cluster de armazenamento não está protegido contra falhas em um de seus Domínios de Proteção personalizados. Para corrigir isso, adicione capacidade de armazenamento adicional ao cluster ou reconfigure os Domínios de Proteção personalizados do cluster para protegê-lo contra possível perda de dados.
- Tolerante a falhas: O cluster de armazenamento possui capacidade livre suficiente para evitar a perda de dados após a falha de um de seus Domínios de Proteção personalizados.
- Resistente a falhas: O cluster de armazenamento possui capacidade livre suficiente para se autorrecuperar após a falha de um de seus Domínios de Proteção personalizados. Após a conclusão do processo de recuperação, o cluster estará protegido contra perda de dados caso outros domínios apresentem falhas.

Se mais de um Domínio de Proteção personalizado for atribuído, cada subsistema atribuirá duplicatas a Domínios de Proteção personalizados separados. Caso isso não seja possível, o sistema recorre à atribuição de duplicados a nós separados. Cada subsistema (por exemplo, bins, slices, provedores de endpoints de protocolo e ensemble) faz isso de forma independente.

Você pode usar a interface do usuário do Element para"Configurar domínios de proteção personalizados" Ou você pode usar os seguintes métodos da API:

- "Layout do domínio de proteção"- Mostra em qual chassi e em qual Domínio de Proteção personalizado cada nó está localizado.
- "Layout de domínio de proteção definido"- Permite que um Domínio de Proteção personalizado seja atribuído a cada nó.

Alta disponibilidade da dupla hélice

A proteção de dados Double Helix é um método de replicação que distribui pelo menos duas cópias redundantes dos dados por todas as unidades de um sistema. A abordagem "sem RAID" permite que um sistema absorva múltiplas falhas simultâneas em todos os níveis do sistema de armazenamento e se recupere rapidamente.

Desempenho e qualidade do serviço

Um cluster de armazenamento SolidFire tem a capacidade de fornecer parâmetros de Qualidade de Serviço (QoS) por volume. Você pode garantir o desempenho do cluster medido em entradas e saídas por segundo (IOPS) usando três parâmetros configuráveis que definem a QoS: IOPS mínimo, IOPS máximo e IOPS de rajada.

O SolidFire Active IQ possui uma página de recomendações de QoS que fornece orientações sobre a configuração ideal e a definição das opções de QoS.

Parâmetros de Qualidade de Serviço

Os parâmetros IOPS são definidos das seguintes maneiras:

- **IOPS mínimo** - O número mínimo de entradas e saídas sustentadas por segundo (IOPS) que o cluster de armazenamento fornece a um volume. O IOPS mínimo configurado para um volume é o nível de desempenho garantido para esse volume. O desempenho não cai abaixo desse nível.
- **IOPS máximo** - O número máximo de IOPS sustentados que o cluster de armazenamento fornece a um volume. Quando os níveis de IOPS do cluster estão criticamente altos, esse nível de desempenho de IOPS não é excedido.
- **IOPS de rajada** - O número máximo de IOPS permitido em um cenário de rajada curta. Se um volume estiver operando abaixo do IOPS máximo, os créditos de burst serão acumulados. Quando os níveis de desempenho se tornam muito altos e são levados ao máximo, breves rajadas de IOPS são permitidas no volume.

  O software Element utiliza Burst IOPS quando um cluster está em execução em um estado de baixa utilização de IOPS do cluster.

  Um único volume pode acumular IOPS de pico e usar os créditos para ultrapassar seu IOPS máximo até o nível de IOPS de pico durante um "período de pico" definido. Um volume pode operar em modo burst por até 60 segundos, caso o cluster tenha capacidade para suportar o burst. Um volume acumula um segundo de crédito de burst (até um máximo de 60 segundos) para cada segundo em que o volume opera abaixo do seu limite máximo de IOPS.

  Os IOPS em rajadas são limitados de duas maneiras:

  - Um volume pode ultrapassar seu IOPS máximo por um número de segundos igual ao número de créditos de burst que o volume acumulou.
  - Quando um volume de operações ultrapassa sua configuração de IOPS máximo, ele é limitado pela configuração de IOPS de pico. Portanto, o IOPS de rajada nunca excede a configuração de IOPS de rajada para o volume.
- **Largura de banda máxima efetiva** - A largura de banda máxima é calculada multiplicando-se o número de IOPS (com base na curva de QoS) pelo tamanho da E/S.

