



Conceitos de ONTAP

ONTAP 9

NetApp
January 17, 2025

Índice

Conceitos de ONTAP	1
Plataformas ONTAP	1
Interfaces de usuário do ONTAP	2
Storage de cluster	3
Pares de alta disponibilidade	4
AutoSupport e consultor digital	5
Arquitetura de rede	6
Protocolos do cliente	9
Discos e agregados	11
Volumes, qtrees, arquivos e LUNs	18
Virtualização de storage	19
Failover de caminho	23
Balanceamento de carga	26
Replicação	29
Eficiência de storage	36
Segurança	47
ONTAP e VMware vSphere	53
Gerenciamento de dados com reconhecimento de aplicações	55
FabricPool	56

Conceitos de ONTAP

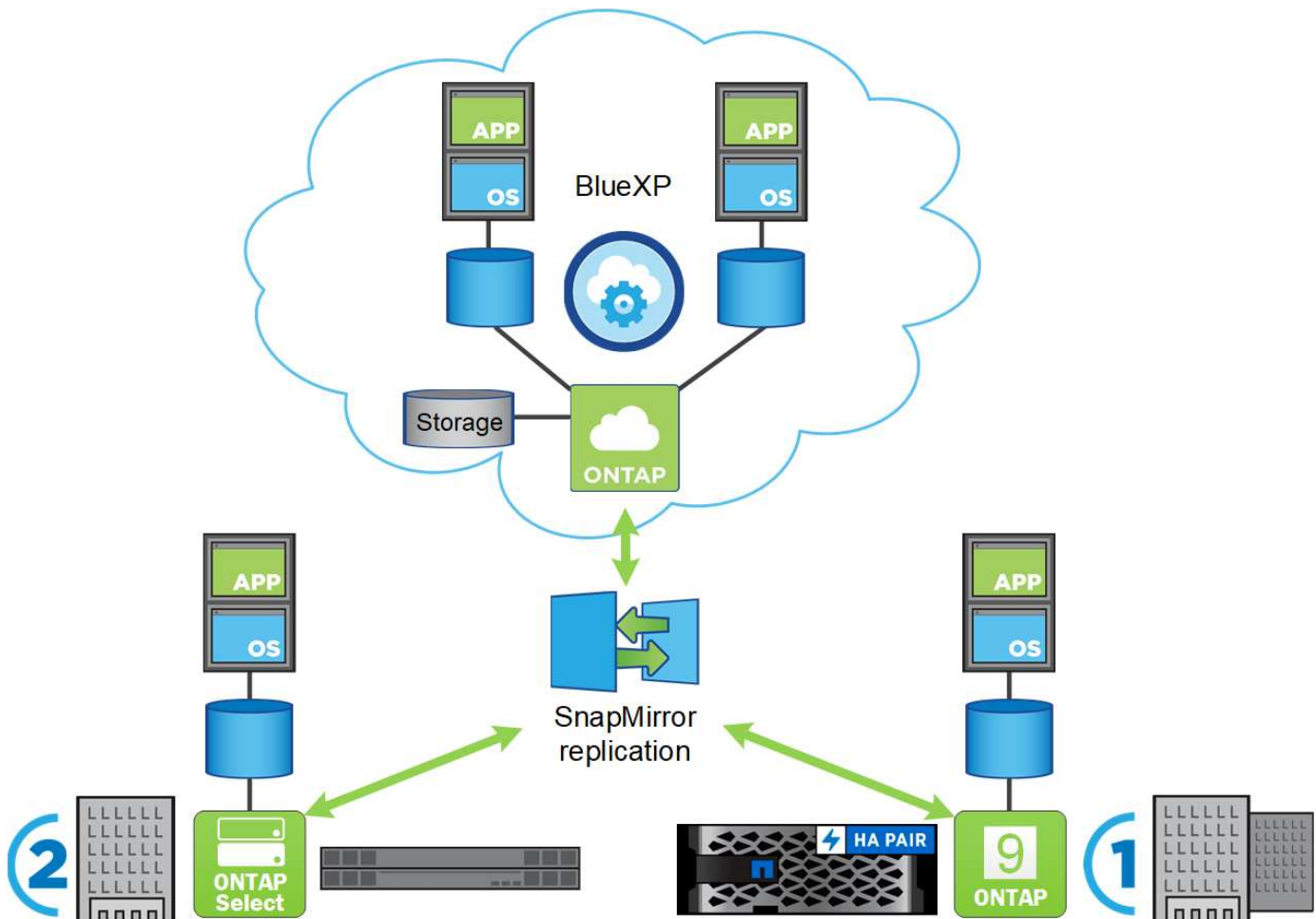
Plataformas ONTAP

O software de gerenciamento de dados ONTAP oferece storage unificado para aplicações que leem e gravam dados em bloco ou arquivo. As opções em configurações de storage variam de flash de alta velocidade a Mídia giratória de baixo preço e storage de objetos baseado na nuvem.

As implementações do ONTAP são executadas no seguinte:

- * Sistemas projetados por NetApp*: "Sistemas flash híbrido da FAS, plataformas All-Flash FAS (AFF) A-Series e C-Series e All-Flash SAN Array (ASA)"
- **Hardware de mercadoria:** "ONTAP Select"
- **Nuvens privadas, públicas ou híbridas:** "Cloud Volumes ONTAP", "Amazon FSX para NetApp ONTAP", "Azure NetApp Files" E "Google Cloud NetApp volumes"
- **Implementações especializadas,** "Data center FlexPod" incluindo , que oferece a melhor infraestrutura convergente da categoria

Juntas, essas implementações formam a estrutura básica do *NetApp Data Fabric*, com uma abordagem comum definida por software para gerenciamento de dados e replicação rápida e eficiente entre plataformas.



Interfaces de usuário do ONTAP

O software de gerenciamento de dados ONTAP oferece várias interfaces que você pode usar para gerenciar clusters do ONTAP. Essas opções de interface oferecem diferentes níveis de acesso e funcionalidade, além de oferecer flexibilidade para gerenciar clusters do ONTAP, conforme apropriado, com base no ambiente.

Use qualquer uma dessas interfaces para administrar clusters do ONTAP e executar operações de gerenciamento de dados

Gerente do sistema da ONTAP

O ONTAP System Manager é uma interface de usuário baseada na Web que oferece uma maneira simplificada e intuitiva de gerenciar seu cluster. É possível administrar operações comuns, como configuração de storage, proteção de dados e configuração e gerenciamento de rede. O System Manager também fornece insights e monitoramento de desempenho de cluster e risco para ajudar você a reagir a problemas do cluster e se antecipar aos problemas antes que eles ocorram. ["Saiba mais"](#).

O ONTAP 9,7 marcou um momento importante para o gerente de sistema do ONTAP. Nessa versão, o NetApp forneceu duas versões do Gerenciador de sistemas ONTAP, introduzindo uma versão redesenhada, mais simplificada e intuitiva, juntamente com a versão que precedeu o ONTAP 9,7. Após o ONTAP 9,7, a versão redesenhada foi redesenhada como Gerente de sistema ONTAP e seu antecessor foi renomeado Gerente de sistema Clássico. O System Manager Classic foi atualizado pela última vez no ONTAP 9,7. Se você estiver usando o System Manager Classic, sua documentação estará ["separadamente"](#) disponível .

BlueXP

A partir do ONTAP 9.12,1, você pode usar a interface BlueXP baseada na Web para gerenciar sua infraestrutura multicloud híbrida a partir de um único painel de controle, mantendo o já conhecido dashboard do System Manager. O BlueXP permite que você crie e administre armazenamento em nuvem (por exemplo, Cloud Volumes ONTAP), use os serviços de dados do NetApp (por exemplo, backup em nuvem) e controle muitos dispositivos de armazenamento no local e na borda. A adição de sistemas ONTAP locais ao BlueXP permite que você gerencie todos os ativos de storage e dados em uma única interface. ["Saiba mais"](#).

Interface de linha de comando ONTAP

O ["Interface de linha de comando ONTAP \(CLI\)"](#) é uma interface baseada em texto que permite interagir com um cluster, nó, SVM e muito mais usando ["comandos"](#)o . Os comandos CLI estão disponíveis com base ["tipo de função"](#)no . Você pode acessar a CLI do ONTAP por meio de SSH ou uma conexão de console a um nó no cluster.

API REST do ONTAP

A partir do ONTAP 9.6, você pode acessar uma API RESTful que permite gerenciar e automatizar programaticamente as operações de cluster. Use a API para executar várias tarefas administrativas do ONTAP, como criar e gerenciar volumes, snapshots e agregados, além de monitorar a performance do cluster. Você pode acessar a API REST do ONTAP diretamente usando um utilitário como curl ou com qualquer linguagem de programação compatível com um CLIENTE REST, como Python, PowerShell e Java. ["Saiba mais"](#).



ONTAPI é uma API ONTAP proprietária que precede a API REST do ONTAP. A interface ONTAPI será desativada em versões futuras do ONTAP. Se você estiver usando o ONTAPI, você deve Planejar o ["Migração para a API REST do ONTAP"](#).

Kits de ferramentas e frameworks NetApp

O NetApp fornece kits de ferramentas de cliente para linguagens e ambientes de desenvolvimento específicos que abstraem a API REST do ONTAP e facilitam a criação de código de automação. ["Saiba mais"](#).

Além desses kits de ferramentas, você pode criar e implantar código de automação usando frameworks. ["Saiba mais"](#).

Storage de cluster

A iteração atual do ONTAP foi originalmente desenvolvida para a arquitetura de armazenamento *cluster* de escalabilidade horizontal do NetApp. Essa é a arquitetura que você normalmente encontra nas implementações de data center do ONTAP. Como essa implementação exerce a maioria das capacidades do ONTAP, é um bom lugar para começar a entender os conceitos que informam a tecnologia ONTAP.

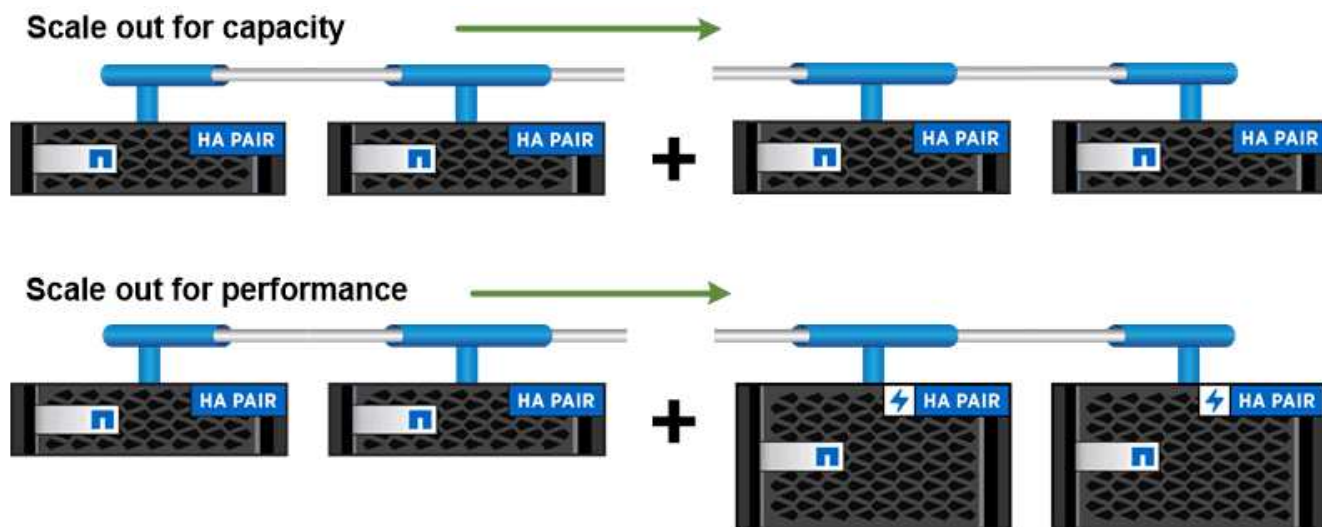
As arquiteturas de data center geralmente implantam controladores FAS ou AFF dedicados que executam o software de gerenciamento de dados ONTAP. Cada controlador, seu armazenamento, sua conectividade de rede e a instância do ONTAP em execução no controlador é chamada de *node*.

Os nós são emparelhados para alta disponibilidade (HA). Juntos, esses pares (até 12 nós para SAN, até 24 nós para nas) compõem o cluster. Os nós se comunicam uns com os outros através de uma interconexão de cluster dedicada e privada.

Dependendo do modelo da controladora, o storage de nós consiste em discos flash, unidades de capacidade ou ambos. As portas de rede no controlador fornecem acesso aos dados. Os recursos físicos de storage e conectividade de rede são virtualizados, visíveis apenas para administradores de cluster, não para clientes nas ou hosts SAN.

Os nós de um par de HA devem usar o mesmo modelo de storage array. Caso contrário, você pode usar qualquer combinação suportada de controladores. É possível fazer escalabilidade horizontal para capacidade adicionando nós com modelos de storage array semelhantes ou para obter performance adicionando nós com storage arrays mais avançados.

