Conceitos

NetApp HCI

NetApp
November 18, 2025

Índice

Conceitos

Visão geral do produto NetApp HCI

O NetApp HCI é um design de infraestrutura de nuvem híbrida em escala empresarial que combina storage, computação, rede e hipervisor. Além disso, adiciona funcionalidades que englobam nuvens públicas e privadas.

A infraestrutura de nuvem híbrida desagregada da NetApp permite o dimensionamento independente da computação e do storage, adaptando-se a workloads com desempenho garantido.

- Atende à demanda de multicloud híbrida
- Dimensiona computação e o storage de forma independente
- Simplifica a orquestração de serviços de dados em várias nuvens híbridas

Componentes do NetApp HCI

Aqui está uma visão geral dos vários componentes do ambiente NetApp HCI:

- O NetApp HCI fornece recursos de storage e computação. Você usa o assistente **mecanismo de implantação do NetApp** para implantar o NetApp HCI. Após a implantação bem-sucedida, os nós de computação aparecem como hosts ESXi e você pode gerenciá-los no VMware vSphere Web Client.
- **Os serviços de gerenciamento** ou microsserviços incluem o coletor Active IQ, o QoSSIOC para o plug-in do vCenter e o serviço mNode; eles são atualizados frequentemente como pacotes de serviços. 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 das principais versões. O **nó de gerenciamento** (mNode) é uma máquina virtual que é executada em paralelo com um ou mais clusters de armazenamento 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.

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

- **O controle de nuvem híbrida da NetApp** permite que você gerencie o NetApp HCI. Você pode atualizar os serviços de gerenciamento, expandir seu sistema, coletar Registros e monitorar sua instalação usando o NetApp SolidFire Active IQ. Você faz login no Controle de nuvem híbrida da NetApp navegando até o endereço IP do nó de gerenciamento.
- O **plug-in NetApp Element para vCenter Server** é uma ferramenta baseada na Web integrada à interface de usuário do vSphere (UI). O plug-in é uma extensão e uma interface escalável e fácil de usar para o VMware vSphere que pode gerenciar e monitorar clusters de armazenamento executando o **software NetApp Element**. O plug-in fornece uma alternativa à IU do Element. Você pode usar a interface de usuário do plug-in para descobrir e configurar clusters e gerenciar, monitorar e alocar storage da capacidade do cluster para configurar datastores e datastores virtuais (para volumes virtuais). Um cluster aparece na rede como um único grupo local que é representado para hosts e administradores por endereços IP virtuais. Você também pode monitorar a atividade do cluster com relatórios em tempo real, incluindo mensagens de erro e alerta para qualquer evento que possa ocorrer durante a execução de várias operações.

Saiba mais "Plug-in do NetApp Element para vCenter Server" sobre o .

- Por padrão, o NetApp HCI envia estatísticas de desempenho e alerta para o serviço **NetApp SolidFire Active IQ**. Como parte do seu contrato de suporte normal, o suporte da NetApp monitora esses dados e alerta você sobre quaisquer gargalos de desempenho ou possíveis problemas do sistema. Você precisa criar uma conta de suporte da NetApp se ainda não tiver uma (mesmo que você tenha uma conta SolidFire Active IQ existente) para que você possa aproveitar esse serviço.

  Saiba mais "NetApp SolidFire Active IQ"sobre o .

URLs do NetApp HCI

Aqui estão os URLs comuns que você usa com o NetApp HCI:

URL	Descrição
`https://[IPv4 address of Bond1G interface on a storage node]`	Acesse o assistente do mecanismo de implantação do NetApp para instalar e configurar o NetApp HCI. "Saiba mais."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	Acesse o Controle de nuvem híbrida da NetApp para atualizar, expandir e monitorar a instalação do NetApp HCI e os serviços de gerenciamento de atualizações. "Saiba mais."
`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]:9443`	Registre o pacote vCenter Plug-in no vSphere Web Client.
`https://activeiq.solidfire.com`	Monitore dados e receba alertas sobre gargalos de desempenho ou possíveis problemas de sistema.
`https://<ManagementNodeIP>/mnode`	Atualize manualmente os serviços de gerenciamento usando a IU da API REST do nó de gerenciamento.
`https://[storage cluster MVIP address]`	Acesse a IU do software NetApp Element.