Exemplo: As configurações de parâmetros de QoS de 100 IOPS mínimos, 1000 IOPS máximos e 1500 IOPS de rajada têm os seguintes efeitos na qualidade do desempenho:

- As cargas de trabalho conseguem atingir e manter um máximo de 1000 IOPS até que a condição de disputa por IOPS se torne evidente no cluster. Em seguida, as IOPS são reduzidas gradualmente até que as IOPS em todos os volumes estejam dentro dos intervalos de QoS designados e a disputa por desempenho seja aliviada.
- O desempenho em todos os volumes é otimizado para atingir o mínimo de 100 IOPS. Os níveis não caem abaixo da configuração de IOPS mínima, mas podem permanecer acima de 100 IOPS quando a disputa de carga de trabalho é aliviada.
- O desempenho nunca é superior a 1000 IOPS, nem inferior a 100 IOPS por um período prolongado. É permitido um desempenho de 1500 IOPS (IOPS de pico), mas apenas para os volumes que acumularam créditos de pico por operarem abaixo do IOPS máximo e somente por curtos períodos de tempo. Os níveis de pico nunca são sustentados.

limites de valor de QoS

Aqui estão os possíveis valores mínimos e máximos para QoS.

Parâmetros	Valor mínimo	Padrão	4 4KB	5 8KB	6 16 KB	262 KB
IOPS mínimo	50	50	15.000	9.375*	5556*	385*
IOPS máximo	100	15.000	200.000**	125.000	74.074	5128
IOPS de rajada	100	15.000	200.000**	125.000	74,074	5128

*Essas estimativas são aproximadas. **O IOPS máximo e o IOPS de rajada podem ser configurados para até 200.000; no entanto, essa configuração só é permitida para liberar efetivamente o desempenho de um volume. O desempenho máximo real de um volume é limitado pelo uso do cluster e pelo desempenho de cada nó.

desempenho de QoS

A curva de desempenho de QoS mostra a relação entre o tamanho do bloco e a porcentagem de IOPS.

O tamanho do bloco e a largura de banda têm um impacto direto no número de IOPS que um aplicativo pode obter. O software Element leva em consideração os tamanhos dos blocos recebidos, normalizando-os para 4k. Dependendo da carga de trabalho, o sistema poderá aumentar o tamanho dos blocos. À medida que o tamanho dos blocos aumenta, o sistema aumenta a largura de banda para um nível necessário para processar os blocos maiores. À medida que a largura de banda aumenta, o número de IOPS que o sistema consegue atingir diminui.

A curva de desempenho de QoS mostra a relação entre o aumento do tamanho dos blocos e a diminuição da porcentagem de IOPS:

Por exemplo, se os tamanhos dos blocos forem de 4k e a largura de banda for de 4000 KBps, o IOPS será de 1000. Se o tamanho dos blocos aumentar para 8k, a largura de banda aumenta para 5000 KBps e o IOPS diminui para 625. Ao levar em consideração o tamanho do bloco, o sistema garante que cargas de trabalho de menor prioridade que utilizam tamanhos de bloco maiores, como backups e atividades do hipervisor, não consumam grande parte do desempenho necessário para o tráfego de maior prioridade que utiliza tamanhos de bloco menores.

Políticas de QoS

Uma política de QoS permite criar e salvar uma configuração padronizada de qualidade de serviço que pode ser aplicada a vários volumes.

As políticas de QoS são mais adequadas para ambientes de serviço, por exemplo, com servidores de banco de dados, aplicativos ou infraestrutura que raramente são reinicializados e precisam de acesso constante e igualitário ao armazenamento. O QoS de volume individual é mais adequado para VMs de uso leve, como desktops virtuais ou VMs especializadas do tipo quiosque, que podem ser reinicializadas, ligadas ou desligadas diariamente ou várias vezes ao dia.

QoS e políticas de QoS não devem ser usadas em conjunto. Se você estiver usando políticas de QoS, não use QoS personalizado em um volume. A QoS personalizada substituirá e ajustará os valores da política de QoS para as configurações de QoS de volume.

O cluster selecionado deve ser Element 10.0 ou posterior para usar políticas de QoS; caso contrário, as funções de política de QoS não estarão disponíveis.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"

Informações sobre direitos autorais

Informações sobre marcas comerciais