Conceitos

Element Software

NetApp
November 13, 2025

Índice

Conceitos

Aprenda conceitos básicos relacionados ao software Element.

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

Visão geral do produto

Um sistema de storage all-flash da SolidFire é composto por componentes de hardware distintos (unidades e nós) combinados em um único pool de recursos de storage. Esse cluster unificado apresenta-se como um único sistema de storage para uso por clientes externos e é gerenciado com o software NetApp Element.

Com a interface Element, a API ou outras ferramentas de gerenciamento, você pode monitorar a capacidade e a performance de storage do cluster do SolidFire e gerenciar a atividade de storage em uma infraestrutura de alocação a vários clientes.

Recursos do SolidFire

Um sistema SolidFire fornece os seguintes recursos:

- Oferece storage de alto desempenho para sua infraestrutura de nuvem privada de grande escala
- Fornece uma escala flexível que permite atender às necessidades dinâmicas de storage
- Usa uma interface de software de elemento de gerenciamento de storage orientada por API
- Garante o desempenho usando políticas de qualidade de Serviço
- Inclui balanceamento de carga automático em todos os nós do cluster
- Reequilibra clusters automaticamente quando os nós são adicionados ou subtraídos

Implantação de SolidFire

Usar os nós de storage fornecidos pelo NetApp e integrados ao software NetApp Element.

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

Encontre mais informações

- "Plug-in do NetApp Element para vCenter Server"

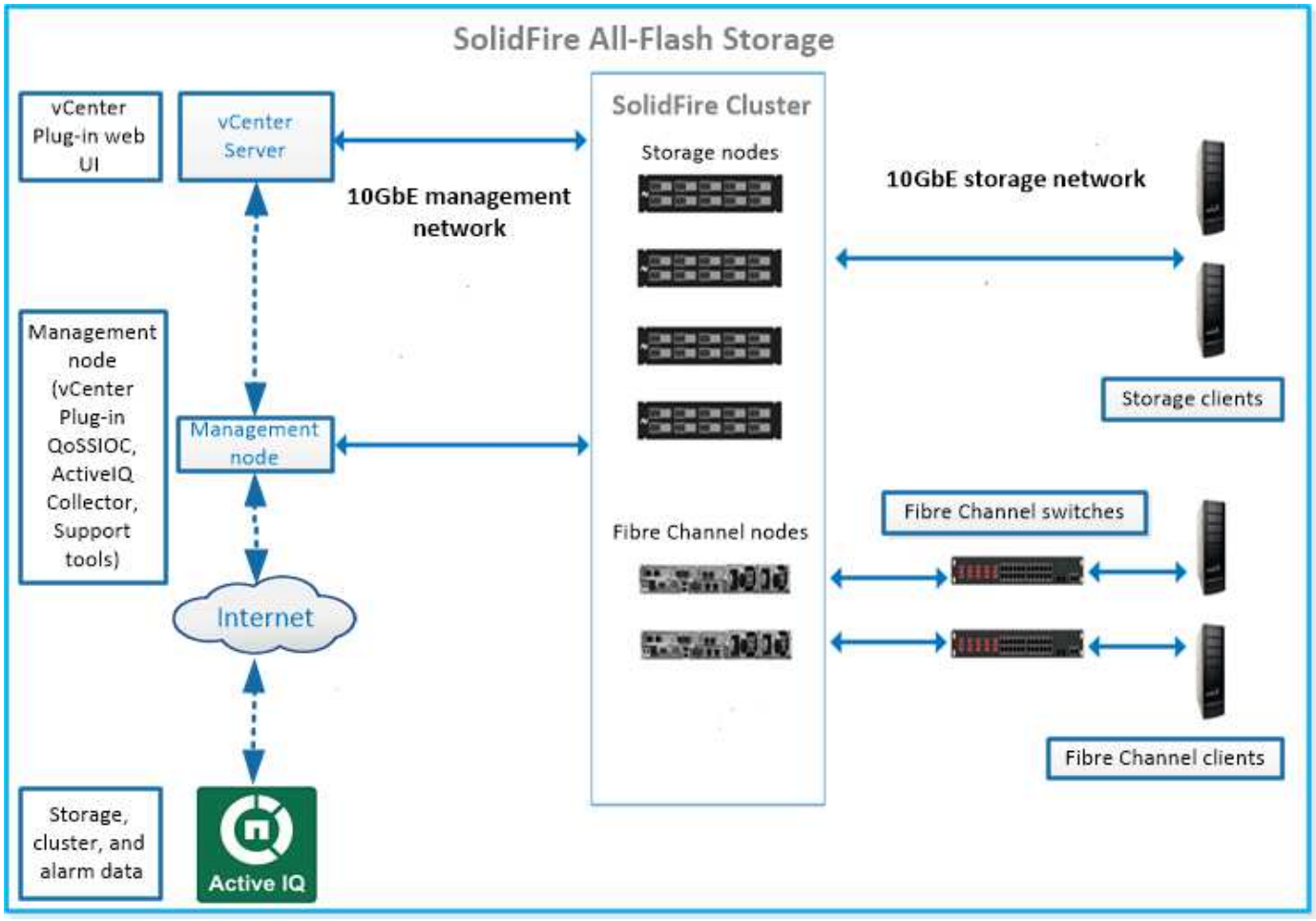
Arquitetura e componentes

Saiba mais sobre a arquitetura SolidFire .

Um sistema de storage all-flash da SolidFire é composto por componentes de hardware distintos (unidades e nós) combinados em um pool de recursos de storage com o software NetApp Element executado independentemente em cada nó. Esse único sistema de storage é gerenciado como uma única entidade usando a IU do software Element, a API e outras ferramentas de gerenciamento.