É claro que você também pode fazer escalabilidade vertical de todas as maneiras tradicionais, atualizando discos ou controladoras conforme necessário. A infraestrutura de storage virtualizada do ONTAP facilita a movimentação de dados sem interrupções, o que significa que você pode escalar verticalmente ou horizontalmente, sem tempo de inatividade.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

Pares de alta disponibilidade

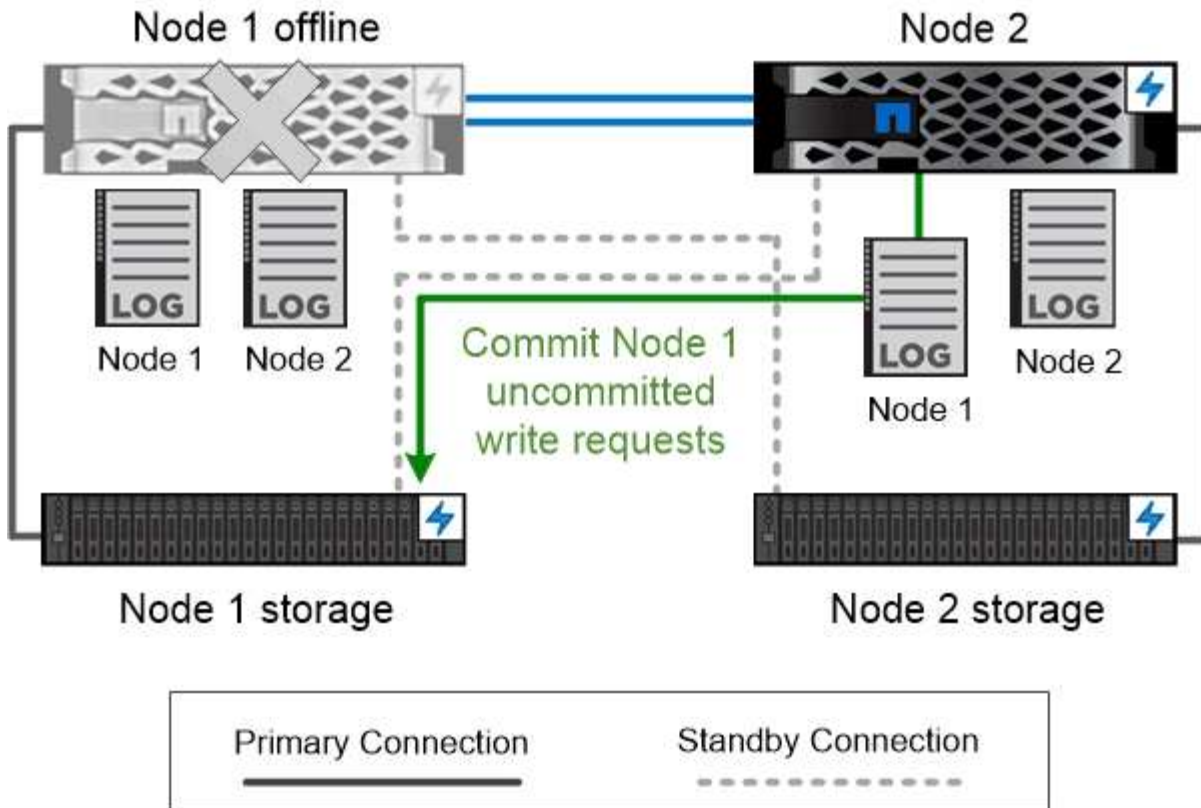
Os nós de cluster são configurados em *high-availability (HA) pairs* para tolerância de falhas e operações ininterruptas. Se um nó falhar ou se você precisar reduzir um nó para manutenção de rotina, seu parceiro pode *assumir o armazenamento e continuar a fornecer dados a partir dele*. O parceiro *devolve* armazenamento quando o nó é colocado de volta na linha.

Os pares HA consistem sempre em modelos de controlador semelhantes. Normalmente, as controladoras residem no mesmo chassi com fontes de alimentação redundantes.

Os pares de HA são nós tolerantes a falhas que podem se comunicar entre si de maneiras diferentes para permitir que cada nó verifique continuamente se seu parceiro está funcionando e espelhar dados de log para a memória não volátil do outro. Quando uma solicitação de gravação é feita em um nó, ela é registrada no NVRAM em ambos os nós antes que uma resposta seja enviada de volta para o cliente ou host. No failover, o parceiro sobrevivente compromete as solicitações de gravação não confirmadas do nó com falha no disco, garantindo a consistência dos dados.

As conexões com a Mídia de armazenamento do outro controlador permitem que cada nó acesse o armazenamento do outro no caso de uma aquisição. Os mecanismos de failover de caminho de rede garantem que os clientes e hosts continuem a se comunicar com o nó sobrevivente.

Para garantir disponibilidade, você deve manter a utilização da capacidade de performance em qualquer nó em 50% para acomodar o workload adicional no caso de failover. Pelo mesmo motivo, você pode querer configurar não mais de 50% do número máximo de interfaces de rede virtual nas para um nó.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

Takeover e giveback em implementações virtualizadas de ONTAP

O storage não é compartilhado entre nós em implementações virtualizadas do ONTAP "sem nada", como o Cloud Volumes ONTAP para AWS ou ONTAP Select. Quando um nó cai, seu parceiro continua fornecendo dados de uma cópia espelhada síncrona dos dados do nó. Ele não assume o storage do nó, apenas sua função de fornecimento de dados.

AutoSupport e consultor digital

O ONTAP oferece monitoramento e geração de relatórios de sistemas orientados por inteligência artificial por meio de um portal da Web e por meio de um aplicativo móvel. O componente AutoSupport do ONTAP envia telemetria que é analisada pelo consultor digital da Active IQ (também conhecido como consultor digital).

O Digital Advisor permite otimizar sua infraestrutura de dados em toda a nuvem híbrida global, fornecendo análises preditivas práticas e suporte proativo por meio de um portal baseado na nuvem e aplicativo móvel. Insights e recomendações orientados por dados do consultor digital estão disponíveis para todos os clientes da NetApp com um contrato de SupportEdge ativo (os recursos variam de acordo com o produto e a camada de suporte).

Aqui estão algumas coisas que você pode fazer com o Digital Advisor:

- Planejar atualizações. O consultor digital identifica problemas no seu ambiente que podem ser resolvidos ao atualizar para uma versão mais recente do ONTAP e o componente do consultor de atualização ajuda você a Planejar uma atualização bem-sucedida.
- Veja o bem-estar do sistema. Seu painel do Digital Advisor relata quaisquer problemas de bem-estar e ajuda você a corrigir esses problemas. Monitore a capacidade do sistema para garantir que você nunca fique sem espaço de armazenamento.
- Gerenciar a performance. O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no System Manager. Identifique problemas de configuração e sistema que estejam afetando a performance.
- Maximizar a eficiência: Visualize as métricas de eficiência de storage e identifique maneiras de armazenar mais dados em menos espaço.
- Ver inventário e configuração. O Digital Advisor exibe o inventário completo e as informações de configuração de software e hardware. Veja quando os contratos de serviço estão expirando para garantir que você permaneça coberto.

Informações relacionadas

["Documentação do NetApp: Consultor digital"](#)

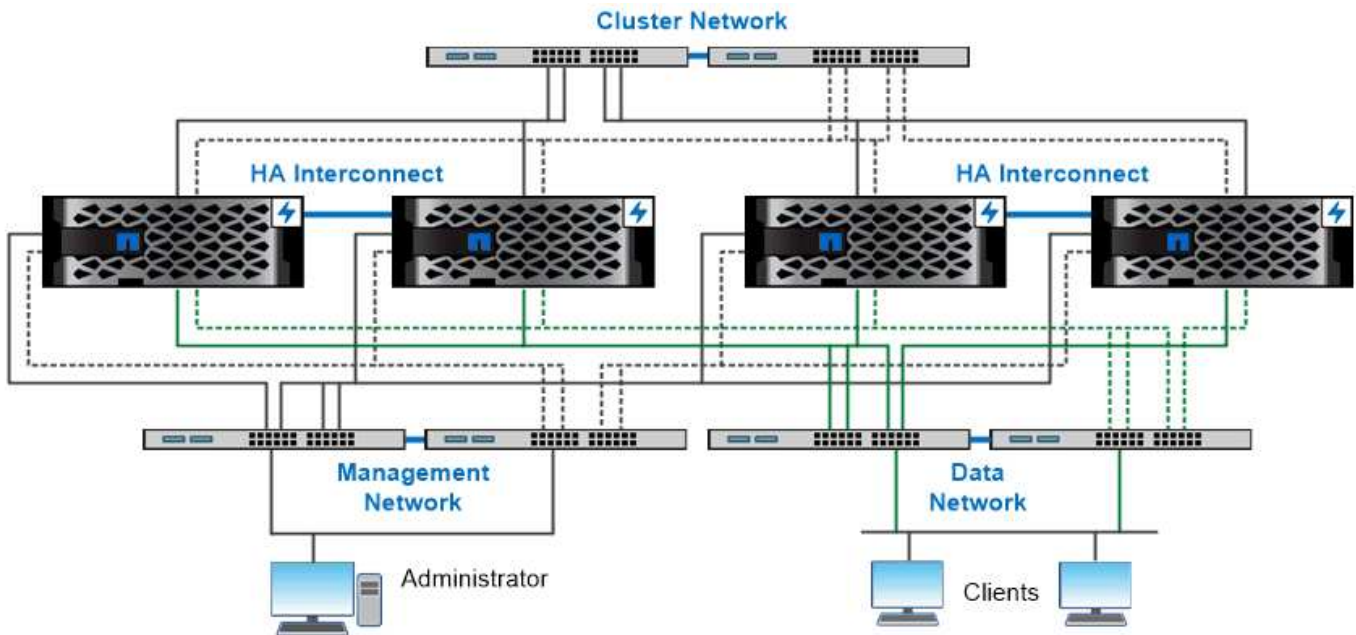
["Inicie o Digital Advisor"](#)

["Serviços da SupportEdge"](#)

Arquitetura de rede

Visão geral da arquitetura de rede

A arquitetura de rede para uma implementação de data center ONTAP normalmente consiste em uma interconexão de cluster, uma rede de gerenciamento para administração de cluster e uma rede de dados. Os NICs (placas de interface de rede) fornecem portas físicas para conexões Ethernet. HBAs (adaptadores de barramento de host) fornecem portas físicas para conexões FC.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

Portas lógicas

Além das portas físicas fornecidas em cada nó, você pode usar *portas lógicas* para gerenciar o tráfego de rede. As portas lógicas são grupos de interface ou VLANs.

Grupos de interfaces

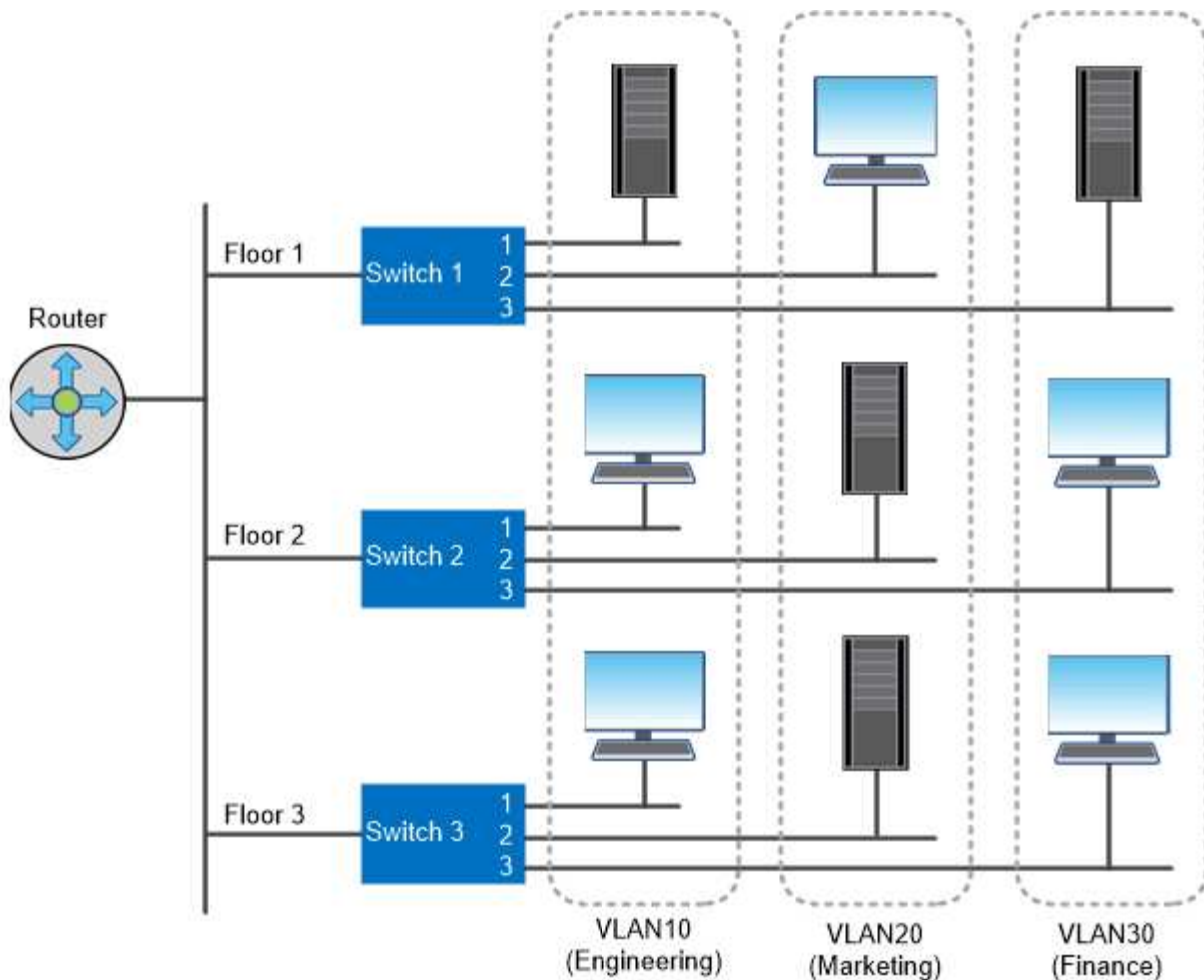
Grupos de interface combinam várias portas físicas em uma única "porta de tronco" lógica. Você pode querer criar um grupo de interfaces que consiste em portas de NICs em diferentes slots PCI para garantir que uma falha de slot reduza o tráfego essencial para os negócios.

Um grupo de interfaces pode ser multimodo, monomodo ou dinâmico. Cada modo oferece diferentes níveis de tolerância a falhas. Você pode usar qualquer um dos tipos de grupo de interface multimodo para equilibrar o tráfego de rede.

VLANs

VLANs separam o tráfego de uma porta de rede (que pode ser um grupo de interfaces) em segmentos lógicos definidos em uma base de porta de switch, em vez de em limites físicos. As *end-stations* pertencentes a uma VLAN estão relacionadas por função ou aplicação.

Você pode agrupar estações finais por departamento, como Engenharia e Marketing, ou por projeto, como release1 e release2. Como a proximidade física das estações finais é irrelevante em uma VLAN, as estações finais podem ser geograficamente remotas.



You can use VLANs to segregate traffic by department.

Suporte para tecnologias de rede padrão do setor

O ONTAP é compatível com todas as principais tecnologias de rede padrão do setor. As principais tecnologias incluem IPspaces, balanceamento de carga DNS e traps SNMP.

Domínios de broadcast, grupos de failover e sub-redes são descritos em [Failover de caminho nas](#).

IPspaces

Você pode usar um *IPspace* para criar um espaço de endereço IP distinto para cada servidor de dados virtual em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Um provedor de serviços, por exemplo, poderia configurar diferentes IPspaces para locatários usando os mesmos endereços IP para acessar um cluster.

Balanceamento de carga DNS

Você pode usar *DNS load balancing* para distribuir o tráfego de rede do usuário entre as portas disponíveis. Um servidor DNS seleciona dinamicamente uma interface de rede para o tráfego com base no número de clientes montados na interface.

Traps SNMP

Você pode usar *SNMP traps* para verificar periodicamente se há limites operacionais ou falhas. Os traps SNMP capturam informações de monitoramento do sistema enviadas assincronamente de um agente SNMP para um gerenciador SNMP.

Conformidade com FIPS

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode ativar e desativar o modo SSL FIPS, definir protocolos SSL globalmente e desativar quaisquer cifras fracas, como RC4.