Encontre mais informações

- "Plug-in do NetApp Element para vCenter Server"
- "Página de recursos do NetApp HCI"

Contas de utilizador

Para acessar recursos de armazenamento no sistema, você precisará configurar contas de usuário.

Gerenciamento de conta de usuário

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.

Com o controle de nuvem híbrida da NetApp, você pode criar e gerenciar os seguintes tipos de contas:

- Contas de usuário do administrador para o cluster de armazenamento
- Contas de usuário autoritativas
- Contas de volume, específicas apenas para o cluster de armazenamento no qual foram criadas.

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 criando, excluindo e editando contas de administrador de cluster, alterando a senha do administrador de cluster e configurando configurações LDAP para gerenciar o acesso do sistema para os usuários.

Contas de usuário autoritativas

As contas de usuário 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.

Encontre mais informações

- "Gerenciar contas de usuário"
- "Saiba mais sobre clusters"
- "Plug-in do NetApp Element para vCenter Server"

Proteção de dados

Os termos de proteção de dados da NetApp HCI incluem diferentes tipos de replicação remota, snapshots de volume, clonagem de volumes, domínios de proteção e alta disponibilidade com tecnologia Helix dupla.

A proteção de dados do NetApp HCI 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 SolidFire
- Domínios de proteção

- 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

```
https://www.netapp.com/pdf.html?item=/media/10607-tr4741pdf.pdf["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 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.

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 do SolidFire para um armazenamento de objetos externo ou para outro cluster do SolidFire. 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 SolidFire

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).

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

Dois layouts de domínio de proteção diferentes, chamados de 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.

Você pode usar manualmente "ativar o monitoramento do domínio de proteção" o 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.

Ao criar um novo cluster, se você estiver usando nós de storage que residem em um chassi compartilhado, considere o projeto para proteção contra falhas no nível do chassi usando o recurso de domínios de proteção.

Você pode definir um layout de domínio de proteção personalizado, 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.

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.

Encontre mais informações

"Plug-in do NetApp Element para vCenter Server"

Clusters

Um cluster é um grupo de nós, funcionando como um todo coletivo, que fornecem recursos de storage ou computação. A partir do NetApp HCI 1,8, você pode ter um cluster de storage com dois nós. Um cluster de armazenamento aparece na rede como um único grupo lógico e pode ser acessado como armazenamento de bloco.

A camada de storage no NetApp HCI é fornecida pelo software NetApp Element e a camada de gerenciamento é fornecida pelo plug-in NetApp Element para vCenter Server. Um nó de armazenamento é um servidor que contém uma coleção de unidades que se comunicam entre si através da interface de rede Bond10G. Cada nó de storage 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.

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.

Você pode gerenciar usuários com o controle de nuvem híbrida da NetApp.

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. 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.

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.

Clusters de storage de dois nós

A partir do NetApp HCI 1,8, é possível configurar um cluster de storage com dois nós de storage.

- Você pode usar certos tipos de nós para formar o cluster de storage de dois nós. "Notas de versão do NetApp HCI 1,8"Consulte .