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

- **Cluster**: O hub do sistema de armazenamento SolidFire que é uma coleção de nós.
- * Nós*: Os componentes de hardware agrupados em um cluster. Existem dois tipos de nós:
  - Nós de storage, que são servidores que contêm uma coleção de unidades
  - Nós Fibre Channel (FC), usados para se conectar a clientes FC
- **Unidades**: Usado em nós de storage para armazenar dados para o cluster. Um nó de armazenamento contém dois tipos de unidades:
  - As unidades de metadados de volume armazenam informações 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 IU da Web do Element e outras ferramentas compatíveis:

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

URLs comuns

Esses são os URLs comuns que você usa com um sistema de storage all-flash SolidFire:

URL	Descrição
`https://[storage cluster MVIP address]`	Acesse a IU do software NetApp Element.
`https://activeiq.solidfire.com`	Monitore dados e receba alertas sobre gargalos de desempenho ou possíveis problemas de sistema.
`https://[management node IP address]`	Acesse o Controle de nuvem híbrida da NetApp para atualizar seus serviços de gerenciamento de instalação e atualização de storage.
`https://[IP address]:442`	A partir da IU por nó, acesse as configurações de rede e cluster e utilize testes e utilitários do sistema. "Saiba mais."
`https://[management node IP address]/mnode`	Use a API REST de serviços de gerenciamento e outras funcionalidades do nó de gerenciamento. "Saiba mais."
`https://[management node IP address]:9443`	Registre o pacote vCenter Plug-in no vSphere Web Client. "Saiba mais."

Encontre mais informações

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

Interfaces de software SolidFire

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

Opções

- Interface do usuário do software NetApp Element
- API do software NetApp Element
- Plug-in do NetApp Element para vCenter Server
- Controle de nuvem híbrida da NetApp
- UIs de nó de gestão
- Utilitários e ferramentas de integração adicionais

Interface do usuário do software NetApp Element

Permite configurar o storage Element, monitorar a capacidade e a performance do cluster e gerenciar as atividades de storage em uma infraestrutura de alocação a vários clientes. Element é o sistema operacional de storage no centro de um cluster SolidFire. O software Element é executado independentemente em todos os nós do cluster e permite que os nós do cluster combinem recursos que são apresentados como um único sistema de storage para clientes externos. O software Element é responsável por toda a coordenação, escala e gerenciamento de cluster do sistema como um todo. A interface do software é construída sobre a API Element.

"Gerenciar storage com o software Element"

API do software NetApp Element

Permite que você use um conjunto de objetos, métodos e rotinas para gerenciar o armazenamento de elementos. A API Element é baseada no protocolo JSON-RPC em HTTPS. Você pode monitorar operações de API na IU do Element habilitando o Registro de API; isso permite que você veja os métodos que estão sendo emitidos para o sistema. Você pode habilitar solicitações e respostas para ver como o sistema responde aos métodos que são emitidos.

"Gerencie o storage com a API Element"

Plug-in do NetApp Element para vCenter Server

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

"Plug-in do NetApp Element para vCenter Server"

Controle de nuvem híbrida da NetApp

Permite atualizar os serviços de gerenciamento e storage Element e gerenciar ativos de storage usando a interface de controle de nuvem híbrida da NetApp.

"Gerencie e monitore o storage com o controle de nuvem híbrida da NetApp"

UIs de nó de gestão

O nó de gerenciamento contém duas UIs: Uma IU para gerenciar serviços baseados EM REST e uma IU por nó para gerenciar configurações de rede e cluster e testes e utilitários do sistema operacional. Na IU da API REST, você pode acessar um menu de APIs relacionadas a serviços que controlam a funcionalidade do sistema baseado em serviços a partir do nó de gerenciamento.

Utilitários e ferramentas de integração adicionais

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

CLI do elemento

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

Ferramentas do Element PowerShell

"Ferramentas do Element PowerShell" Você pode usar uma coleção de funções do Microsoft Windows PowerShell que usam a API Element para gerenciar um sistema de storage SolidFire.

SDKs do elemento

"SDKs do elemento" Permita que você gerencie seu cluster SolidFire usando estas ferramentas:

- Element Java SDK: Permite aos programadores integrar a API Element com a linguagem de programação Java.
- Element .NET SDK: Permite aos programadores integrar a API Element com a plataforma de programação .NET.
- Element Python SDK: Permite aos programadores integrar a API Element com a linguagem de programação Python.

Pacote de testes da API do SolidFire Postman

Permite que os programadores usem uma coleção "Carteiro"de funções que testem chamadas de API Element.

Adaptador de replicação de armazenamento SolidFire

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

SolidFire Vro

"SolidFire Vro" Fornece uma maneira conveniente de usar a API Element para administrar seu sistema de storage SolidFire com o VMware vRealize Orchestrator.

Fornecedor VSS SolidFire

"Fornecedor VSS SolidFire" Integra cópias de sombra do VSS a clones e snapshots do Element.

Encontre mais informações

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

SolidFire Active IQ

"SolidFire Active IQ" é uma ferramenta baseada na web que fornece visualizações históricas continuamente atualizadas de dados em todo o cluster. Você pode configurar alertas para eventos, limites ou métricas específicos. Com o SolidFire Active IQ, você monitora a performance e a capacidade do sistema, além de se manter informado sobre a integridade do cluster.

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

- Número de nós e status dos nós: Saudável, offline ou falha

- Representação gráfica da CPU, uso de memória e limitação de nó
- Detalhes sobre o nó, como número de série, localização do slot no chassi, modelo e versão do software NetApp Element executado no nó de storage
- Informações relacionadas à CPU e ao armazenamento sobre as máquinas virtuais

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

Para mais informações

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

Nó de gerenciamento do software Element

"Nó de gerenciamento (mNode)"O é uma máquina virtual que é executada em paralelo com um ou mais clusters de storage baseados em software Element. Ele é usado para atualizar e fornecer serviços de sistema, incluindo monitoramento e telemetria, gerenciar ativos e configurações de cluster, executar testes e utilitários do sistema e habilitar o acesso ao suporte 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 relatam essas informações ao Active IQ para monitoramento remoto (se ativado). Os nós de gerenciamento também são responsáveis pela coordenação das atualizações de software dos nós do cluster.

A partir da versão do Element 11,3, o nó de gerenciamento funciona como um host microservice, permitindo atualizações mais rápidas de serviços de software selecionados fora das principais versões. Esses microsserviços ou "serviços de gestão" são atualizados frequentemente como pacotes de serviços.

Serviços de gerenciamento para storage all-flash SolidFire

A partir da versão do Element 11,3, **serviços de gerenciamento** são hospedados no "nó de gerenciamento", permitindo atualizações mais rápidas de serviços de software selecionados fora dos principais lançamentos.