Visão geral da RDMA

As ofertas de acesso remoto à memória direta (RDMA) da ONTAP são compatíveis com cargas de trabalho sensíveis à latência e de alta largura de banda. O RDMA permite que os dados sejam copiados diretamente entre a memória do sistema de armazenamento e a memória do sistema host, contornando as interrupções da CPU e a sobrecarga.

NFS sobre RDMA

A partir do ONTAP 9.10,1, você pode configurar "[NFS sobre RDMA](#)" para habilitar o uso do armazenamento GPUDirect do NVIDIA para cargas de trabalho aceleradas por GPU em hosts com GPUs NVIDIA compatíveis.

Interconexão de cluster RDMA

A interconexão de cluster RDMA reduz a latência, diminui os tempos de failover e acelera a comunicação entre nós em um cluster.

A partir do ONTAP 9.10,1, o RDMA de interconexão de cluster é suportado para determinados sistemas de hardware quando usado com placas de rede de cluster X1151A. A partir do ONTAP 9.13,1, as placas de rede X91153A também suportam RDMA de interconexão de cluster. Consulte a tabela para saber quais sistemas são suportados em diferentes versões do ONTAP.

Sistemas	Versões de ONTAP compatíveis
<ul style="list-style-type: none">AFF A400ASA A400	ONTAP 9.10,1 e posterior
<ul style="list-style-type: none">AFF A900ASA A900FAS9500	ONTAP 9.13,1 e posterior

Dada a configuração apropriada do sistema de armazenamento, nenhuma configuração adicional é necessária para usar a interconexão RDMA.

Protocolos do cliente

O ONTAP dá suporte a todos os principais protocolos de cliente padrão do setor: NFS, SMB, FC, FCoE, iSCSI, NVMe e S3.

NFS

NFS é o protocolo de acesso a arquivos tradicional para sistemas UNIX e LINUX. Os clientes podem acessar arquivos em volumes ONTAP usando os seguintes protocolos.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- PNFS

Você pode controlar o acesso a arquivos usando permissões de estilo UNIX, permissões de estilo NTFS ou uma combinação de ambos.

Os clientes podem acessar os mesmos arquivos usando os protocolos NFS e SMB.

SMB

SMB é o protocolo tradicional de acesso a arquivos para sistemas Windows. Os clientes podem acessar arquivos em volumes ONTAP usando os protocolos SMB 2,0, SMB 2,1, SMB 3,0 e SMB 3.1.1. Assim como no NFS, uma combinação de estilos de permissão é compatível.

O SMB 1,0 está disponível, mas desativado por padrão no ONTAP 9.3 e versões posteriores.

FC

Fibre Channel é o protocolo original de bloco em rede. Em vez de arquivos, um protocolo de bloco apresenta um disco virtual inteiro a um cliente. O protocolo FC tradicional usa uma rede FC dedicada com switches FC especializados e exige que o computador cliente tenha interfaces de rede FC.

Um LUN representa o disco virtual e um ou mais LUNs são armazenados em um volume ONTAP. O mesmo LUN pode ser acessado através dos protocolos FC, FCoE e iSCSI, mas vários clientes só podem acessar o mesmo LUN se fizerem parte de um cluster que evite colisões de gravação.

FCoE

O FCoE é basicamente o mesmo protocolo que o FC, mas usa uma rede Ethernet de nível de data center em vez do transporte FC tradicional. O cliente ainda requer uma interface de rede específica para FCoE.

iSCSI

iSCSI é um protocolo de bloco que pode ser executado em redes Ethernet padrão. A maioria dos sistemas operacionais cliente oferece um iniciador de software que é executado em uma porta Ethernet padrão. O iSCSI é uma boa escolha quando você precisa de um protocolo de bloco para um aplicativo específico, mas não tem rede FC dedicada disponível.

NVMe/FC e NVMe/TCP

O NVMe, o protocolo de bloco mais recente, foi projetado especificamente para funcionar com storage baseado em flash. Ele oferece sessões dimensionáveis, uma redução significativa na latência e um aumento no paralelismo, o que o torna adequado para aplicações de baixa latência e alta taxa de transferência, como bancos de dados e análises in-memory.

Diferentemente do FC e iSCSI, o NVMe não usa LUNs. Em vez disso, ele usa namespaces, que são armazenados em um volume ONTAP. Os namespaces NVMe podem ser acessados somente pelo protocolo NVMe.

S3

A partir do ONTAP 9.8, é possível habilitar um servidor do Serviço de armazenamento simples (S3) do ONTAP em um cluster do ONTAP, permitindo que você forneça dados no armazenamento de objetos usando buckets do S3.

O ONTAP dá suporte a dois cenários de caso de uso no local para fornecer storage de objetos S3:

- Disposição do FabricPool em um bucket no cluster local (disposição em um bucket local) ou cluster remoto (camada de nuvem).
- S3 acesso de aplicativo cliente a um bucket no cluster local ou em um cluster remoto.



O ONTAP S3 é apropriado se você quiser recursos de S3 em clusters existentes sem hardware e gerenciamento adicionais. Para implantações maiores de 300TB TB, o software NetApp StorageGRID continua a ser a principal solução da NetApp para storage de objetos. Saiba mais "[StorageGRID](#)" sobre .

Discos e agregados

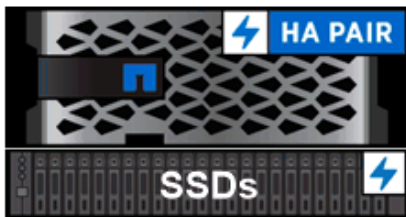
Visão geral de discos e camadas locais (agregados)

Você pode gerenciar o storage físico do ONTAP usando o Gerenciador do sistema e a CLI. Você pode criar, expandir e gerenciar camadas locais (agregados), trabalhar com camadas locais (agregados) do Flash Pool, gerenciar discos e gerenciar políticas de RAID.

Quais são os níveis locais (agregados)

Níveis locais (também chamados de *agregados*) são contentores para os discos gerenciados por um nó. Use as camadas locais para isolar workloads com demandas de desempenho diferentes, categorizar dados com padrões de acesso diferentes ou separar dados para fins regulatórios.

- Para aplicações essenciais aos negócios que precisam da menor latência possível e da maior performance possível, você pode criar um nível local que consiste inteiramente de SSDs.
- Para categorizar dados com diferentes padrões de acesso, você pode criar um *nível local híbrido*, implantando flash como cache de alto desempenho para um conjunto de dados em funcionamento, ao mesmo tempo em que usa HDDs de baixo custo ou storage de objetos para dados acessados com menos frequência.
 - Um *Flash Pool* consiste em SSDs e HDDs.
 - Um *FabricPool* consiste em um nível local totalmente SSD com um armazenamento de objetos anexado.
- Se você precisar separar os dados arquivados de dados ativos para fins regulatórios, poderá usar um nível local que consiste em HDDs de capacidade ou uma combinação de HDDs de desempenho e capacidade.



Datacenter



Cloud

You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.

Trabalhando com camadas locais (agregados)

Você pode executar as seguintes tarefas:

- ["Gerenciar camadas locais \(agregados\)"](#)
- ["Gerenciar discos"](#)
- ["Gerenciar configurações RAID"](#)
- ["Gerenciar camadas do Flash Pool"](#)

Você executa essas tarefas se as seguintes tarefas forem verdadeiras:

- Você não quer usar uma ferramenta de script automatizado.
- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você tem uma configuração do MetroCluster e segue os procedimentos descritos ["MetroCluster"](#) na documentação para configuração inicial e diretrizes para camadas locais (agregados) e gerenciamento de disco.

Informações relacionadas

- ["Gerenciar categorias de nuvem do FabricPool"](#)

Camadas locais (agregados) e grupos RAID

As tecnologias RAID modernas protegem contra falhas de disco reconstruindo os dados de um disco com falha em um disco sobressalente. O sistema compara as informações de índice em um "disco de paridade" com os dados nos restantes discos íntegros para reconstruir os dados em falta, tudo sem tempo de inatividade ou um custo significativo de desempenho.

Um nível local (agregado) consiste em um ou mais *grupos RAID*. O *tipo RAID* do nível local determina o

número de discos de paridade no grupo RAID e o número de falhas de disco simultâneas que a configuração RAID protege contra.

O tipo RAID padrão, RAID-DP (paridade RAID-dupla), requer dois discos de paridade por grupo RAID e protege contra a perda de dados no caso de dois discos falharem ao mesmo tempo. Para RAID-DP, o tamanho do grupo RAID recomendado está entre 12 e 20 HDDs e entre 20 e 28 SSDs.

Você pode espalhar o custo total dos discos de paridade criando grupos RAID na extremidade mais alta da recomendação de dimensionamento. Esse é especialmente o caso dos SSDs, que são muito mais confiáveis do que as unidades de capacidade. Para camadas locais que usam HDDs, você deve equilibrar a necessidade de maximizar o storage em disco em comparação a fatores de compensação, como o tempo de reconstrução mais longo necessário para grupos RAID maiores.

Camadas locais espelhadas e sem espelhamento (agregados)

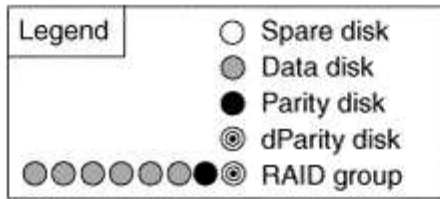
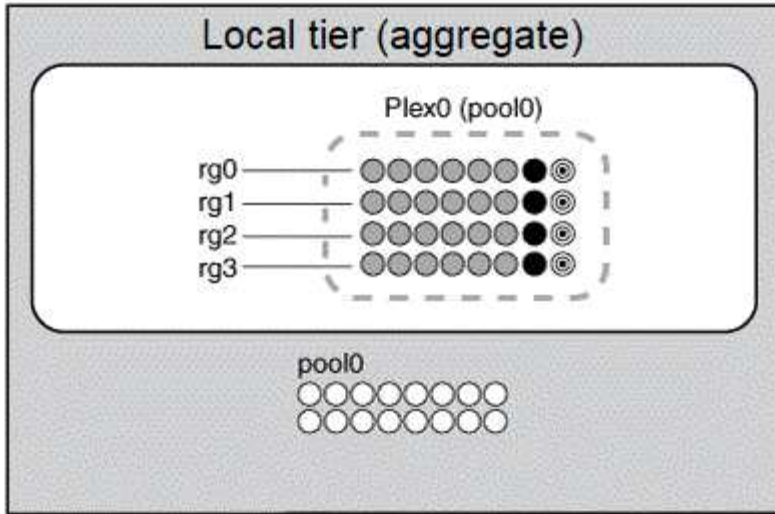
O ONTAP tem um recurso opcional chamado *SyncMirror* que você pode usar para espelhar sincronamente dados de nível local (agregado) em cópias, ou *plexes*, armazenados em diferentes grupos RAID. Os plexes garantem contra a perda de dados se mais discos falharem do que o tipo RAID protege contra, ou se houver perda de conectividade com discos do grupo RAID.

Quando você cria um nível local com o System Manager ou usando a CLI, você pode especificar que o nível local é espelhado ou sem espelhamento.

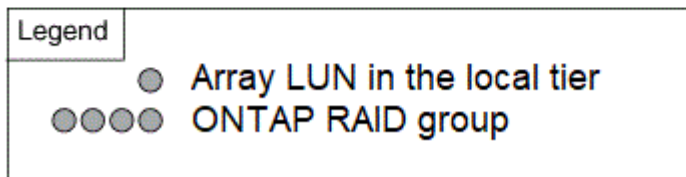
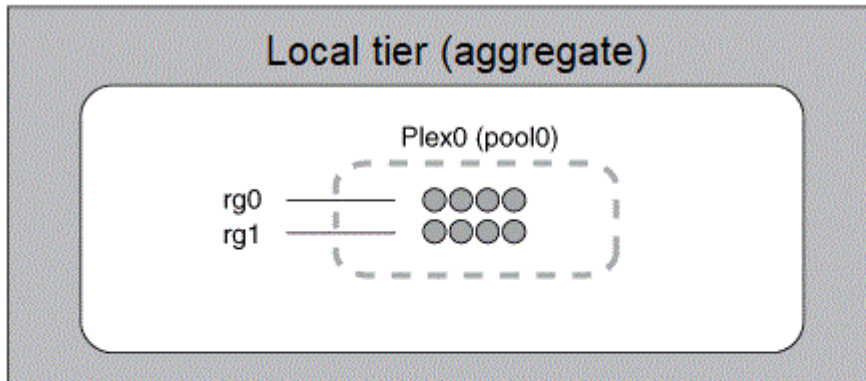
Como os agregados (camadas locais sem espelhamento) funcionam

Se você não especificar que as camadas locais são espelhadas, elas serão criadas como camadas locais sem espelhamento (agregados). Os níveis locais não espelhados têm apenas um *Plex* (uma cópia de seus dados), que contém todos os grupos RAID pertencentes a esse nível local.

O diagrama a seguir mostra um nível local sem espelhamento composto de discos, com seu único Plex. O nível local tem quatro grupos RAID: rg0, RG1, RG2 e rg3. Cada grupo RAID tem seis discos de dados, um disco de paridade e um disco de paridade (paridade dupla). Todos os discos usados pelo nível local vêm do mesmo pool, "pool0".



O diagrama a seguir mostra um nível local sem espelhamento com LUNs de array, com um Plex. Ele tem dois grupos RAID, rg0 e RG1. Todos os LUNs de array usados pelo nível local vêm do mesmo pool, "pool0".



Como funcionam os agregados (camadas locais espelhadas)

Agregados espelhados têm dois *plexes* (cópias de seus dados), que usam a funcionalidade SyncMirror para duplicar os dados para fornecer redundância.