  Em um cluster de dois nós, os nós de storage são limitados a nós com unidades de 480GB TB e 960GB TB, e os nós devem ser do mesmo tipo de modelo.

- Os clusters de storage de dois nós são mais adequados para implantações de pequena escala com workloads que não dependem de grandes requisitos de capacidade e alta performance.
- Além de dois nós de storage, um cluster de storage de dois nós também inclui dois nós de testemunha do NetApp HCI*.

  Saiba mais sobre "Nós de testemunhas."

- É possível escalar um cluster de storage de dois nós para um cluster de storage de três nós. Os clusters de três nós aumentam a resiliência, fornecendo a capacidade de recuperação automática de falhas nos nós de storage.
- Os clusters de storage de dois nós fornecem os mesmos recursos e funcionalidades de segurança dos clusters de storage de quatro nós tradicionais.
- Os clusters de storage de dois nós usam as mesmas redes que os clusters de storage de quatro nós. As redes são configuradas durante a implantação do NetApp HCI usando o assistente do mecanismo de implantação do NetApp.

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. Nós de testemunha em um cluster de dois nós são usados para garantir que haja nós de armazenamento suficientes para formar um quórum de ensemble válido. Para a criação de conjunto, os nós de storage são preferidos em vez de nós de testemunha. Para o conjunto mínimo de três nós envolvendo um cluster de armazenamento de dois nós, dois nós de armazenamento e um nó de testemunha são usados.

Em um conjunto de três nós com dois nós de armazenamento e um nó de testemunha, se um nó de armazenamento ficar offline, o cluster entra em um estado degradado. Dos dois nós de testemunhas, apenas um pode estar ativo no conjunto. O segundo nó testemunha não pode ser adicionado ao conjunto, porque ele executa a função de backup. O cluster permanece em estado degradado até que o nó de armazenamento offline volte a um estado online ou um nó de substituição se junte ao cluster.

Se um nó de testemunha falhar, o nó de testemunha restante junta-se ao conjunto para formar um conjunto de três nós. Você pode implantar um novo nó testemunha para substituir o nó testemunha com falha.

Autorrecuperação e manipulação de falhas em clusters de storage de dois nós

Se um componente de hardware falhar em um nó que faz parte de um cluster tradicional, o cluster poderá rebalancear os dados que estavam no componente que falhou em relação a outros nós disponíveis no cluster. Essa capacidade de recuperação automática não está disponível em um cluster de storage de dois nós, porque é necessário que um mínimo de três nós de storage físico esteja disponível para o cluster para recuperação automática. Quando um nó em um cluster de dois nós falha, o cluster de dois nós não requer a regeneração de uma segunda cópia de dados. Novas gravações são replicadas para dados de bloco no nó de storage ativo restante. Quando o nó com falha é substituído e se junta ao cluster, os dados são rebalanceados entre os dois nós de storage físico.

Clusters de storage com três ou mais nós

A expansão de dois nós de storage para três nós de storage torna o cluster mais resiliente, permitindo a recuperação automática em caso de falhas de nó e de unidade, mas não fornece capacidade adicional. Pode expandir utilizando o "IU do controle de nuvem híbrida da NetApp". Ao expandir de um cluster de dois nós para um cluster de três nós, a capacidade pode ser perdida (Capacidade ociosaconsulte). O assistente da IU mostra avisos sobre a capacidade perdida antes da instalação. Um nó de testemunha único ainda está disponível para manter o quorum do conjunto no caso de uma falha do nó de armazenamento, com um segundo nó de testemunha em espera. Quando você expande um cluster de storage de três nós para um cluster de quatro nós, a capacidade e o desempenho aumentam. Em um cluster de quatro nós, os nós de testemunha não são mais necessários para formar o quorum do cluster. É possível expandir para até 64 nós de computação e 40 nós de storage.