Os serviços de gerenciamento fornecem recursos de gerenciamento central e estendido para storage all-flash SolidFire. Esses serviços incluem "Controle de nuvem híbrida da NetApp", telemetria do sistema Active IQ, log e atualizações de serviço, bem como o serviço QSSIOC para o plug-in Element para vCenter.

Saiba mais "lançamentos de serviços de gerenciamento"sobre o .

Nós

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

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

seguintes:

- Nó de gerenciamento
- Nó de storage
- Nó Fibre Channel

estados dos nós varia dependendo da associação de 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 de cluster, executar testes e utilitários do sistema e habilitar o acesso ao suporte NetApp para solução de problemas. "Saiba mais"

Nó de storage

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 metadados para storage e gerenciamento de dados. Cada nó contém uma imagem de fábrica do software NetApp Element.

Os nós de storage têm as seguintes características:

- Cada nó tem um nome exclusivo. Se um nome de nó não for especificado por um administrador, o padrão será SF-XXXX, onde XXXX é quatro carateres aleatórios gerados pelo sistema.
- Cada nó tem seu próprio cache de gravação de memória de acesso aleatório (NVRAM) não volátil de alto desempenho para melhorar o desempenho geral do sistema e reduzir a latência de gravação.
- Cada nó é conetado a duas redes, armazenamento e gerenciamento, cada um 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 storage ou adicionar nós de storage a um cluster existente para aumentar a capacidade de storage e a performance.
- 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 conetividade a um switch Fibre Channel, que você pode se conetar a clientes Fibre Channel. Os nós Fibre Channel agem como um conversor 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 têm as seguintes características:

- Os switches Fibre Channel gerenciam o estado da malha, fornecendo 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 a operação de outras portas.
- Vários pares de portas podem se comunicar simultaneamente em uma malha.

estados de operação do nó

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

- **Disponível**

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

- **Pendente**

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

  A autenticação não é necessária para acessar o nó.

- **Pendente ativo**

  O sistema está em processo de instalação do software Element compatível no nó. Quando concluído, o nó se moverá para o estado Ativo.

- **Ativo**

  O nó está participando de um cluster.

  A autenticação é necessária para modificar o nó.

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

Encontre mais informações

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

Clusters

Um cluster é o centro de um sistema de storage SolidFire e é composto por uma coleção de nós. É necessário ter pelo menos quatro nós em um cluster para que as eficiências de storage do SolidFire sejam obtidas. Um cluster aparece na rede como um único grupo lógico e pode ser acessado como armazenamento de bloco.

A criação de um novo cluster inicializa um nó como proprietário de comunicações para um cluster e estabelece 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 IU do Element ou a API.

É possível fazer escalabilidade horizontal de um cluster adicionando nós adicionais. Quando você adiciona um novo nó, não há interrupção do serviço e o cluster usa automaticamente a performance e a capacidade do novo nó.

Os administradores e hosts podem acessar o cluster usando endereços IP virtuais. Qualquer nó no cluster pode hospedar os endereços IP virtuais. O IP virtual de gerenciamento (MVIP) permite o gerenciamento de cluster por meio de uma conexão 1GbE, enquanto o IP virtual de armazenamento (SVIP) permite o acesso do host ao armazenamento por meio de uma conexão 10GbEG. 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 do elemento versão 11,0, os nós podem ser configurados com IPv4, IPv6 ou ambos os endereços para sua rede de gerenciamento. Isso se aplica aos nós de storage e aos nós de gerenciamento, com exceção do nó de gerenciamento 11,3 e posterior que não oferece suporte para 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 storage autoritativo
- Regra dos terços
- Capacidade ociosa
- Eficiência de storage
- Quorum do cluster de storage

Clusters de storage autoritativo

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 storage, ele será o cluster autoritativo. Se o nó de gerenciamento tiver dois ou mais clusters de storage, um desses clusters será atribuído como o cluster autoritativo e somente os usuários desse cluster poderão fazer login no controle de nuvem híbrida da NetApp. Para descobrir qual cluster é o cluster autorizado, você pode usar a `GET /mnode/about` API. Na resposta, o endereço IP `token_url` no campo é o endereço IP virtual de gerenciamento (MVIP) do cluster de armazenamento autorizado. Se você tentar fazer login no Controle de nuvem híbrida do NetApp como um usuário que não está no cluster autoritativo, a tentativa de login falhará.

Muitos recursos de controle de nuvem híbrida da NetApp foram desenvolvidos para funcionar com vários clusters de storage, mas a autenticação e a autorização têm limitações. A limitação em torno da autenticação e autorização é que o usuário do cluster autorizado pode executar ações em outros clusters vinculados ao Controle de nuvem híbrida NetApp mesmo que não seja um usuário nos outros clusters de armazenamento.

Antes de prosseguir com o gerenciamento de vários clusters de storage, você deve garantir que os usuários definidos nos clusters autoritativos sejam definidos em todos os outros clusters de storage com as mesmas permissões. Pode gerir utilizadores a partir do "Interface do usuário do software Element".

Consulte "criar e gerenciar ativos de cluster de storage" para obter mais informações sobre como trabalhar com ativos de cluster de storage de nós de gerenciamento.

Regra dos terços

Quando você mistura tipos de nós de storage em um cluster de storage da NetApp SolidFire, nenhum nó de storage pode conter mais de 33% da capacidade total do cluster de storage.

Capacidade ociosa

Se um nó recém-adicionado representar mais de 50% da capacidade total do cluster, parte da capacidade desse nó será inutilizável ("encalhado"), de modo que esteja em conformidade com a regra de capacidade. Esse continua sendo o caso até que mais capacidade de storage seja adicionada. Se um nó muito grande for adicionado que também desobedeça à regra de capacidade, o nó anteriormente encalhado não ficará mais encalhado, enquanto o nó recém-adicionado fica encalhado. A capacidade deve ser sempre adicionada em pares para evitar que isso aconteça. Quando um nó fica preso, uma falha de cluster apropriada é lançada.

Eficiência de storage

Os clusters de storage do NetApp SolidFire utilizam deduplicação, compactação e thin Provisioning para reduzir a quantidade de storage físico necessária para armazenar um volume.