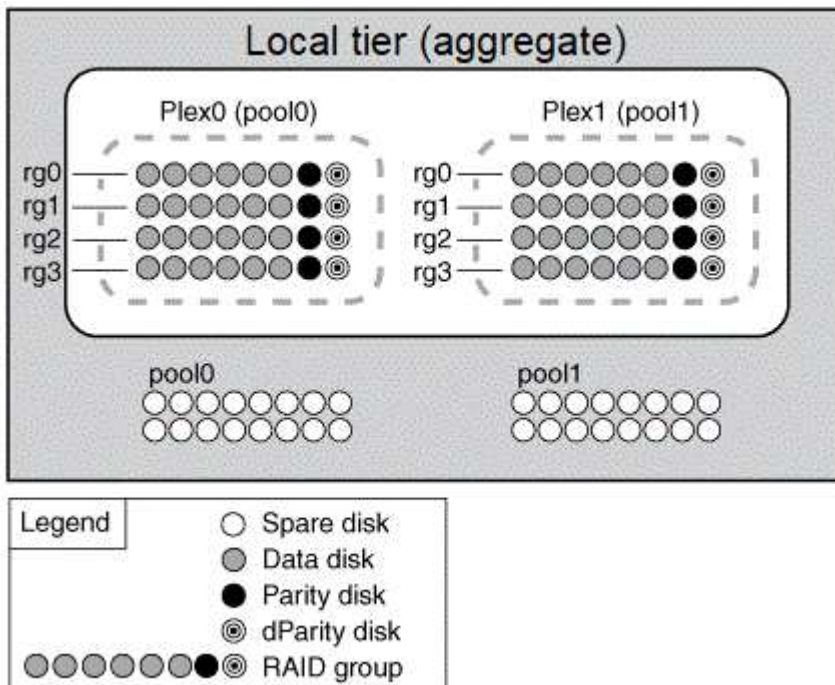
Ao criar um nível local, você pode especificar que ele é um nível local espelhado. Além disso, você pode adicionar um segundo Plex a um nível local sem espelhamento existente para torná-lo um nível espelhado. Utilizando a funcionalidade SyncMirror, o ONTAP copia os dados no Plex original (plex0) para o novo Plex (plex1). Os plexos são separados fisicamente (cada Plex tem seus próprios grupos RAID e seu próprio pool),

e os plexos são atualizados simultaneamente.

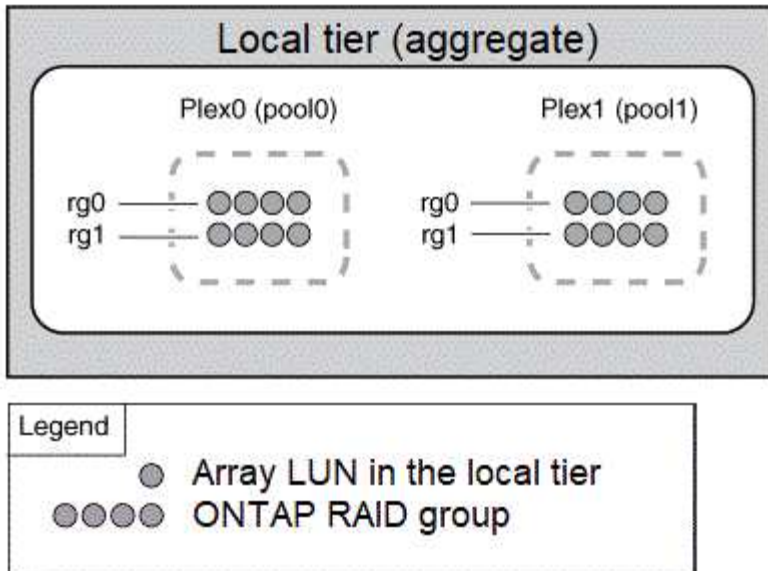
Essa configuração oferece proteção adicional contra a perda de dados se mais discos falharem do que o nível RAID do agregado protege contra ou se houver perda de conectividade, porque o Plex não afetado continua fornecendo dados enquanto você corrige a causa da falha. Depois que o Plex que teve um problema é corrigido, os dois plexos ressinchronizam e restabelecem a relação do espelho.

Os discos e LUNs de array no sistema são divididos em dois pools: "pool0" e "pool1". Plex0 obtém seu armazenamento de pool0GB e plex1GB recebe seu armazenamento de pool1GB.

O diagrama a seguir mostra um nível local composto por discos com a funcionalidade SyncMirror ativada e implementada. Um segundo Plex foi criado para o nível local, "plex1". Os dados em plex1 são uma cópia dos dados em plex0 e os grupos RAID também são idênticos. Os 32 discos sobressalentes são alocados para pool0 ou pool1 usando 16 discos para cada pool.



O diagrama a seguir mostra um nível local composto por LUNs de array com a funcionalidade SyncMirror ativada e implementada. Um segundo Plex foi criado para o nível local, "plex1". Plex1 é uma cópia do plex0 e os grupos RAID também são idênticos.



É recomendável manter pelo menos 20% de espaço livre para agregados espelhados para performance e disponibilidade ideais de storage. Embora a recomendação seja de 10% para agregados não espelhados, os 10% adicionais de espaço podem ser usados pelo sistema de arquivos para absorver alterações incrementais. Mudanças incrementais aumentam a utilização de espaço para agregados espelhados devido à arquitetura baseada em Snapshot copy-on-write da ONTAP. O não cumprimento destas práticas recomendadas pode ter um impacto negativo no desempenho.

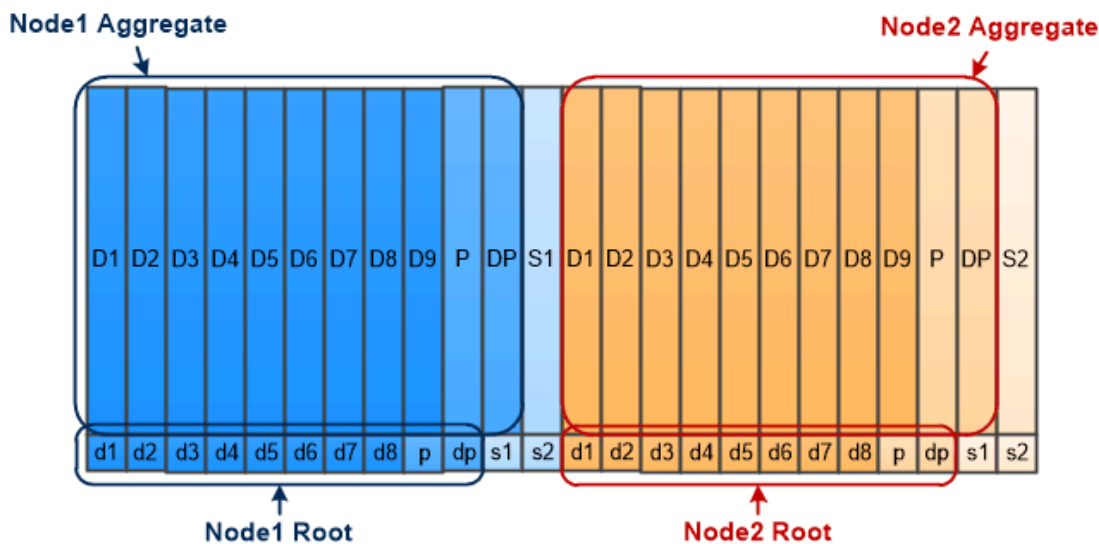
Particionamento de dados raiz

Cada nó deve ter um agregado de raiz para arquivos de configuração do sistema de storage. O agregado raiz tem o tipo RAID do agregado de dados.

O System Manager não suporta o particionamento root-data ou root-data-data-data.

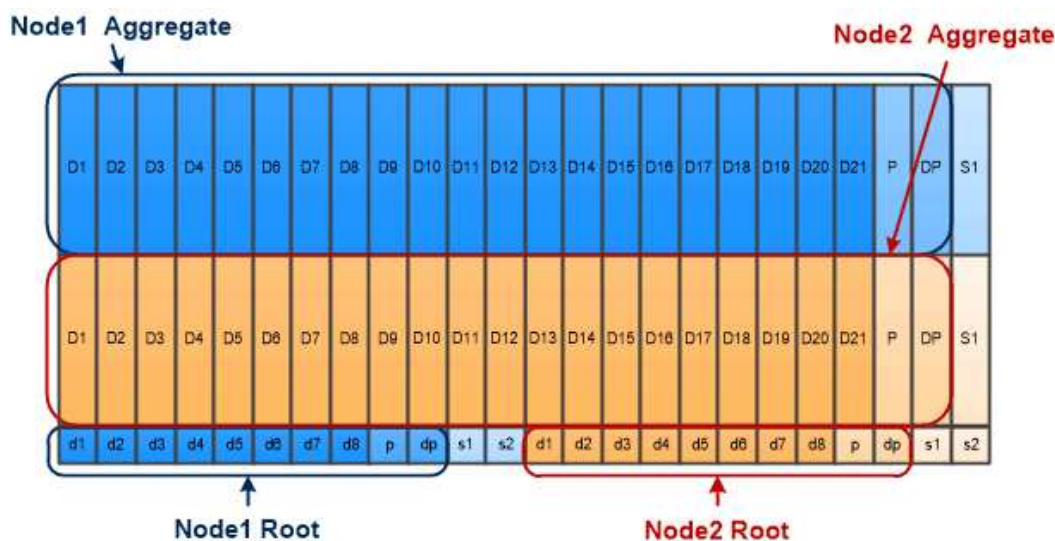
Um agregado de raiz do tipo RAID-DP normalmente consiste em um disco de dados e dois discos de paridade. Isso é um "imposto de paridade" significativo para pagar pelos arquivos do sistema de armazenamento, quando o sistema já está reservando dois discos como discos de paridade para cada grupo RAID no agregado.

Root-data partitioning reduz o imposto de paridade ao dividir o agregado de raiz entre partições de disco, reservando uma pequena partição em cada disco como partição raiz e uma grande partição para dados.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

Como a ilustração sugere, quanto mais discos forem usados para armazenar o agregado raiz, menor a partição raiz. Esse também é o caso de uma forma de particionamento de dados-raiz chamada *root-data-data partitioning*, que cria uma pequena partição como a partição raiz e duas partições maiores, igualmente dimensionadas para dados.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Ambos os tipos de particionamento de dados raiz fazem parte do recurso ONTAP *Advanced Drive Partitioning (ADP)*. Ambos são configurados de fábrica: Particionamento de dados raiz para sistemas FAS2xxx, FAS9000, FAS8200, FAS80xx e AFF de nível básico, particionamento de dados-raiz apenas para sistemas AFF.

Saiba mais "[Advanced Drive Partitioning](#)" sobre o .

Unidades particionadas e usadas para o agregado raiz

As unidades particionadas para uso no agregado raiz dependem da configuração do sistema.

Saber quantas unidades são usadas para o agregado raiz ajuda você a determinar quanto da capacidade das unidades é reservada para a partição raiz e quanto está disponível para uso em um agregado de dados.

A funcionalidade de particionamento de dados raiz é compatível com plataformas de nível básico, todas as plataformas Flash FAS e plataformas FAS com apenas SSDs anexados.

Para plataformas de nível básico, apenas as unidades internas são particionadas.

Para todas as plataformas Flash FAS e plataformas FAS com apenas SSDs conectados, todas as unidades conectadas ao controlador quando o sistema é inicializado são particionadas, até um limite de 24 TB por nó. As unidades adicionadas após a configuração do sistema não são particionadas.

Volumes, qtrees, arquivos e LUNs

O ONTAP serve dados para clientes e hosts de contentores lógicos chamados *FlexVol volumes*. porque esses volumes são apenas vagamente acoplados ao agregado que contém, eles oferecem maior flexibilidade no gerenciamento de dados do que os volumes tradicionais.

É possível atribuir vários volumes do FlexVol a um agregado, cada um dedicado a um aplicativo ou serviço diferente. Você pode expandir e contratar um FlexVol volume, mover um FlexVol volume e fazer cópias eficientes de um FlexVol volume. Você pode usar *qtrees* para particionar um FlexVol volume em unidades mais gerenciáveis e *cotas* para limitar o uso de recursos de volume.

Os volumes contêm sistemas de arquivos em um ambiente nas e LUNs em um ambiente SAN. Um LUN (número de unidade lógica) é um identificador para um dispositivo chamado *unidade lógica* endereçado por um protocolo SAN.

LUNs são a unidade básica de armazenamento em uma configuração SAN. O host do Windows vê LUNs no seu sistema de armazenamento como discos virtuais. Migre LUNs para volumes diferentes sem interrupções, conforme necessário.

Além dos volumes de dados, há alguns volumes especiais que você precisa saber sobre:

- Um volume de raiz *node* (normalmente "vol0") contém informações e logs de configuração do nó.
- Um volume raiz *SVM* serve como ponto de entrada para o namespace fornecido pelo SVM e contém informações de diretório de namespace.
- *Volumes do sistema* contêm metadados especiais, como logs de auditoria de serviço.

Você não pode usar esses volumes para armazenar dados.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

FlexGroup volumes

Em algumas empresas, um único namespace pode exigir petabytes de storage, excedendo até mesmo a capacidade de 100TB TB do FlexVol volume.

Um volume *FlexGroup* suporta até 400 bilhões de arquivos com 200 volumes de membros constituintes que trabalham de forma colaborativa para equilibrar dinamicamente a alocação de carga e espaço uniformemente entre todos os membros.

Não há sobrecarga necessária de manutenção ou gerenciamento com um volume FlexGroup. Basta criar o volume FlexGroup e compartilhá-lo com seus clientes nas. ONTAP faz o resto.

Virtualização de storage

Visão geral da virtualização de storage

Você usa *máquinas virtuais de armazenamento (SVMs)* para fornecer dados a clientes e hosts. Como uma máquina virtual em execução em um hipervisor, uma SVM é uma entidade lógica que abstrai recursos físicos. Os dados acessados pelo SVM não ficam vinculados a um local no storage. O acesso à rede ao SVM não está vinculado a uma porta física.



Os SVMs eram anteriormente chamados de "vserver". A interface de linha de comando ONTAP ainda usa o termo "vserver".

Um SVM serve dados para clientes e hosts de um ou mais volumes, por meio de uma ou mais interfaces lógicas de rede (LIFs). Os volumes podem ser atribuídos a qualquer agregado de dados no cluster. LIFs podem ser hospedados por qualquer porta física ou lógica. Os volumes e LIFs podem ser movidos sem interromper o serviço de dados, não importando se você está realizando atualizações de hardware,

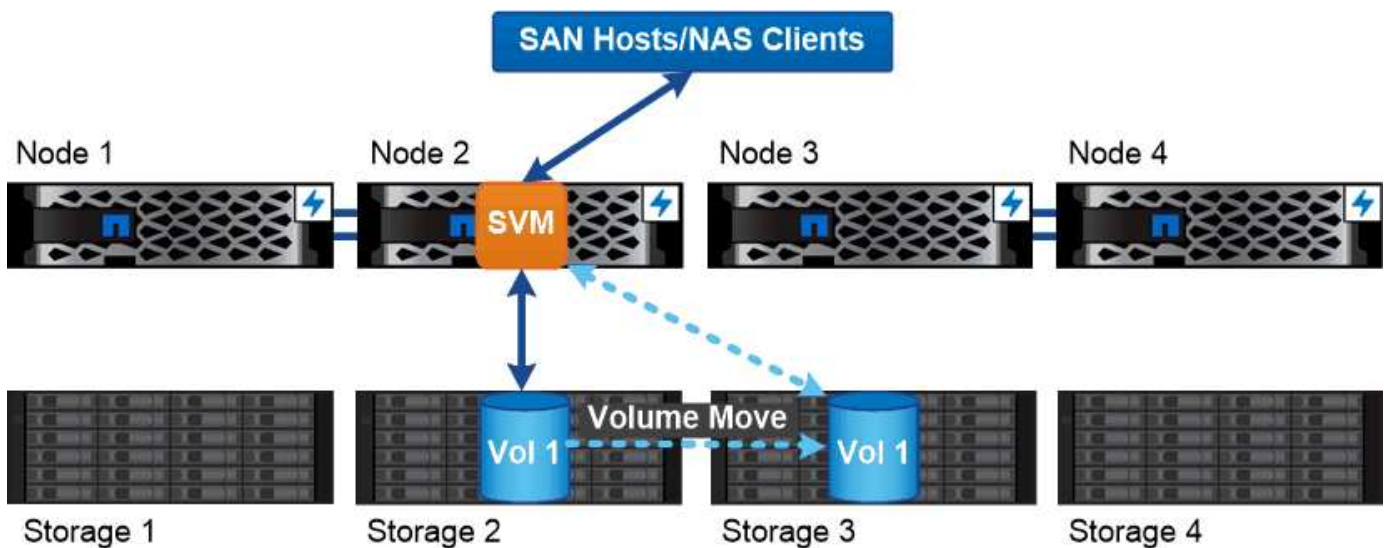
adicionando nós, equilibrando a performance ou otimizando a capacidade entre agregados.