Encontre mais informações

- "Cluster de storage de dois nós NetApp HCI | TR-4823"
- "Plug-in do NetApp Element para vCenter Server"
- "Centro de Documentação de Software SolidFire e Element"

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 HCI e Element definem várias funções de nó para um cluster. Os quatro tipos de funções de nós são **nó de gerenciamento**, **nó de storage**, **nó de computação** e **nós de testemunha NetApp HCI**.

Nó de gerenciamento

O nó de gerenciamento (às vezes abreviado como mNode) 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.

O nó de gerenciamento é uma máquina virtual (VM) que é executada em paralelo com um ou mais clusters de storage baseados em software Element. Além das atualizações, ele é usado para 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. 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 gerenciamento, como o coletor Active IQ, o QoSSIOC para o plug-in do vCenter e o serviço de nós de gerenciamento, são atualizados com frequência como pacotes de serviços.

Nós de storage

Os nós de storage do NetApp HCI são um hardware que fornece os recursos de storage para um sistema NetApp HCI. 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 do NetApp HCI podem ser gerenciados usando o ponto de extensão NetApp Element Management.

Nós de computação

Os nós de computação do NetApp HCI são um hardware que fornece recursos de computação, como CPU, memória e rede, necessários para virtualização na instalação do NetApp HCI. Como cada servidor executa o VMware ESXi, o gerenciamento de nós de computação do NetApp HCI (adicionando ou removendo hosts) deve ser feito fora do plug-in no menu hosts e clusters no vSphere. Independentemente de se tratar de um cluster de storage de quatro nós ou de um cluster de storage de dois nós, o número mínimo de nós de computação permanece dois para uma implantação do NetApp HCI.

Nós de testemunhas

Os nós de testemunhas do NetApp HCI são VMs que são executadas em nós de computação em paralelo com um cluster de storage baseado em software Element. Os nós de testemunha não hospedam serviços de fatia ou bloco. Um nó de testemunha permite a disponibilidade do cluster de storage em caso de falha do nó de storage. Você pode gerenciar e atualizar nós de testemunhas da mesma maneira que outros nós de storage. Um cluster de storage pode ter até quatro nós de testemunha. Seu principal objetivo é garantir que existam nós de cluster suficientes para formar um quórum de ensemble válido.

Requisito: Configure as VMs do nó testemunha para usar o datastore local (padrão definido pelo NDE) para o nó de computação. Você não deve configurá-los em armazenamento compartilhado, como volumes de armazenamento SolidFire. Para impedir que as VMs migrem automaticamente, defina o nível de automação do DRS (Distributed Resource Scheduler) para a VM Witness Node como **Disabled**. Isso impede que ambos os nós de testemunhas sejam executados no mesmo nó de computação e criem uma configuração de par de HA (non-high availability).

Em um cluster de storage de dois nós, um mínimo de dois nós de testemunha são implantados para redundância no caso de uma falha do nó de testemunha. Quando o processo de instalação do NetApp HCI instala nós de testemunha, um modelo de VM é armazenado no VMware vCenter que você pode usar para reimplantar um nó de testemunha caso ele seja removido, perdido ou corrompido acidentalmente. Você também pode usar o modelo para reimplantar um nó de testemunha se precisar substituir um nó de computação com falha que estava hospedando o nó de testemunha. Para obter instruções, consulte a seção **Redeploy Witness Nodes para clusters de storage de dois e três nós** "aqui".

Saiba mais sobre "Requisitos de recursos do Witness Node" e "Requisitos de endereço IP do nó testemunha".

Encontre mais informações

- "Cluster de storage de dois nós NetApp HCI | TR-4823"