- **Compressão**

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

- **Desduplicação**

  A deduplicação reduz a quantidade de storage físico necessária para um volume descartando blocos de dados duplicados.

- * Provisionamento thin*

  Um volume ou LUN com thin Provisioning é aquele para o qual o storage não é reservado com antecedência. Em vez disso, o storage é alocado dinamicamente, conforme necessário. O espaço livre é liberado de volta ao sistema de armazenamento quando os dados no volume ou LUN são excluídos

Quorum do cluster de storage

O software Element cria um cluster de storage a partir de nós selecionados, que mantém um banco de dados replicado da configuração do cluster. É necessário um mínimo de três nós para participar do conjunto de cluster para manter o quorum para resiliência de cluster.

Segurança

Quando você usa seu sistema de storage all-flash SolidFire, seus dados são protegidos por protocolos de segurança padrão do setor.

Criptografia em repouso (hardware)

Todas as unidades nos nós de storage são capazes de criptografia aproveitar a criptografia AES de 256 bits no nível da unidade. Cada unidade tem sua própria chave de criptografia, que é criada quando a unidade é inicializada pela primeira vez. Quando você ativa o recurso de criptografia, uma senha em todo o cluster é criada e partes da senha são então distribuídas para todos os nós do cluster. Nenhum nó único armazena a senha inteira. A senha é então usada para proteger com senha todo o acesso às unidades. A senha é necessária para desbloquear a unidade e, em seguida, não é necessária, a menos que a energia seja removida da unidade ou a unidade esteja bloqueada.

"Ativar o recurso de criptografia de hardware em repouso" não afeta o desempenho ou a eficiência no cluster. Se uma unidade ou nó habilitado para criptografia for removido da configuração do cluster com a API Element ou a IU do Element, a criptografia em repouso será desativada nas unidades. Depois que a unidade é removida, a unidade pode ser protegida apagada usando o `SecureEraseDrives` método API. Se uma unidade física ou nó for removido à força, os dados permanecerão protegidos pela senha de todo o cluster e pelas chaves de criptografia individuais da unidade.

Criptografia em repouso (software)

Outro tipo de criptografia em repouso, a criptografia de software em repouso permite que todos os dados gravados em SSDs em um cluster de storage sejam criptografados. "Quando ativado", criptografa todos os

dados gravados e descriptografa todos os dados lidos automaticamente no software. A criptografia de software em repouso espelha a implementação do SED (Self-Encrypting Drive) no hardware para fornecer segurança de dados na ausência de SED.

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

A criptografia em repouso baseada em software e hardware pode ser usada independentemente ou em combinação com a outra.

Gerenciamento de chaves externas

Você pode configurar o software Element para usar um KMS (serviço de gerenciamento de chaves em conformidade com KMIP) de terceiros para gerenciar chaves de criptografia de cluster de storage. Quando você ativa esse recurso, a chave de criptografia de senha de acesso à unidade em todo o cluster de armazenamento é gerenciada por um KMS que você especificar.

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

- Gemalto SafeNet KeySecure
- SAFENET NA KeySecure
- HyTrust KeyControl
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

Para obter mais informações sobre como configurar o gerenciamento de chaves externas, "comece a usar o gerenciamento de chaves externas" consulte a documentação.

Autenticação de vários fatores

A autenticação multifator (MFA) permite exigir que os usuários apresentem vários tipos de evidências para se autenticar com a IU da Web ou a IU do nó de storage do NetApp Element no login. Você pode configurar o Element para aceitar apenas autenticação multifator para logins integrados ao seu sistema de gerenciamento de usuário e provedor de identidade existente. Você pode configurar o Element para integrar com 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 emparelhar a autenticação multifator com provedores de identidade (IDPs) compatíveis com SAML 2,0 comuns, como o Microsoft ative Directory Federation Services (ADFS) e o Shibboleth.

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

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

Os clusters de storage do NetApp SolidFire oferecem suporte a criptografia em conformidade com os requisitos FIPS (Federal Information Processing Standard) 140-2 para módulos criptográficos. Você pode ativar a conformidade com o FIPS 140-2 no cluster do SolidFire para comunicações HTTPS e criptografia de unidade.

Quando você ativa o modo operacional FIPS 140-2 no cluster, o cluster ativa o módulo de segurança criptográfica (NCSM) do NetApp e aproveita a criptografia com certificação FIPS 140-2 nível 1 para todas as comunicações via HTTPS para a IU e API do NetApp Element. Use a `EnableFeature` API Element com o

`fips` parâmetro para habilitar a criptografia HTTPS FIPS 140-2. Em clusters de storage com hardware compatível com FIPS, você também pode ativar a criptografia de unidade FIPS para dados em repouso usando a `EnableFeature` API Element com o `FipsDrives` parâmetro.

Para obter mais informações sobre como preparar um novo cluster de armazenamento para criptografia FIPS 140-2-2, "Criar um cluster compatível com unidades FIPS"consulte .

Para obter mais informações sobre como ativar o FIPS 140-2 em um cluster preparado existente, "A API EnableFeature Element"consulte .

Para mais informações

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

Contas e permissões

Para administrar e fornecer acesso a recursos de storage em seu sistema, você precisará configurar contas para recursos do sistema.

Com o storage Element, você pode criar e gerenciar os seguintes tipos de contas:

- Contas de usuário do administrador para o cluster de armazenamento
- Contas de usuário para acesso ao volume de armazenamento
- Contas de usuários de cluster autoritativas para o controle de nuvem híbrida da NetApp

Contas de administrador de cluster de storage

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

- **Conta de administrador de cluster principal**: Esta conta de administrador é criada quando o cluster é criado. Esta conta é a conta administrativa primária com o mais alto nível de acesso ao cluster. Essa conta é análoga a um usuário root em um sistema Linux. Pode alterar a palavra-passe desta conta de administrador.
- **Conta de administrador de cluster**: Você pode dar a uma conta de administrador de cluster um intervalo limitado de acesso administrativo 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 IU de elementos no sistema de storage.

> É necessária uma conta de administrador de cluster local (não LDAP) para aceder a nós ativos num cluster através da IU por nó. As credenciais da conta não são necessárias para acessar um nó que ainda não faz parte de um cluster.