O mesmo SVM pode ter um LIF para tráfego nas e um LIF para tráfego SAN. Os clientes e hosts precisam apenas do endereço do LIF (endereço IP para NFS, SMB ou iSCSI; WWPN para FC) para acessar o SVM. Os LIFs mantêm seus endereços à medida que se movem. As portas podem hospedar várias LIFs. Cada SVM tem sua própria segurança, administração e namespace.

Além de SVMs de dados, o ONTAP implanta SVMs especiais para administração:

- Um *admin SVM* é criado quando o cluster é configurado.
- Um *nó SVM* é criado quando um nó se junta a um cluster novo ou existente.
- Um *sistema SVM* é criado automaticamente para comunicações em nível de cluster em um IPspace.

Você não pode usar esses SVMs para fornecer dados. Há também LIFs especiais para tráfego dentro e entre clusters e para gerenciamento de clusters e nós.



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

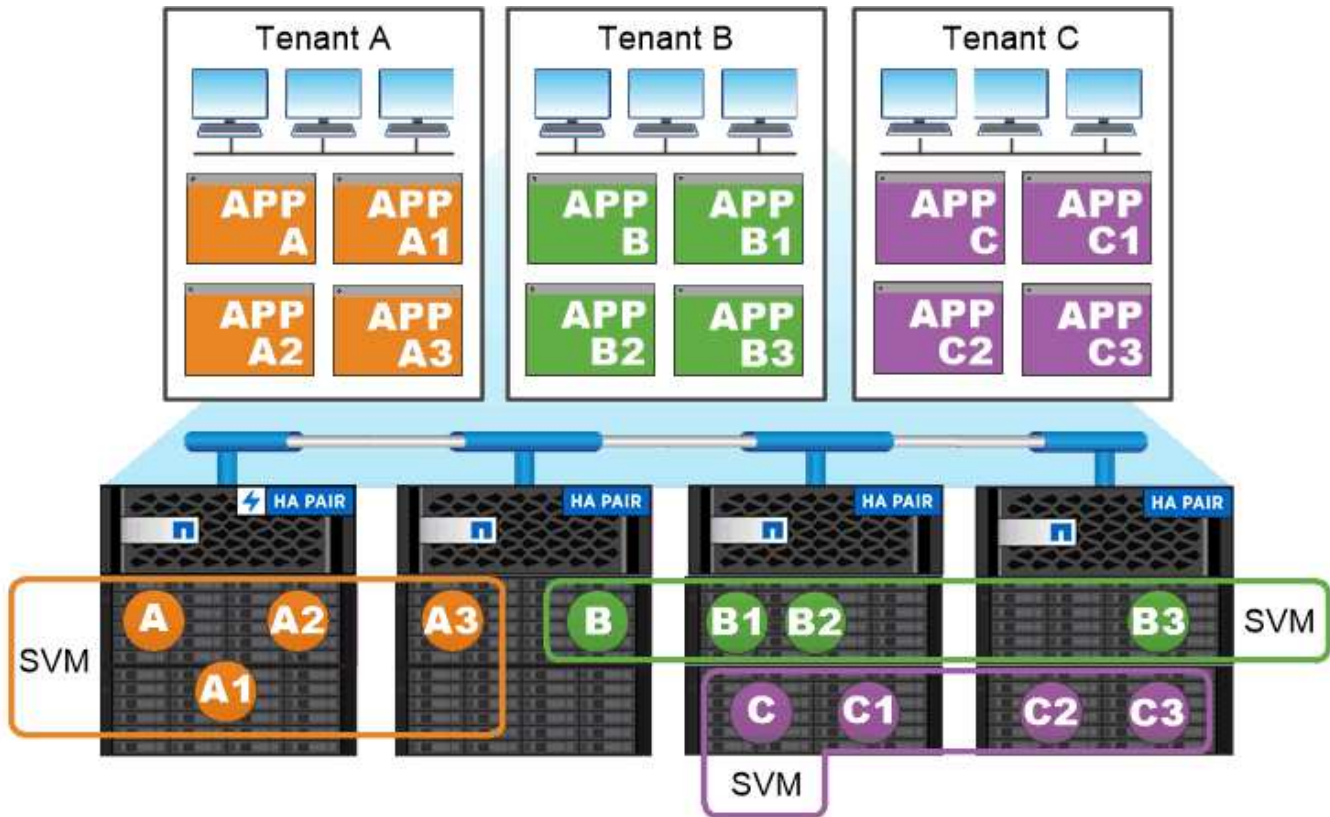
Por que ONTAP é como middleware

Os objetos lógicos que o ONTAP usa para tarefas de gerenciamento de armazenamento atendem aos objetivos familiares de um pacote de middleware bem projetado: Proteger o administrador de detalhes de implementação de baixo nível e isolar a configuração de alterações nas características físicas, como nós e portas. A ideia básica é que o administrador deve ser capaz de mover volumes e LIFs facilmente, reconfigurando alguns campos em vez de toda a infraestrutura de armazenamento.

Casos de uso da SVM

Os fornecedores de serviços usam SVMs em acordos seguros de alocação a vários clientes para isolar os dados de cada locatário, fornecer a cada locatário sua própria autenticação e administração e simplificar o chargeback. Você pode atribuir vários LIFs ao mesmo SVM para atender a diferentes necessidades do cliente. Além disso, você pode usar a QoS para proteger contra cargas de trabalho de locatários "bullying" as cargas de trabalho de outros locatários.

Os administradores usam SVMs para fins semelhantes na empresa. Talvez você queira segregar dados de diferentes departamentos ou manter os volumes de storage acessados por hosts em um SVM e volumes de compartilhamento de usuários em outro. Alguns administradores colocam LUNs iSCSI/FC e armazenamentos de dados NFS em um SVM e compartilhamentos SMB em outro.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

Administração de clusters e SVM

Um *administrador de cluster* acessa o administrador SVM para o cluster. O administrador SVM e um administrador de cluster com o nome reservado `admin` são criados automaticamente quando o cluster é configurado.

Um administrador de cluster com a função padrão `admin` pode administrar todo o cluster e seus recursos. O administrador do cluster pode criar administradores de cluster adicionais com funções diferentes, conforme necessário.

Um *administrador do SVM* acessa um data SVM. O administrador do cluster cria SVMs de dados e administradores de SVM conforme necessário.

Por padrão, os administradores do SVM recebem `vsadmin` a função. O administrador do cluster pode atribuir funções diferentes aos administradores do SVM, conforme necessário.

Controle de Acesso baseado em função (RBAC)

A *função* atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Namespaces e pontos de junção

Um *namespace* é um agrupamento lógico de volumes Unidos em *pontos de junção* para criar uma única hierarquia de sistema de arquivos. Um cliente com permissões suficientes pode acessar arquivos no namespace sem especificar a localização dos arquivos no armazenamento. Os volumes Junctioned podem residir em qualquer lugar do cluster.

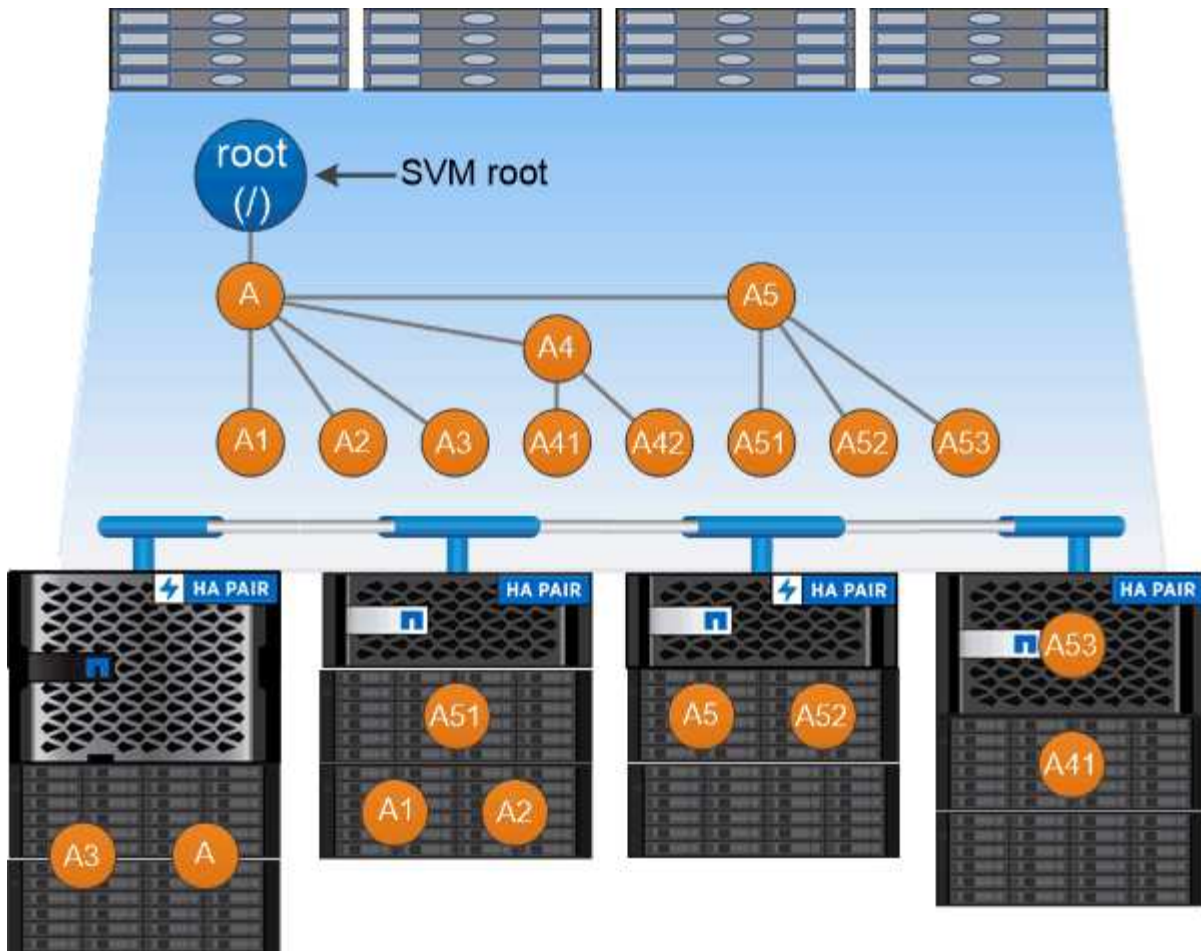
Em vez de montar cada volume contendo um arquivo de interesse, os clientes nas montam um NFS *export* ou acessam um SMB *share*. a exportação ou compartilhamento representa todo o namespace ou um local intermediário dentro do namespace. O cliente acessa apenas os volumes montados abaixo do seu ponto de acesso.

Você pode adicionar volumes ao namespace conforme necessário. Você pode criar pontos de junção diretamente abaixo de uma junção de volume pai ou em um diretório dentro de um volume. Um caminho para uma junção de volume para um volume chamado "vol3" pode ser `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou mesmo `/dir1/dir2/vol3`. O caminho é chamado de *caminho de junção*.

Cada SVM tem um namespace único. O volume raiz da SVM é o ponto de entrada para a hierarquia de namespace.



Para garantir que os dados permaneçam disponíveis no caso de uma interrupção do nó ou failover, você deve criar uma cópia de *load-sharing mirror* para o volume raiz da SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção /eng/home :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Failover de caminho

Visão geral do failover de caminho

Há diferenças importantes em como o ONTAP gerencia o failover de caminho em topologias nas e SAN. Um LIF nas migra automaticamente para uma porta de rede diferente após uma falha de link. Um SAN LIF não migra (a menos que você o mova manualmente após a falha). Em vez disso, a tecnologia multipathing no host desvia o tráfego para um LIF diferente - no mesmo SVM, mas acessando uma porta de rede

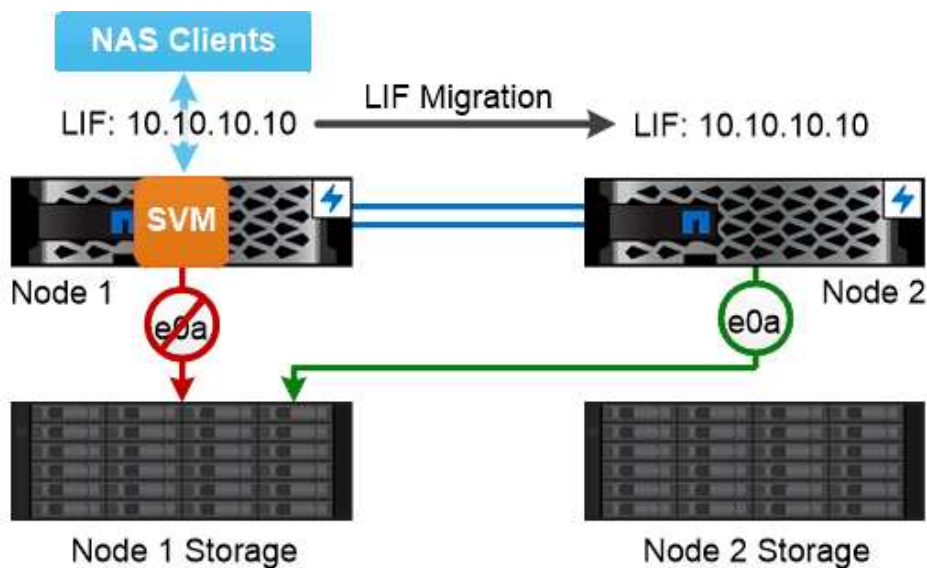
diferente.