- "Plug-in do NetApp Element para vCenter Server"
- "Centro de Documentação de Software SolidFire e Element"

Armazenamento

Modo de manutenção

Se você precisar colocar um nó de storage off-line para manutenção, como atualizações de software ou reparos de host, poderá minimizar o impacto de e/S para o restante do cluster de storage, habilitando o modo de manutenção desse nó. Você pode usar o modo de manutenção com os nós de dispositivo e os nós de SDS empresarial do SolidFire.

Quando um nó de armazenamento é desligado, ele é exibido como **indisponível** na coluna Status do nó na página armazenamento no HCC, pois essa coluna exibe o status do nó da perspetiva do cluster. O status desligado do nó é indicado pelo ícone **Offline** ao lado do nome do host do nó.

Você só poderá fazer a transição de um nó de storage para o modo de manutenção se o nó estiver em bom estado (não tiver falhas de cluster de bloqueio) e se o cluster de storage for tolerante a uma falha de nó único. Depois de ativar o modo de manutenção para um nó saudável e tolerante, o nó não é transferido imediatamente; ele é monitorado até que as seguintes condições sejam verdadeiras:

- Todos os volumes hospedados no nó falharam
- O nó não está mais hospedando como o principal para qualquer volume
- Um nó de espera temporário é atribuído para cada volume que está sendo reprovado

Depois que esses critérios são atendidos, o nó é transferido para o modo de manutenção. Se esses critérios não forem atendidos dentro de um período de 5 minutos, o nó não entrará no modo de manutenção.

Quando você desativa o modo de manutenção para um nó de armazenamento, o nó é monitorado até que as seguintes condições sejam verdadeiras:

- Todos os dados são totalmente replicados para o nó
- Todas as avarias do bloco de bloqueio são resolvidas
- Todas as atribuições temporárias de nó de espera para os volumes hospedados no nó foram inativadas

Depois que esses critérios são atendidos, o nó é transferido para fora do modo de manutenção. Se esses critérios não forem atendidos dentro de uma hora, o nó não fará a transição para fora do modo de manutenção.

Você pode ver os estados das operações do modo de manutenção ao trabalhar com o modo de manutenção usando a API Element:

- **Disabled**: Nenhuma manutenção foi solicitada.
- **FailedToRecoover**: O nó não conseguiu recuperar da manutenção.
- **RecoveringFromMaintenance**: O nó está em processo de recuperação da manutenção.
- **PreparingForMaintenance**: Ações estão sendo tomadas para permitir que um nó tenha a manutenção executada.
- **ReadyForMaintenance**: O nó está pronto para a manutenção ser executada.

Encontre mais informações

- "Ative o modo de manutenção com a API Element"
- "Desative o modo de manutenção com a API Element"
- "Documentação da API do NetApp Element"
- "Plug-in do NetApp Element para vCenter Server"

Volumes

O storage é provisionado no sistema NetApp Element como volumes. Os volumes são dispositivos de bloco acessados pela rede usando clientes iSCSI ou Fibre Channel.

O plug-in do NetApp Element para vCenter Server 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.

Se você estiver implantando um nó de gerenciamento para o NetApp HCI usando o mecanismo de implantação do NetApp, os volumes persistentes serão ativados e configurados automaticamente.

Uma opção para ativar volumes persistentes está incluída nos scripts de instalação e atualização ao implantar um novo nó de gerenciamento. 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 com o NetApp-HCI- previamente anexado ao nome no cluster atribuído. 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

Encontre mais informações

- "Gerenciar volumes"
- "Plug-in do NetApp Element para vCenter Server"
- "Centro de Documentação de Software SolidFire e Element"

Grupos de acesso de volume

Um grupo de acesso de volume é uma coleção de volumes que os usuários podem acessar usando iniciadores iSCSI ou Fibre Channel.