Você pode "gerenciar contas de administrador de cluster"criar, excluir e editar contas de administrador de cluster, alterar a senha do administrador de cluster e configurar configurações LDAP para gerenciar o acesso do sistema para os usuários.

Contas de utilizador

As contas de usuário são usadas para controlar o acesso aos recursos de armazenamento em uma rede baseada no software NetApp Element. Pelo menos uma conta de usuário é necessária antes que um volume possa ser criado.

Quando você cria um volume, ele é atribuído a uma conta. Se você criou um volume virtual, a conta será o recipiente de armazenamento.

Aqui estão algumas considerações adicionais:

- A conta contém a autenticação CHAP necessária para acessar os volumes atribuídos a ela.
- Uma conta pode ter até 2000 volumes atribuídos a ela, mas um volume pode pertencer a apenas uma conta.
- As contas de usuário podem ser gerenciadas a partir do ponto de extensão Gerenciamento do NetApp Element.

Contas de usuário de cluster autoritativas

As contas de usuários de cluster autoritativas podem se autenticar em qualquer ativo de storage associado à instância de controle de nuvem híbrida da NetApp de nós e clusters. Com essa conta, você pode gerenciar volumes, contas, grupos de acesso e muito mais em todos os clusters.

As contas de usuário autoritativas são gerenciadas a partir do menu superior direito opção Gerenciamento de usuários no Controle de nuvem híbrida do NetApp.

O "cluster de storage autoritativo" é o cluster de storage que o Controle de nuvem híbrida da NetApp usa para autenticar usuários.

Todos os usuários criados no cluster de storage autoritativo podem fazer login no controle de nuvem híbrida da NetApp. Os 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 storage, ele será o cluster autoritativo.
- Se o nó de gerenciamento tiver dois ou mais clusters de storage, um desses clusters será atribuído como o cluster autoritativo e somente os usuários desse cluster poderão fazer login no controle de nuvem híbrida da NetApp.

Embora muitos recursos de controle de nuvem híbrida da NetApp funcionem com vários clusters de storage, a autenticação e a autorização têm as limitações necessárias. A limitação em torno da autenticação e autorização é que os usuários do cluster autoritativo podem executar ações em outros clusters vinculados ao Controle de nuvem híbrida NetApp mesmo que não sejam um usuário nos outros clusters de armazenamento. Antes de prosseguir com o gerenciamento de vários clusters de storage, você deve garantir que os usuários definidos nos clusters autoritativos sejam definidos em todos os outros clusters de storage com as mesmas permissões. Você pode gerenciar usuários a partir do controle de nuvem híbrida da NetApp.

Contas de volume

As contas específicas de volume são específicas apenas para o cluster de armazenamento em que foram criadas. Essas contas permitem que você defina permissões em volumes específicos na rede, mas não têm efeito fora desses volumes.

As contas de volume são gerenciadas na tabela volumes de controle de nuvem híbrida da NetApp.

Armazenamento

Volumes

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

O storage Element permite criar, exibir, 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 de volume.

Volumes persistentes

Os volumes persistentes permitem que os dados de configuração do nó de gerenciamento sejam armazenados em um cluster de storage especificado, em vez de localmente com uma VM, para que os dados possam ser preservados em caso de perda ou remoção do nó de gerenciamento. Volumes persistentes são uma configuração de nó de gerenciamento opcional, mas recomendada.

Uma opção para ativar volumes persistentes está incluída nos scripts de instalação e atualização quando "implantando um novo nó de gerenciamento"o . Os volumes persistentes são volumes em um cluster de storage baseado em software Element que contém informações de configuração de nó de gerenciamento para a VM do nó de gerenciamento de host que permanecem além da vida útil da VM. Se o nó de gerenciamento for perdido, uma VM de nó de gerenciamento de substituição poderá se reconetar e recuperar dados de configuração da VM perdida.

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

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

Volumes virtuais (vVols)

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

Ligações

O cluster do NetApp Element escolhe um ponto de extremidade de protocolo ideal, cria uma ligação que associa o host ESXi e o volume virtual ao ponto de extremidade do protocolo e retorna a ligação ao host ESXi. Depois que estiver vinculado, o host ESXi pode executar operações de e/S com o volume virtual vinculado.

Endpoints do protocolo

Os hosts do 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 de protocolo associado direciona e/S para o volume virtual com o qual é emparelhado.

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 endpoint de protocolo correspondente. Por exemplo, um cluster de quatro nós terá quatro pontos de extremidade de protocolo.

ISCSI é o único protocolo suportado para o software NetApp Element. O protocolo Fibre Channel não é suportado. Os endpoints de 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 de volume.

Contêineres de armazenamento

Os contêineres de storage são construções lógicas que mapeiam para contas NetApp Element e são usados para geração de relatórios e alocação de recursos. Eles agregam capacidade de storage bruto ou funcionalidades de storage agregado que o sistema de storage pode fornecer a volumes virtuais. Um datastore VVol criado no vSphere é mapeado para um contentor de storage individual. Por padrão, um único contêiner de storage tem todos os recursos disponíveis no cluster do NetApp Element. Se for necessária uma governança mais granular para a alocação a vários clientes, é possível criar vários contêineres de storage.

Os contêineres de armazenamento funcionam como contas tradicionais e podem conter volumes virtuais e volumes tradicionais. Suporte para um máximo de quatro contêineres de storage por cluster. É necessário pelo menos um contêiner de storage para usar a funcionalidade do Vols. Você pode descobrir contêineres de storage no vCenter durante a criação do Vols.

Fornecedor VASA

Para que o vSphere fique ciente do recurso vVol no cluster do NetApp Element, o administrador do vSphere deve Registrar o provedor NetApp Element VASA no vCenter. O provedor VASA é o caminho de controle fora da banda entre o vSphere e o cluster do Element. Ele é responsável pela execução de solicitações no cluster Element em nome do vSphere, como criação de VMs, disponibilização de VMs para o vSphere e publicidade de recursos de storage para o vSphere.