Failover de caminho nas

Um LIF nas migra automaticamente para uma porta de rede sobrevivente após uma falha de link em sua porta atual. A porta para a qual o LIF migra deve ser um membro do grupo *failover* para o LIF. A política de grupo *failover* restringe os destinos de failover para um LIF de dados para portas no nó que possui os dados e seu parceiro de HA.

Para conveniência administrativa, o ONTAP cria um grupo de failover para cada domínio *broadcast* na arquitetura de rede. Os domínios de broadcast agrupam portas que pertencem à mesma rede de camada 2. Se você estiver usando VLANs, por exemplo, para segregar o tráfego por departamento (Engenharia, Marketing, Finanças e assim por diante), cada VLAN define um domínio de broadcast separado. O grupo de failover associado ao domínio de broadcast é atualizado automaticamente sempre que você adicionar ou remover uma porta de domínio de broadcast.

É quase sempre uma boa ideia usar um domínio de broadcast para definir um grupo de failover para garantir que o grupo de failover permaneça atual. Ocasionalmente, no entanto, você pode querer definir um grupo de failover que não esteja associado a um domínio de broadcast. Por exemplo, você pode querer que LIFs failover apenas para portas em um subconjunto das portas definidas no domínio de broadcast.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

sub-redes

Uma *sub-rede* reserva um bloco de endereços IP em um domínio de broadcast. Esses endereços pertencem à mesma rede de camada 3 e são alocados às portas no domínio de broadcast quando você cria um LIF. Geralmente é mais fácil e menos propenso a erros especificar um nome de sub-rede quando você define um endereço LIF do que especificar um endereço IP e uma máscara de rede.

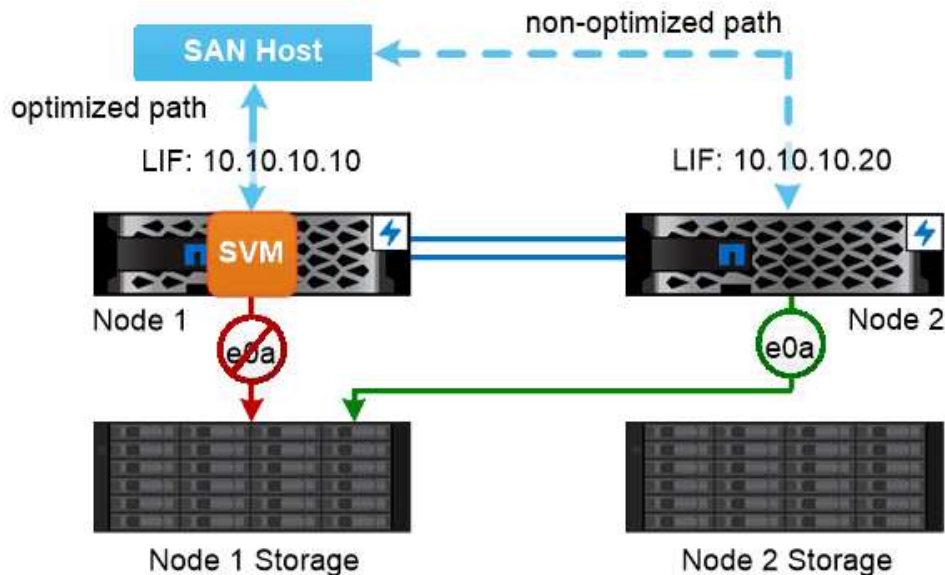
Failover de caminho SAN

Um host SAN usa ALUA (Asymmetric Logical Unit Access) e MPIO (multipath I/o) para redirecionar o tráfego para um LIF sobrevivente após uma falha de link. Caminhos predefinidos determinam as possíveis rotas para o LUN servido pelo SVM.

Em um ambiente SAN, os hosts são considerados como *iniciadores* de solicitações para LUN *destinos*. O MPIO habilita vários caminhos de iniciadores para destinos. ALUA identifica os caminhos mais diretos, chamados *caminhos otimizados*.

Normalmente, você configura vários caminhos otimizados para LIFs no nó proprietário do LUN e vários caminhos não otimizados para LIFs em seu parceiro de HA. Se uma porta falhar no nó proprietário, o host roteia o tráfego para as portas sobreviventes. Se todas as portas falharem, o host roteia o tráfego pelos caminhos não otimizados.

Por padrão, o ONTAP Selective LUN Map (SLM) limita o número de caminhos do host para um LUN. Um LUN recém-criado só pode ser acessado por meio de caminhos para o nó que possui o LUN ou seu parceiro de HA. Você também pode limitar o acesso a um LUN configurando LIFs em um *conjunto de portas* para o iniciador.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

movendo volumes em ambientes SAN

Por padrão, o ONTAP *Selective LUN Map (SLM)* limita o número de caminhos para um LUN de um host SAN. Um LUN recém-criado só pode ser acessado por meio de caminhos para o nó que possui o LUN ou seu parceiro de HA, os *nodos de relatórios* para o LUN.

Isso significa que, quando você move um volume para um nó em outro par de HA, você precisa adicionar nós de geração de relatórios para o par de HA de destino ao mapeamento de LUN. Em seguida, você pode especificar os novos caminhos na configuração do MPIO. Depois que a movimentação de volume estiver concluída, você poderá excluir os nós de relatório do par de HA de origem do mapeamento.

Balanceamento de carga

O desempenho de workloads começa a ser afetado pela latência quando a quantidade de trabalho em um nó excede os recursos disponíveis. Você pode gerenciar um nó sobrecarregado aumentando os recursos disponíveis (atualizando discos ou CPU) ou reduzindo a carga (movendo volumes ou LUNs para nós diferentes, conforme necessário).

Você também pode usar a qualidade do serviço (QoS) do ONTAP para garantir que a performance de workloads essenciais não seja degradada pelos workloads da concorrência:

- Você pode definir uma taxa de transferência de QoS *ceiling* em um workload da concorrência para limitar seu impacto nos recursos do sistema (QoS Max).
- Você pode definir uma taxa de transferência de QoS *floor* para um workload crítico, garantindo que ele atenda aos destinos mínimos de taxa de transferência, independentemente da demanda por workloads da concorrência (QoS min).
- Você pode definir um limite e um espaço de QoS para o mesmo workload.

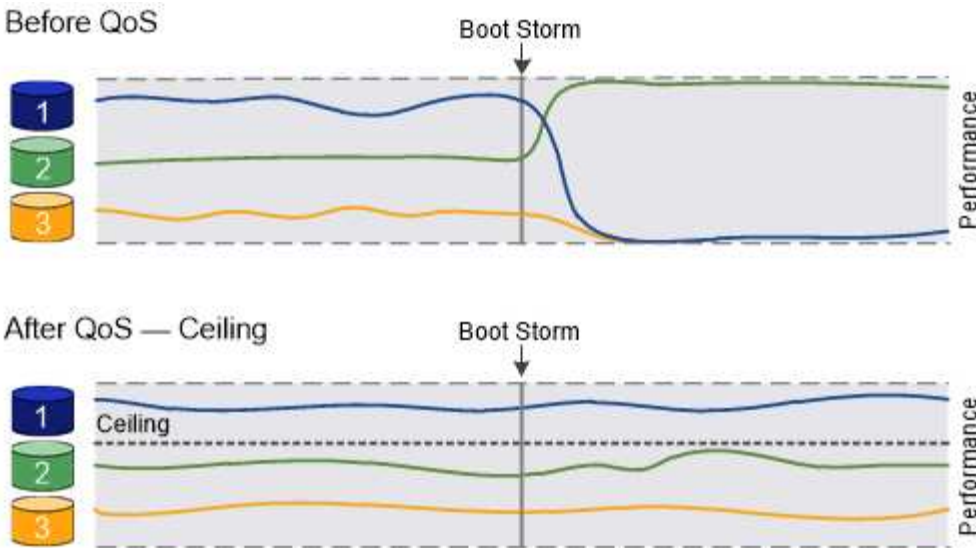
Limites máximos de taxa de transferência

Um limite máximo de taxa de transferência limita a taxa de transferência de uma carga de trabalho a um número máximo de IOPS ou MB/s. Na figura abaixo, o limite máximo de produtividade para a carga de trabalho 2 garante que não seja "bully" cargas de trabalho 1 e 3.

Um *grupo de políticas* define o limite máximo de taxa de transferência para uma ou mais cargas de trabalho. Um workload representa as operações de e/S de um *objeto de storage*: um volume, arquivo ou LUN ou todos os volumes, arquivos ou LUNs em uma SVM. Você pode especificar o limite máximo ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.



A taxa de transferência para cargas de trabalho pode exceder o limite máximo especificado em até 10%, especialmente se uma carga de trabalho sofrer mudanças rápidas na taxa de transferência. O teto pode ser excedido em até 50% para lidar com explosões.



The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

Andares com taxa de transferência

Um piso de taxa de transferência garante que a taxa de transferência para um workload não fique abaixo de um número mínimo de IOPS. Na figura abaixo, os andares de taxa de transferência para o workload 1 e o workload 3 garantem que eles atendam aos destinos mínimos de taxa de transferência, independentemente da demanda por workload 2.

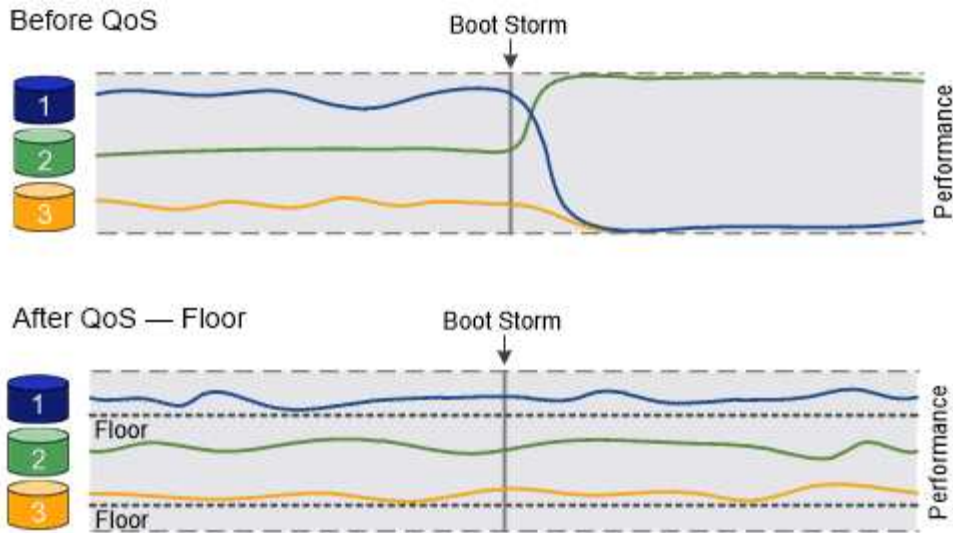


Como os exemplos sugerem, um teto de throughput limita a taxa de transferência diretamente. Um piso de taxa de transferência mantém a taxa de transferência indiretamente, dando prioridade às cargas de trabalho para as quais o piso foi definido.

Uma carga de trabalho representa as operações de e/S de um volume, LUN ou, a partir de ONTAP 9.3, arquivo. Um grupo de políticas que define um piso de taxa de transferência não pode ser aplicado a um SVM. Você pode especificar o piso ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.



A taxa de transferência para uma carga de trabalho pode ficar abaixo do nível especificado se houver capacidade de desempenho (espaço livre) insuficiente no nó ou no agregado, ou durante operações críticas como `volume move trigger-cutover`. Mesmo quando a capacidade suficiente está disponível e as operações críticas não estão ocorrendo, a taxa de transferência para uma carga de trabalho pode cair abaixo do piso especificado em até 5%.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

QoS adaptável

Normalmente, o valor do grupo de políticas que você atribui a um objeto de storage é fixo. Você precisa alterar o valor manualmente quando o tamanho do objeto de armazenamento muda. Um aumento na quantidade de espaço usado em um volume, por exemplo, geralmente requer um aumento correspondente no limite de produtividade especificado para o volume.

O *Adaptive QoS* dimensiona automaticamente o valor do grupo de políticas para o tamanho do workload, mantendo a taxa de IOPS/TB|GB conforme o tamanho do workload muda. Essa é uma vantagem significativa quando você gerencia centenas ou milhares de cargas de trabalho em uma implantação grande.

Normalmente, você usa QoS adaptável para ajustar limites máximos de taxa de transferência, mas também pode usá-la para gerenciar andares de taxa de transferência (quando o tamanho do workload aumenta). O tamanho do workload é expresso como o espaço alocado para o objeto de storage ou o espaço usado pelo objeto de storage.



O espaço usado está disponível para pisos de throughput no ONTAP 9.5 e posterior. Não é suportado para pisos de rendimento no ONTAP 9.4 e anteriores.

A partir do ONTAP 9.13,1, você pode usar QoS adaptável para definir pisos e tetos de taxa de transferência no nível da SVM.

- Uma política *allocated space* mantém a relação IOPS/TB|GB de acordo com o tamanho nominal do objeto de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB terá um limite máximo de taxa de transferência de 15.000 IOPS enquanto o volume permanecer nesse tamanho. Se o volume for redimensionado para 300 GB, a QoS adaptável ajusta o limite da taxa de transferência para 30.000 IOPS.
- Uma política *used space* (o padrão) mantém a taxa IOPS/TB|GB de acordo com a quantidade de dados reais armazenados antes da eficiência de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB que tenha 100 GB de dados armazenados teria um limite máximo de taxa de transferência de 10.000 IOPS. À medida que a quantidade de espaço usado muda, a QoS adaptável ajusta o teto de taxa de transferência de acordo com a taxa.

Replicação

Cópias Snapshot

Tradicionalmente, as tecnologias de replicação da ONTAP atenderam à necessidade de recuperação de desastres (DR) e arquivamento de dados. Com o advento dos serviços de nuvem, a replicação do ONTAP foi adaptada à transferência de dados entre pontos de extremidade no NetApp Data Fabric. A base para todos esses usos é a tecnologia ONTAP Snapshot.