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 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.

Encontre mais informações

- "Gerenciar grupos de acesso de volume"
- "Plug-in do NetApp Element para vCenter Server"
- "Centro de Documentação de Software SolidFire e Element"

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.

Encontre mais informações

- "Gerenciar iniciadores"
- "Grupos de acesso de volume"
- "Gerenciar grupos de acesso de volume"
- "Plug-in do NetApp Element para vCenter Server"
- "Centro de Documentação de Software SolidFire e Element"

Domínios de proteção personalizados

Você pode definir um layout de domínio de proteção personalizado, 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 nenhum domínio de proteção personalizado for atribuído:

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

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.

> O uso de domínios de proteção personalizados pressupõe que nenhum nó compartilha um chassi.

Os seguintes métodos da API Element expõem esses novos domínios de proteção:

- 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.

Entre em Contato com o suporte da NetApp para obter mais detalhes sobre o uso de domínios de proteção personalizados.

Encontre mais informações

"Gerencie o storage com a API Element"

Licenciamento do NetApp HCI

Ao usar o NetApp HCI, você pode precisar de licenças adicionais dependendo do que estiver usando.

Licenciamento do NetApp HCI e VMware vSphere

O licenciamento do VMware vSphere depende da sua configuração:

Opção de rede	Licenciamento
Opção A: Dois cabos para nós de computação que usam a marcação de VLAN (todos os nós de computação)	Requer o uso do vSphere Distributed Switch, que requer o licenciamento do VMware vSphere Enterprise Plus.
Opção B: Seis cabos para nós de computação usando VLANs marcadas (nó de computação de H410C 2RU 4 nós)	Esta configuração usa o vSphere Standard Switch como padrão. O uso opcional do vSphere Distributed Switch requer o licenciamento do VMware Enterprise Plus.
Opção C: Seis cabos para nós de computação que usam VLANs nativas e marcadas (nó de computação de H410C nós, 2RU 4 nós)	Esta configuração usa o vSphere Standard Switch como padrão. O uso opcional do vSphere Distributed Switch requer o licenciamento do VMware Enterprise Plus.

Licenciamento de NetApp HCI e ONTAP Select

Se você recebeu uma versão do ONTAP Select para uso em conjunto com um sistema NetApp HCI adquirido, as seguintes limitações adicionais se aplicam:

- A licença do ONTAP Select, que é fornecida com a venda do sistema NetApp HCI, só pode ser usada em conjunto com os nós de computação do NetApp HCI.
- O storage dessas instâncias do ONTAP Select deve residir apenas nos nós de storage do NetApp HCI.
- É proibido o uso de nós de computação de terceiros ou nós de storage de terceiros.

Encontre mais informações

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

Valores máximos de configuração do Controle de nuvem híbrida da NetApp

O NetApp HCI inclui o controle de nuvem híbrida da NetApp para simplificar o ciclo de vida da computação e o gerenciamento do storage. Ele dá suporte às atualizações do

software Element em nós de storage para clusters de storage do NetApp HCI e do NetApp SolidFire, bem como às atualizações de firmware para nós de computação do NetApp HCI no NetApp HCI. Ele está disponível por padrão nos nós de gerenciamento no NetApp HCI.

Além de comunicar os componentes de hardware e software fornecidos pela NetApp em uma instalação do NetApp HCI, o Controle de nuvem híbrida da NetApp interage com componentes de terceiros no ambiente do cliente, como o VMware vCenter. A NetApp qualifica a funcionalidade do Controle de nuvem híbrida da NetApp e sua interação com esses componentes de terceiros no ambiente do cliente até uma certa escala. Para uma experiência ideal com o controle de nuvem híbrida da NetApp, a NetApp recomenda permanecer dentro da faixa de valores máximos de configuração.