O provedor VASA é executado como parte do mestre do cluster no software Element. O mestre de cluster é um serviço altamente disponível que faz failover para qualquer nó no cluster, conforme necessário. Se o master do cluster falhar, o provedor VASA se move com ele, garantindo alta disponibilidade para o provedor VASA. Todas as tarefas de gerenciamento de provisionamento e armazenamento usam o provedor VASA, que lida com todas as alterações necessárias no cluster do Element.

Para o Element 12,5 e anterior, não Registre mais de um provedor NetApp Element VASA em uma única instância do vCenter. Quando um segundo provedor NetApp Element VASA é adicionado, isso torna todos os armazenamentos de dados VVOL inacessíveis.

O suporte DO VASA para até 10 vCenters está disponível como um patch de atualização se você já registrou um provedor VASA no vCenter. Para instalar, siga as instruções no manifesto VASA39 e baixe o arquivo .tar.gz do "Transferências de software da NetApp"site. O fornecedor NetApp Element VASA utiliza um certificado NetApp. Com esse patch, o certificado é usado não modificado pelo vCenter para oferecer suporte a vários vCenters para uso em VASA e VVols. Não modifique o certificado. Certificados SSL personalizados não são suportados pela VASA.

Encontre mais informações

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

Grupos de acesso de volume

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

Os grupos de acesso de volume no armazenamento NetApp SolidFire permitem que os IQNs do iniciador iSCSI ou WWPNs do Fibre Channel acessem uma coleção de volumes. Cada IQN que você adicionar a um grupo de acesso pode acessar cada volume no grupo sem usar a autenticação CHAP. Cada WWPN que você adicionar a um grupo de acesso permite o acesso à rede Fibre Channel aos volumes no grupo de acesso.

Os grupos de acesso ao volume têm os seguintes limites:

- Um máximo de 128 iniciadores por grupo de acesso de volume.
- Um máximo de 64 grupos de acesso por volume.
- Um grupo de acesso pode ser composto por um máximo de 2000 volumes.
- Um IQN ou WWPN pode pertencer a apenas um grupo de acesso de volume.
- Para clusters Fibre Channel, um único volume pode pertencer a um máximo de quatro grupos de acesso.

Iniciadores

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

A proteção de dados de storage do Element inclui os seguintes conceitos:

- Tipos de replicação remota
- Snapshots de volume para proteção de dados
- Clones de volume
- Visão geral do processo de backup e restauração para armazenamento de elementos

- Domínios de proteção
- Domínios de proteção personalizados
- Dupla Helix alta disponibilidade

Tipos de replicação remota

A replicação remota de dados pode assumir as seguintes formas:

- Replicação síncrona e assíncrona entre clusters
- Replicação somente snapshot
- Replicação entre clusters Element e ONTAP com o SnapMirror

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

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.

É possível emparelhar um cluster de storage com até quatro outros clusters de storage. É possível replicar dados de volume de forma síncrona ou assíncrona de qualquer cluster em um par de cluster 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 pela latência, perda de pacotes, jitter e largura de banda.

A replicação síncrona é apropriada para as seguintes situações:

- Replicação de vários sistemas a uma curta distância
- Um local de recuperação de desastres que é geograficamente local para a fonte
- Aplicações sensíveis ao tempo e à proteção de bancos de dados
- Aplicações de continuidade dos negócios que exigem que o local secundário atue como o local principal quando o local principal está inativo

Replicação assíncrona

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

A replicação assíncrona é apropriada para as seguintes situações:

- O local de recuperação de desastre está longe de ser a fonte, e a aplicação não tolera latências induzidas pela rede.
- Há limitações de largura de banda na rede conetando os clusters de origem e destino.

Replicação somente snapshot

A proteção de dados somente snapshot replica os dados alterados em momentos específicos para um cluster

remoto. Somente os snapshots criados no cluster de origem são replicados. As gravações ativas do volume de origem não são.

É possível definir a frequência das replicações de instantâneos.

A replicação Snapshot não afeta a replicação assíncrona ou síncrona.

Replicação entre clusters Element e ONTAP com o SnapMirror

Com a tecnologia NetApp SnapMirror, é possível replicar snapshots obtidos usando o software NetApp Element para a ONTAP para fins de recuperação de desastres. Em uma relação SnapMirror, Element é um endpoint e ONTAP é o outro.

O SnapMirror é uma tecnologia de replicação Snapshot da NetApp que facilita a recuperação de desastres, projetada para failover de armazenamento primário para armazenamento secundário em um local remoto geograficamente. A tecnologia SnapMirror cria uma réplica, ou espelho, dos dados em funcionamento no storage secundário a partir da qual você pode continuar fornecendo dados se houver interrupção no local primário. Os dados são espelhados no nível do volume.

A relação entre o volume de origem no storage primário e o volume de destino no storage secundário é chamada de relação de proteção de dados. Os clusters são referidos como pontos de extremidade nos quais os volumes residem e os volumes que contêm os dados replicados devem ser colocados em campo. Um relacionamento de pares permite que clusters e volumes troquem dados com segurança.

O SnapMirror é executado nativamente nas controladoras NetApp ONTAP e é integrado ao Element, que é executado nos clusters NetApp HCI e SolidFire. A lógica para controlar o SnapMirror reside no software ONTAP; portanto, todas as relações do SnapMirror devem envolver pelo menos um sistema ONTAP para executar o trabalho de coordenação. Os usuários gerenciam relacionamentos entre clusters Element e ONTAP principalmente por meio da IU do Element. No entanto, algumas tarefas de gerenciamento residem no Gerenciador de sistemas do NetApp ONTAP. Os usuários também podem gerenciar o SnapMirror por meio da CLI e da API, que estão disponíveis no ONTAP e no Element.

Consulte "TR-4651: Arquitetura e Configuração do NetApp SolidFire SnapMirror" (login necessário)

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

Depois de ativar o SnapMirror, você pode criar relacionamentos do SnapMirror a partir da guia proteção de dados no software Element.

O software NetApp Element 10,1 e superior suporta a funcionalidade SnapMirror para copiar e restaurar snapshots com sistemas ONTAP.

Os sistemas que executam o elemento 10,1 e acima incluem código que pode se comunicar diretamente com o SnapMirror em sistemas ONTAP executando 9,3 ou superior. A API do Element fornece métodos para habilitar a funcionalidade do SnapMirror em clusters, volumes e snapshots. Além disso, a IU do Element inclui recursos para gerenciar as relações do 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 do ONTAP para volumes de elementos em casos de uso específicos com funcionalidade limitada.