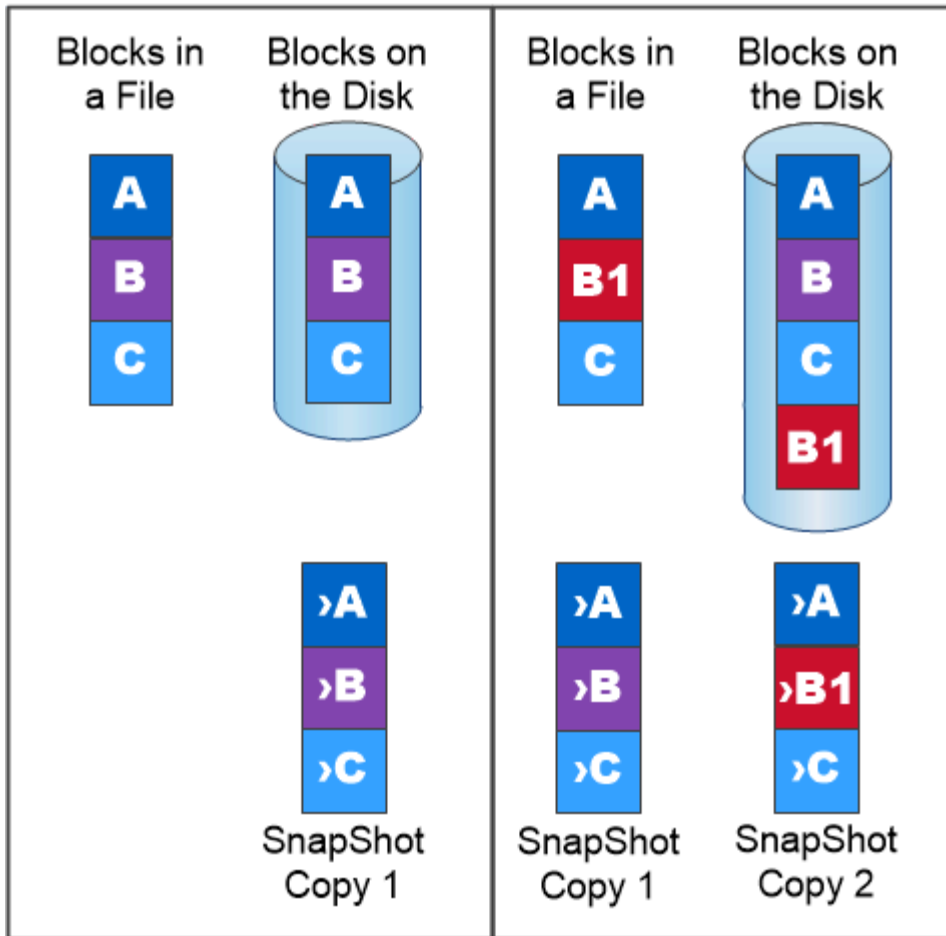
Uma *cópia Snapshot* é uma imagem pontual e somente leitura de um volume. Depois que uma cópia Snapshot é criada, o sistema de arquivos ativo e a cópia Snapshot apontam para os mesmos blocos de disco; portanto, a cópia Snapshot não usa espaço extra em disco. Com o tempo, a imagem consome espaço de armazenamento mínimo e incorre em uma sobrecarga de desempenho insignificante, pois registra apenas alterações nos arquivos desde que a última cópia Snapshot foi feita.

As cópias snapshot devem sua eficiência à tecnologia de virtualização de storage central da ONTAP, seu *Write Anywhere File Layout (WAFL)*. como um banco de dados, o WAFL usa metadados para apontar para blocos de dados reais no disco. Mas, ao contrário de um banco de dados, o WAFL não substitui os blocos existentes. Ele grava dados atualizados em um novo bloco e altera os metadados.

As cópias snapshot são eficientes porque, em vez disso, copiar blocos de dados, o ONTAP faz referência aos metadados ao criar uma cópia Snapshot. Isso elimina tanto o "tempo de busca" que outros sistemas incorrem em localizar os blocos a copiar e o custo de fazer a cópia em si.

Você pode usar uma cópia Snapshot para recuperar arquivos individuais ou LUNs ou restaurar todo o conteúdo de um volume. O ONTAP compara as informações do ponteiro na cópia Snapshot com os dados no disco para reconstruir o objeto em falta ou danificado, sem tempo de inatividade ou um custo significativo de desempenho.

Uma política *Snapshot* define como o sistema cria cópias Snapshot de volumes. A política especifica quando criar as cópias Snapshot, quantas cópias devem ser mantidas, como nomeá-las e como rotulá-las para replicação. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes, nomeá-las "diárias" (anexadas com um carimbo de data/hora) e rotulá-las "diárias" para replicação.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Recuperação de desastres da SnapMirror e transferência de dados

SnapMirror é uma tecnologia de recuperação de desastres, projetada para failover de armazenamento primário para armazenamento secundário em um local geograficamente remoto. Como o nome indica, o SnapMirror cria uma réplica, ou *mirror*, dos seus dados de trabalho em armazenamento secundário a partir do qual você pode continuar a servir dados em caso de uma catástrofe no local principal.

Os dados são espelhados no nível do volume. A relação entre o volume de origem no armazenamento primário e o volume de destino no armazenamento secundário é chamada de *relação de proteção de dados*. Os clusters nos quais os volumes residem e os SVMs que servem dados dos volumes devem ser *peered*. Uma relação de mesmo nível permite que clusters e SVMs troquem dados com segurança.



Você também pode criar uma relação de proteção de dados entre SVMs. Nesse tipo de relacionamento, toda ou parte da configuração do SVM, de exportações de NFS e compartilhamentos de SMB para RBAC, são replicados, bem como os dados nos volumes de sua propriedade.

A partir do ONTAP 9.10.1, você pode criar relacionamentos de proteção de dados entre buckets do S3 usando o SnapMirror S3. Buckets de destino podem estar em sistemas ONTAP locais ou remotos, ou em sistemas

que não sejam da ONTAP, como StorageGRID e AWS.

Na primeira vez que você invocar o SnapMirror, ele executa uma *transferência de linha de base* do volume de origem para o volume de destino. A transferência de linha de base normalmente envolve as seguintes etapas:

- Faça uma cópia Snapshot do volume de origem.
- Transfira a cópia Snapshot e todos os blocos de dados que ela faz referência ao volume de destino.
- Transfira as cópias Snapshot restantes e menos recentes no volume de origem para o volume de destino para o caso de o espelhamento "ativo" estar corrompido.

Quando a transferência de linha de base estiver concluída, o SnapMirror transferirá apenas novas cópias Snapshot para o espelhamento. As atualizações são assíncronas, seguindo a programação configurada. A retenção espelha a política do Snapshot na origem. Você pode ativar o volume de destino com interrupção mínima em caso de desastre no local principal e reativar o volume de origem quando o serviço é restaurado.

Como o SnapMirror transfere apenas cópias Snapshot após a criação da linha de base, a replicação é rápida e sem interrupções. Como o caso de uso de failover indica, as controladoras no sistema secundário devem ser equivalentes ou quase equivalentes às controladoras no sistema primário para atender dados com eficiência do storage espelhado.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

usando SnapMirror para transferência de dados

Você também pode usar o SnapMirror para replicar dados entre pontos de extremidade no NetApp Data Fabric. Você pode escolher entre replicação única ou replicação recorrente ao criar a política do SnapMirror.

Backups da nuvem do SnapMirror para storage de objetos

O *SnapMirror Cloud* é uma tecnologia de backup e recuperação projetada para usuários do ONTAP que desejam transferir seus fluxos de trabalho de proteção de dados para a nuvem. As organizações que se afastam de arquiteturas herdadas de backup para fita

podem usar o storage de objetos como um repositório alternativo para retenção e arquivamento de dados a longo prazo. A nuvem da SnapMirror fornece replicação de storage ONTAP a objeto como parte de uma estratégia incremental de backup para sempre.

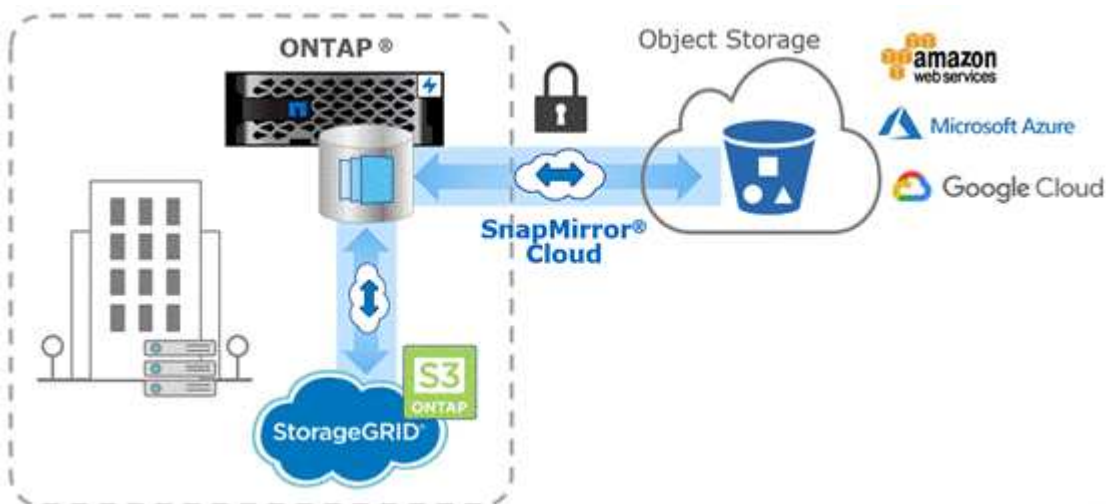
O SnapMirror Cloud foi apresentado no ONTAP 9.8 como uma extensão para a família de tecnologias de replicação do SnapMirror. Embora o SnapMirror seja frequentemente usado para backups de ONTAP para ONTAP, a nuvem do SnapMirror usa o mesmo mecanismo de replicação para transferir cópias Snapshot para ONTAP para backups de storage de objetos em conformidade com S3.

Destinado a casos de uso de backup, o SnapMirror Cloud é compatível com fluxos de trabalho de arquivos e retenção de longo prazo. Assim como no SnapMirror, o backup inicial na nuvem do SnapMirror realiza uma transferência de linha de base de um volume. Para backups subsequentes, o SnapMirror Cloud gera uma cópia snapshot do volume de origem e transfere a cópia snapshot somente com os blocos de dados alterados para um destino de storage de objetos.

As relações de nuvem do SnapMirror podem ser configuradas entre sistemas ONTAP e determinados destinos de storage de objetos no local e na nuvem pública, incluindo Amazon S3, Google Cloud Storage e storage de Blobs do Microsoft Azure. Destinos adicionais de storage de objetos no local incluem o StorageGRID e o ONTAP S3.

A replicação de nuvem do SnapMirror é um recurso licenciado da ONTAP e requer uma aplicação aprovada para orquestrar fluxos de trabalho de proteção de dados. Várias opções de orquestração estão disponíveis para o gerenciamento de backups de nuvem do SnapMirror:

- Vários parceiros de backup de 3rd partes que oferecem suporte para replicação na nuvem da SnapMirror. Os fornecedores participantes estão disponíveis no "[NetApp blog](#)".
- Backup e recuperação do BlueXP para uma solução nativa da NetApp para ambientes ONTAP
- APIs para desenvolver software personalizado para workflows de proteção de dados ou aproveitar ferramentas de automação



Arquivamento SnapVault

A licença do SnapMirror é usada para dar suporte às relações do SnapVault para backup e às relações do SnapMirror para recuperação de desastres. A partir do ONTAP 9.3, as licenças do SnapVault são obsoletas e as licenças do SnapMirror podem ser usadas

para configurar relações de Vault, mirror e mirror-and-Vault. A replicação do SnapMirror é usada para replicação ONTAP para ONTAP de cópias Snapshot, compatível com casos de uso de backup e recuperação de desastres.

O *SnapVault* é uma tecnologia de arquivamento, projetada para replicação de cópias Snapshot de disco para disco para conformidade com padrões e outros fins relacionados à governança. Em contraste com uma relação do SnapMirror, em que o destino geralmente contém apenas as cópias Snapshot atualmente no volume de origem, um destino do SnapVault geralmente retém cópias Snapshot pontuais criadas por um período muito mais longo.

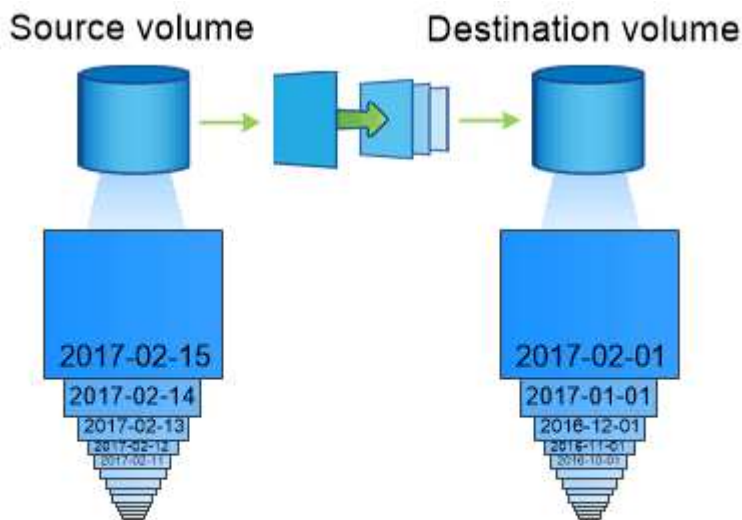
Por exemplo, você pode manter cópias Snapshot mensais de seus dados em um período de 20 anos, para cumprir com as regulamentações contábeis governamentais dos seus negócios. Como não há necessidade de fornecer dados do armazenamento do Vault, você pode usar discos mais lentos e menos caros no sistema de destino.

Tal como acontece com o SnapMirror, o SnapVault executa uma transferência de linha de base na primeira vez que você a invoca. Ele faz uma cópia Snapshot do volume de origem e, em seguida, transfere a cópia e os blocos de dados que ela faz referência ao volume de destino. Diferentemente do SnapMirror, o SnapVault não inclui cópias Snapshot mais antigas na linha de base.

As atualizações são assíncronas, seguindo a programação configurada. As regras definidas na política de relacionamento identificam quais novas cópias snapshot devem incluir nas atualizações e quantas cópias devem ser mantidas. Os rótulos definidos na política ("em quarto lugar", por exemplo) devem corresponder a um ou mais rótulos definidos na política de captura instantânea na origem. Caso contrário, a replicação falha.



SnapMirror e SnapVault compartilham a mesma infraestrutura de comando. Você especifica qual método deseja usar ao criar uma política. Ambos os métodos exigem clusters com peered e SVMs com peered.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Backup em nuvem e suporte para backups tradicionais

Além dos relacionamentos de proteção de dados do SnapMirror e do SnapVault, que eram disco a disco somente para o ONTAP 9.7 e anteriores, agora há várias soluções de backup que oferecem uma alternativa mais econômica para a retenção de dados a longo prazo.

Várias aplicações de proteção de dados de terceiros oferecem backup tradicional para dados gerenciados pela ONTAP. Veeam, Veritas e CommVault, entre outros, oferecem backup integrado para sistemas ONTAP.