Se você exceder esses máximos testados, poderá ter problemas com o Controle de nuvem híbrida da NetApp, como uma interface de usuário mais lenta e respostas de API ou funcionalidade indisponíveis. Se você se envolver com o NetApp para suporte ao produto com o Controle de nuvem híbrida da NetApp em ambientes configurados além dos máximos de configuração, o suporte da NetApp solicitará que você altere a configuração para estar dentro dos máximos de configuração documentados.

Valores máximos de configuração

O controle de nuvem híbrida da NetApp dá suporte a ambientes VMware vSphere com até 500 nós de computação NetApp. Ele dá suporte a até 20 clusters de storage baseados no software NetApp Element com 40 nós de storage por cluster.

Segurança da NetApp HCI

Quando você usa o NetApp HCI, seus dados são protegidos por protocolos de segurança padrão do setor.

Criptografia em repouso para nós de storage

O NetApp HCI permite criptografar todos os dados armazenados no cluster de storage.

Todas as unidades nos nós de storage capazes de criptografia usam 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 de armazenamento é criada e pedaços da senha são distribuídos para todos os nós no cluster. Nenhum nó único armazena a senha inteira. A senha é então usada para proteger com senha todo o acesso às unidades. Você precisa da senha para desbloquear a unidade e, como a unidade está criptografando todos os dados, seus dados estão seguros em todos os momentos.

Quando você ativa a criptografia em repouso, o desempenho e a eficiência do cluster de storage não são afetados. Além disso, se você remover uma unidade ou nó habilitado para criptografia do cluster de armazenamento com a API Element ou a IU Element, a criptografia em repouso será desativada nas unidades e as unidades serão apagadas com segurança, protegendo os dados que foram armazenados anteriormente nessas unidades. Depois de remover a unidade, você pode apagar com segurança a unidade com o `SecureEraseDrives` método API. Se você remover forçosamente uma unidade ou nó do cluster de armazenamento, os dados permanecerão protegidos pela senha de todo o cluster e pelas chaves de criptografia individuais da unidade.

Para obter informações sobre como ativar e desativar a criptografia em repouso, consulte "Ativar e desativar a encriptação para um cluster" no Centro de Documentação do SolidFire e do Element.

Criptografia de software em repouso

A criptografia de software em repouso permite que todos os dados gravados nos SSDs de um cluster de storage sejam criptografados. Isso fornece uma camada primária de criptografia nos nós SDS empresariais do SolidFire que não incluem unidades com criptografia automática (SEDs).

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, consulte "Introdução ao gerenciamento de chaves externas" no Centro de Documentação do SolidFire e do Element.

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 o MFA, consulte "Habilitando a autenticação multifator" no Centro de Documentação do SolidFire e do Element.

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

Os clusters de storage e os sistemas NetApp HCI da 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 NetApp HCI ou 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, "Criação de 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 .

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

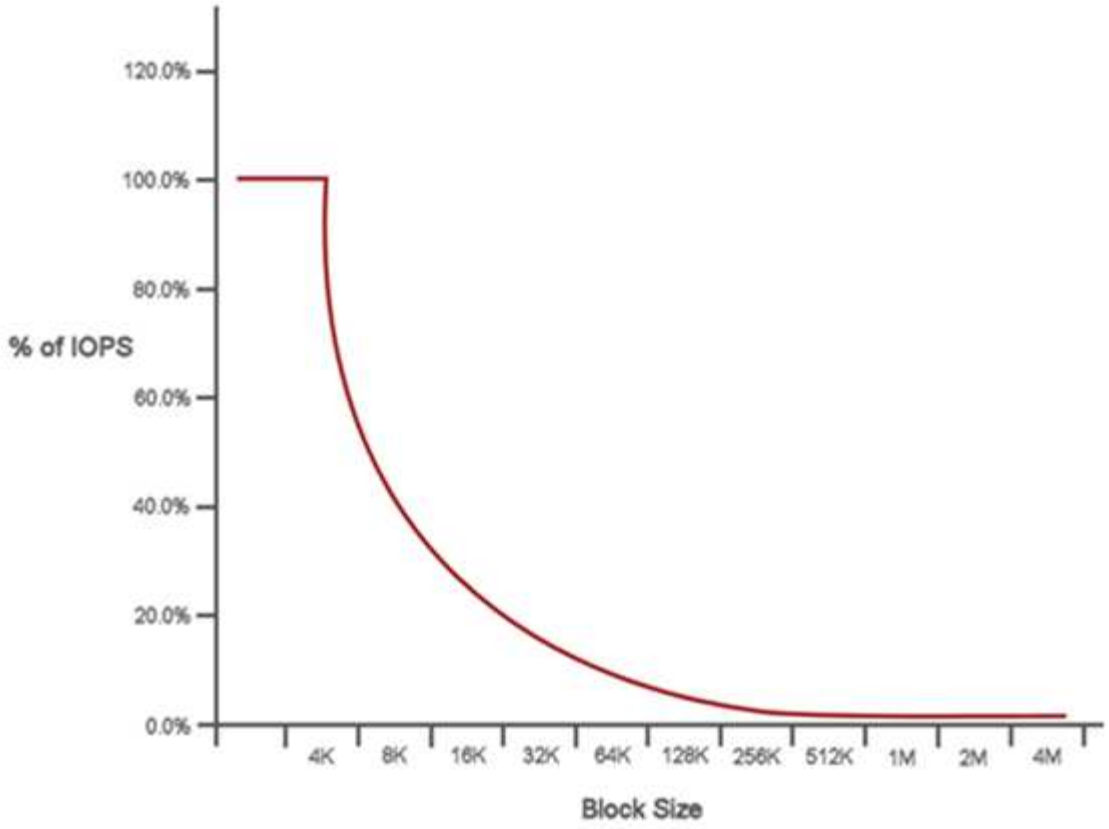
*Estas estimativas são aproximadas. **IOPS máximo e IOPS de explosão podem ser definidos até 200.000K; no entanto, essa configuração só pode ser descompactada efetivamente o desempenho de um volume. O desempenho máximo de um volume no mundo real é limitado pelo uso do cluster e pelo desempenho por nó.

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

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

- "Página de recursos do NetApp HCI"

Informações sobre direitos autorais

Informações sobre marcas comerciais