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

Snapshots de volume para proteção de dados

Um snapshot de volume é uma cópia pontual de um volume que você poderia usar posteriormente para restaurar um volume para esse tempo específico.

Embora os snapshots sejam semelhantes aos clones de volume, os snapshots são simplesmente réplicas de metadados de volume, para que você não possa montá-los ou gravá-los. A criação de um snapshot de volume também exige apenas uma pequena quantidade de recursos e espaço do sistema, o que torna a criação de snapshot 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.

É possível fazer backup de snapshots de um cluster de elementos para um armazenamento de objetos externo ou para outro cluster de elementos. Ao fazer backup de um snapshot em um armazenamento de objetos externo, você deve ter uma conexão com o armazenamento de objetos que permita operações de leitura/gravação.

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

Clones de volume

Um clone de um único volume ou vários volumes é uma cópia pontual dos dados. Quando você clonar um volume, o sistema cria um snapshot do volume e cria uma cópia dos dados referenciados pelo snapshot.

Este é um processo assíncrono, e a quantidade de tempo que o processo requer depende do tamanho do volume que você está clonando e da carga atual do cluster.

O cluster dá suporte a até duas solicitações de clone em execução por volume de cada vez e até oito operações de clone de volume ativo de cada vez. Solicitações além desses limites são enfileiradas para processamento posterior.

Visão geral do processo de backup e restauração para armazenamento de elementos

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

Pode efetuar uma cópia de segurança de um volume para o seguinte:

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

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

Domínios de proteção

Um domínio de proteção é um nó ou um conjunto de nós agrupados de modo que qualquer parte ou até mesmo todos eles possam falhar, mantendo a disponibilidade dos dados. Os domínios de proteção permitem

que um cluster de armazenamento recupere automaticamente da perda de um chassi (afinidade de chassi) ou de um domínio inteiro (grupo de chassi).

Você pode ativar manualmente o monitoramento de domínio de proteção usando o ponto de extensão de configuração do NetApp Element no plug-in do 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 Element ou a IU da Web.

Um layout do domínio de proteção atribui cada nó a um domínio de proteção específico.

Dois layouts diferentes de domínio de proteção, chamados níveis de domínio de proteção, são suportados.

- 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 do nível do 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 storage que residem em um chassi compartilhado, considere a possibilidade de criar uma proteção contra falhas no nível do chassi usando o recurso domínios de proteção.

domínios de proteção personalizados

Você pode definir um layout personalizado do domínio de proteção que corresponda ao layout específico do chassi e do nó e onde cada nó está associado a um e apenas um domínio de proteção personalizado. Por padrão, cada nó é atribuído ao mesmo domínio de proteção personalizado padrão.

Se não forem atribuídos domínios de proteção personalizados:

- A operação do cluster não é afetada.
- O nível personalizado não é tolerante nem resiliente.

Quando você configura domínios de proteção personalizados para um cluster, há três níveis possíveis de proteção, que você pode ver no painel da IU da Web do Element:

- Não protegido: O cluster de armazenamento não está protegido contra a falha de 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 proteger o cluster contra possíveis perdas de dados.
- Tolerante a falhas: O cluster de armazenamento tem 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 tem capacidade livre suficiente para se auto-curar após a falha de um de seus domínios de proteção personalizados. Após a conclusão do processo de recuperação, o cluster será protegido contra a perda de dados se domínios adicionais falharem.

Se mais de um domínio de proteção personalizado for atribuído, cada subsistema atribuirá duplicatas a domínios de proteção personalizados separados. Se isso não for possível, ele reverte a atribuir duplicatas a nós separados. Cada subsistema (por exemplo, compartimentos, fatias, provedores de endpoint de protocolo e ensemble) faz isso de forma independente.

Você pode usar a IU do Element para "Configurar domínios de proteção personalizados"ou usar os seguintes métodos de API:

- "GetProtectionDomainLayout" - Mostra em qual chassi e em qual domínio de proteção personalizado cada nó está.
- "SetProtectionDomainLayout" - Permite que um domínio de proteção personalizado seja atribuído a cada nó.

Dupla Helix alta disponibilidade

A proteção de dados Double Helix é um método de replicação que espalha pelo menos duas cópias redundantes de dados em todas as unidades dentro de um sistema. A abordagem "sem RAID" permite que um sistema absorva várias falhas simultâneas em todos os níveis do sistema de storage e faça o reparo rapidamente.

Desempenho e qualidade do serviço

Um cluster de storage da SolidFire pode fornecer parâmetros de qualidade do 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 QoS: Min IOPS, Max IOPS e Burst IOPS.

O SolidFire Active IQ tem uma página de recomendações de QoS que fornece conselhos sobre a configuração ideal e a configuração de configurações de QoS.

Parâmetros de qualidade do serviço

Os parâmetros de 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 garantido de desempenho para um volume. O desempenho não desce abaixo deste nível.
- **IOPS máximo** - o número máximo de IOPS contínuo que o cluster de armazenamento fornece a um volume. Quando os níveis de IOPS do cluster são extremamente altos, esse nível de desempenho de IOPS não é excedido.
- **IOPS de explosão** - o número máximo de IOPS permitido em um cenário de pico curto. Se um volume estiver em execução abaixo do IOPS máximo, os créditos de pico sazonal serão acumulados. Quando os níveis de desempenho se tornam muito altos e são empurrados para os níveis máximos, pequenas explosões de IOPS são permitidas no volume.

  O software Element usa IOPS Burst quando um cluster está sendo executado em um estado de baixa utilização de IOPS do cluster.

  Um único volume pode acumular IOPS Burst e usar os créditos para estourar acima de seu IOPS máximo até seu nível de IOPS Burst por um "período de explosão" definido. Um volume pode estourar por até 60 segundos se o cluster tiver a capacidade de acomodar a sobrecarga. Um volume acumula um segundo de crédito de explosão (até um máximo de 60 segundos) para cada segundo em que o volume é executado abaixo do limite máximo de IOPS.

  As IOPS de explosão são limitadas de duas maneiras:

- Um volume pode estourar acima de seu IOPS máximo por um número de segundos igual ao número de créditos de explosão acumulados pelo volume.
- Quando um volume ultrapassa sua configuração de IOPS máximo, ele é limitado por sua configuração IOPS Burst. Portanto, o IOPS de pico contínuo nunca excede a configuração IOPS de pico contínuo do volume.

- **Largura de banda máxima efetiva** - a largura de banda máxima é calculada multiplicando o número de IOPS (com base na curva de QoS) pelo tamanho de e/S.

  Exemplo: As configurações de parâmetros de QoS de 100 IOPS mínimo, 1000 IOPS máximo e 1500 IOPs Burst têm os seguintes efeitos na qualidade do desempenho:

  - Os workloads podem alcançar e sustentar um máximo de 1000 IOPS até que a condição de contenção de workload para IOPS fique aparente no cluster. Em seguida, as IOPS são reduzidas de forma incremental até que as IOPS em todos os volumes estejam dentro dos intervalos de QoS designados e a contenção de desempenho seja aliviada.
  - A performance em todos os volumes é empurrada para o IOPS mínimo de 100K. Os níveis não ficam abaixo da configuração min IOPS, mas podem permanecer acima de 100 IOPS quando a contenção de workload é aliviada.
  - A performance nunca é superior a 1000 IOPS ou inferior a 100 IOPS por um período contínuo. O desempenho de 1500 IOPS (IOPS Burst) é permitido, mas somente para os volumes que acumularam créditos de explosão executando abaixo de IOPS máximo e permitido por curtos períodos de tempo. Os níveis de explosão nunca são sustentados.

Limites de valor de QoS

Aqui estão os possíveis valores mínimos e máximos para QoS.

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

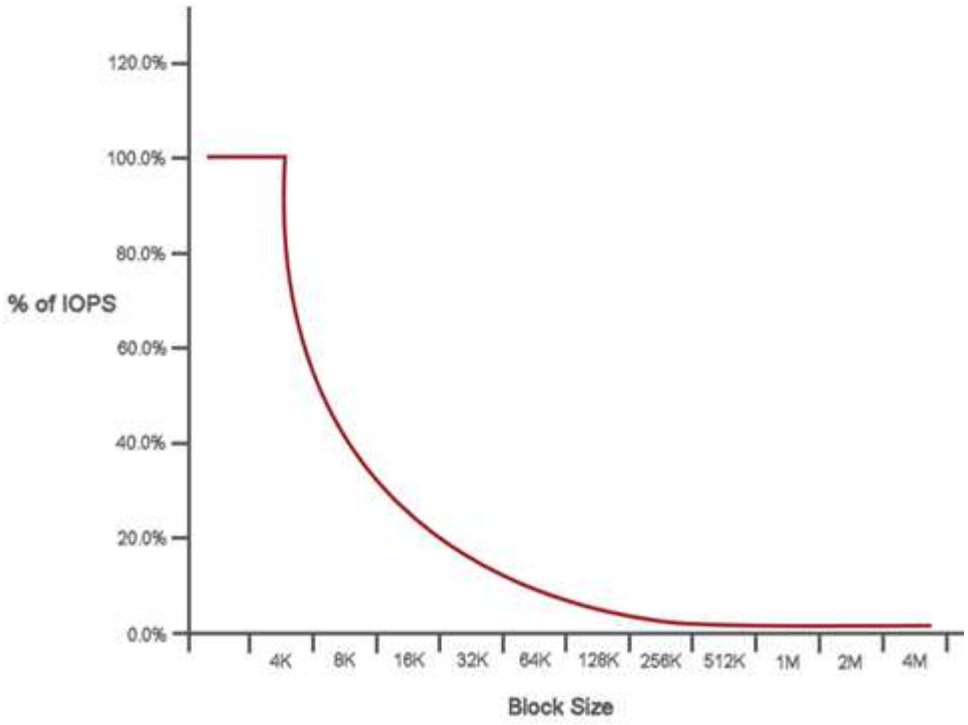
*Estas estimativas são aproximadas. **IOPS máximo e IOPS de explosão podem ser definidos até 200.000K; no entanto, essa configuração só pode ser descompactada efetivamente o desempenho de um volume. O desempenho máximo de um volume no mundo real é limitado pelo uso do cluster e pelo desempenho por nó.

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 impactos direto no número de IOPS que um aplicativo pode obter. O software Element leva em conta os tamanhos de bloco que recebe normalizando os tamanhos de bloco para 4K. Com base no workload, o sistema pode aumentar os tamanhos de blocos. À medida que os tamanhos de blocos aumentam, o sistema aumenta a largura de banda para um nível necessário para processar os tamanhos de blocos maiores. À medida que a largura de banda aumenta o número de IOPS, o sistema pode atingir diminuições.

A curva de desempenho de QoS mostra a relação entre o aumento dos tamanhos de bloco e a porcentagem decrescente de IOPS:



Por exemplo, se os tamanhos de bloco forem 4K e a largura de banda for 4000 kbps, as IOPS são 1000. Se os tamanhos de bloco aumentarem para 8k, a largura de banda aumenta para 5000 kbps e o IOPS diminui para 625. Levando em consideração o tamanho dos blocos, o sistema garante que workloads de prioridade mais baixa que usam tamanhos de bloco mais altos, como backups e atividades de hipervisor, não levem muito da performance necessária ao tráfego de prioridade mais alta usando tamanhos de bloco menores.

Políticas de QoS

Uma política de QoS permite que você crie e salve uma configuração padronizada de qualidade de serviço que pode ser aplicada a muitos volumes.

As políticas de QoS são melhores para ambientes de serviço, por exemplo, com servidores de banco de dados, aplicativos ou infraestrutura que raramente reiniciam e precisam de acesso igual e constante ao storage. A QoS de volume individual é a melhor 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.

As políticas de QoS e QoS não devem ser usadas juntas. 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 configurações de QoS de volume.

O cluster selecionado deve ser o elemento 10,0 ou posterior para usar políticas de QoS; caso contrário, as funções de política de QoS não estão disponíveis.

Encontre mais informações

- "Documentação do software SolidFire e Element"

Informações sobre direitos autorais

Informações sobre marcas comerciais