A partir do ONTAP 9.8, a nuvem SnapMirror oferece replicação assíncrona de cópias Snapshot de instâncias do ONTAP para pontos de extremidade de storage de objetos. A replicação de nuvem do SnapMirror requer uma aplicação licenciada para orquestração e gerenciamento de workflows de proteção de dados. Os relacionamentos de nuvem da SnapMirror são compatíveis com sistemas ONTAP para selecionar destinos de storage de objetos no local e na nuvem pública, incluindo AWS S3, Google Cloud Storage Platform ou storage de Blobs do Microsoft Azure, o que fornece eficiência aprimorada com software de backup de fornecedor. Entre em Contato com seu representante da NetApp para obter uma lista de aplicativos certificados compatíveis e fornecedores de storage de objetos.

Se você estiver interessado em proteção de dados nativa da nuvem, o BlueXP pode ser usado para configurar relações SnapMirror ou SnapVault entre volumes no local e instâncias do Cloud Volumes ONTAP na nuvem pública.

O BlueXP também fornece backups de instâncias do Cloud Volumes ONTAP usando um modelo de software como serviço (SaaS). Os usuários podem fazer backup de suas instâncias do Cloud Volumes ONTAP em um storage de objetos em nuvem pública compatível com S3 e S3 usando o backup e a recuperação do BlueXP .

["Documentação do Cloud Volumes ONTAP"](#)

["Documentação do BlueXP"](#)

["NetApp BlueXP"](#)

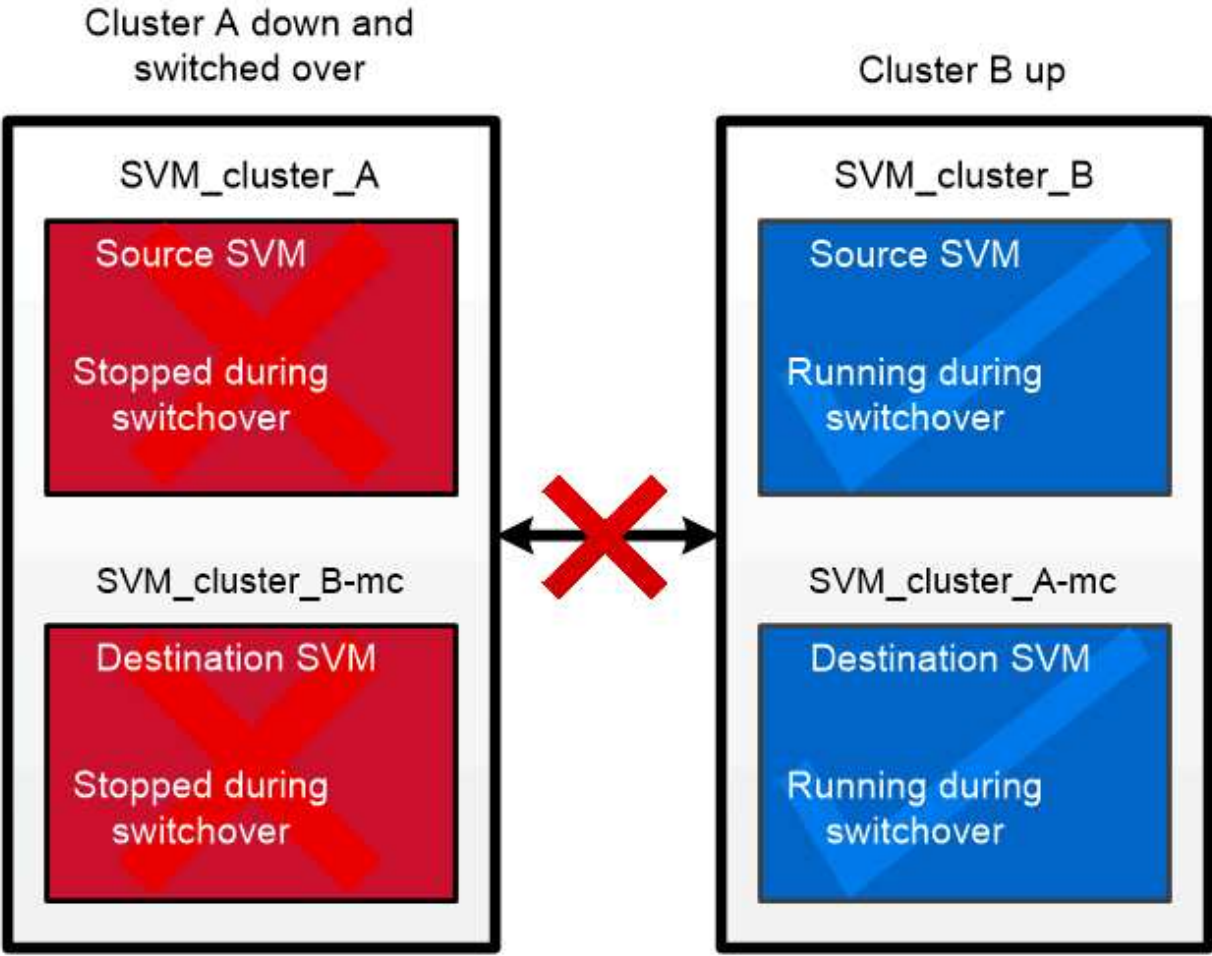
Disponibilidade contínua da MetroCluster

As configurações do MetroCluster protegem os dados com a implementação de dois clusters espelhados separados fisicamente. Cada cluster replica de forma síncrona os dados e a configuração da SVM do outro. Em caso de desastre em um local, o administrador pode ativar o SVM espelhado e começar a fornecer dados do local que sobreviveu.

- As configurações de *Fabric-Attached MetroCluster* e *MetroCluster IP* são compatíveis com clusters metropolitano.
- As configurações do *Stretch MetroCluster* suportam clusters em todo o campus.

Os clusters devem ser percorridos em ambos os casos.

O MetroCluster usa um recurso ONTAP chamado *SyncMirror* para espelhar sincronamente dados agregados para cada cluster em cópias ou *plexes* no armazenamento do outro cluster. Se ocorrer um switchover, o Plex remoto no cluster sobrevivente fica on-line e o SVM secundário começa a fornecer dados.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

Using SyncMirror em implementações não-MetroCluster você pode usar o SyncMirror em uma implementação não-MetroCluster para proteger contra perda de dados se mais discos falharem do que o tipo RAID protege contra, ou se houver perda de conectividade com discos do grupo RAID. O recurso está disponível somente para pares de HA.

Os dados agregados são espelhados em plexos armazenados em diferentes compartimentos de disco. Se uma das gavetas ficar indisponível, o Plex não afetado continuará fornecendo dados enquanto você corrigir a causa da falha.

Tenha em mente que um agregado espelhado usando o SyncMirror requer o dobro de storage que um agregado sem espelhamento. Cada Plex requer tantos discos quanto o Plex que ele espelha. Você precisaria de 2.880 GB de espaço em disco, por exemplo, para espelhar um agregado de 1.440 GB, 1.440 GB para cada Plex.

Com o SyncMirror, é recomendável manter pelo menos 20% de espaço livre para agregados espelhados para performance e disponibilidade ideais de storage. Embora a recomendação seja de 10% para agregados não espelhados, os 10% adicionais de espaço podem ser usados pelo sistema de arquivos para absorver alterações incrementais. Mudanças incrementais aumentam a utilização de espaço para agregados espelhados devido à arquitetura baseada em Snapshot copy-on-write da ONTAP. A não adesão a essas práticas recomendadas pode ter um impacto negativo no desempenho de resincronização do SyncMirror, o que afeta indiretamente fluxos de trabalho operacionais, como NDU para implantações de nuvem não compartilhadas e switchback para implantações de MetroCluster.



O SyncMirror também está disponível para implementações de virtualização FlexArray.

Eficiência de storage

Visão geral da eficiência de storage da ONTAP

A eficiência de storage é a medida de como um sistema de storage utiliza o espaço disponível com a otimização dos recursos de storage, a minimização do desperdício de espaço e a redução do espaço físico dos dados gravados. Uma maior eficiência de storage permite armazenar a quantidade máxima de dados no menor espaço possível com o menor custo possível. Por exemplo, a utilização de tecnologias eficientes de storage que detetam e eliminam blocos de dados duplicados e blocos de dados preenchidos com zeros diminui a quantidade geral de storage físico de que você precisa e reduz o custo geral.

O ONTAP oferece uma ampla gama de tecnologias de eficiência de storage que reduzem a quantidade de hardware físico ou storage de nuvem consumida pelos dados, além de gerar melhorias significativas na performance do sistema, incluindo leituras mais rápidas de dados, cópias mais rápidas dos conjuntos de dados e provisionamento de VM mais rápido.

As tecnologias de eficiência de storage da ONTAP incluem:

- * Provisionamento thin*

Thin Provisioning Permite alocar armazenamento em um volume ou LUN conforme necessário, em vez de reservá-lo com antecedência. Isso reduz a quantidade de storage físico de que você precisa, permitindo alocar em excesso seus volumes ou LUNs com base no uso potencial sem reservar espaço que não está sendo usado atualmente.

• **Desduplicação**

Desduplicação reduz a quantidade de armazenamento físico necessária para um volume de três maneiras distintas.

◦ **Deduplicação de bloco zero**

A deduplicação de bloco zero detecta e elimina blocos de dados preenchidos com todos os zeros e apenas atualiza metadados. 100% do espaço normalmente usado por blocos zero é então salvo. A deduplicação de bloco zero é ativada por padrão em todos os volumes desduplicados.

◦ **Deduplicação in-line**

A deduplicação in-line detecta blocos de dados duplicados e os substitui por referências a um bloco compartilhado exclusivo antes que os dados sejam gravados no disco. A deduplicação in-line acelera o provisionamento de VM em 20% a 30%. Dependendo da sua versão do ONTAP e da sua plataforma, a deduplicação in-line está disponível no nível de volume ou agregado. Ele é habilitado por padrão em sistemas AFF e ASA. Você precisa habilitar manualmente a deduplicação in-line em sistemas FAS.

◦ * Deduplicação em segundo plano*

A deduplicação em segundo plano também detecta blocos de dados duplicados e os substitui por referências a um bloco compartilhado exclusivo. No entanto, aumenta ainda mais a eficiência de storage fazendo isso depois que os dados são gravados no disco. Você pode configurar a deduplicação em segundo plano para ser executada quando certos critérios são atendidos no sistema de storage. Por exemplo, você pode habilitar a deduplicação em segundo plano quando o volume atingir 10% de utilização. Você também pode acionar manualmente a deduplicação em segundo plano ou configurá-la para ser executada em um cronograma específico. Ele é habilitado por padrão em sistemas AFF e ASA. Você precisa habilitar manualmente a deduplicação em segundo plano em sistemas FAS.

A deduplicação é compatível com volumes e volumes em um agregado. Leituras de dados deduplicados normalmente não implicam custos de desempenho.

• **Compressão**

Compactação reduz a quantidade de storage físico necessária para um volume, combinando blocos de dados em grupos de compressão, cada um dos quais é armazenado como um único bloco. Quando uma solicitação de leitura ou substituição é recebida, apenas um pequeno grupo de blocos é lido, não o arquivo inteiro. Este processo otimiza o desempenho de leitura e substituição e permite uma maior escalabilidade no tamanho dos arquivos que estão sendo compactados.

A compressão pode ser executada em linha ou no pós-processo. A compactação in-line proporciona economia imediata de espaço ao compactar dados na memória antes de serem gravados no disco. A compressão pós-processo primeiro grava os blocos no disco como descompactados e, em seguida, em um horário programado comprime os dados. Ele é habilitado por padrão em sistemas AFA. Você precisa ativar manualmente a compactação em todos os outros sistemas.

• **Compactação**

A compactação reduz a quantidade de storage físico necessária para um volume, tomando blocos de dados armazenados em blocos de 4 KB, mas com menos de 4 KB de tamanho e combinando-os em um único bloco. A compactação ocorre enquanto os dados ainda estão na memória para que espaço desnecessário nunca seja consumido nos discos. Ele é habilitado por padrão em sistemas AFF e ASA. É necessário ativar manualmente a compactação em sistemas FAS.

- **Volumes, arquivos e LUNs do FlexClone**

Tecnologia FlexClone Aproveita os metadados do Snapshot para criar cópias graváveis e pontuais de um volume, arquivo ou LUN. As cópias compartilham blocos de dados com os pais, não consumindo storage, exceto o necessário para os metadados até que as alterações sejam gravadas em uma cópia ou seu pai. Quando uma alteração é escrita, apenas o delta é armazenado.

Onde as cópias tradicionais de conjuntos de dados podem levar minutos ou até horas para criar, a tecnologia FlexClone permite copiar até mesmo os maiores conjuntos de dados quase instantaneamente.

- * Eficiência de armazenamento sensível à temperatura*

O ONTAP fornece "**eficiência de storage sensível à temperatura**" benefícios avaliando a frequência com que os dados do seu volume são acessados e mapeando essa frequência para o grau de compressão aplicado a esses dados. Para dados inativos acessados com pouca frequência, blocos de dados maiores são compactados. Para dados ativos acessados com frequência e substituídos com mais frequência, blocos de dados menores são compactados, tornando o processo mais eficiente.

A eficiência de storage sensível à temperatura (TSSE), introduzida no ONTAP 9.8, é ativada automaticamente em volumes AFF recém-criados com provisionamento reduzido. Ele não está habilitado no "**Plataformas AFF A70, AFF A90 e AFF A1K**" que são introduzidos no ONTAP 9.15,1, que usam um processador de descarga de hardware.

- * CPU ou eficiência de armazenamento dedicado do processador de descarga*

A partir do ONTAP 9.15,1, o ONTAP fornece "**CPU ou eficiência de storage do processador de descarga dedicado**" e dá compactação de dados nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90. Nos sistemas AFF A70, AFF A90 e AFF A1K, a eficiência de storage é ativada automaticamente e não requer configuração.

Você pode aproveitar essas tecnologias em suas operações diárias com o mínimo de esforço. Por exemplo, suponha que você precise fornecer 5.000 usuários com armazenamento para diretórios base, e você estima que o espaço máximo necessário para qualquer usuário é de 1 GB. Você pode reservar um agregado de 5 TB com antecedência para atender à necessidade total de storage potencial. No entanto, você também sabe que os requisitos de capacidade do diretório base variam muito em toda a sua organização. Em vez de reservar 5 TB de espaço total para sua organização, você pode criar um agregado de 2 TB. Em seguida, você pode usar thin Provisioning para atribuir nominalmente 1 GB de armazenamento a cada usuário, mas alocar o armazenamento apenas conforme necessário. Você pode monitorar ativamente o agregado ao longo do tempo e aumentar o tamanho físico real, conforme necessário.

Em outro exemplo, suponha que você esteja usando uma infraestrutura de desktop virtual (VDI) com uma grande quantidade de dados duplicados entre seus desktops virtuais. A deduplicação reduz o uso do storage eliminando automaticamente blocos duplicados de informações na VDI, substituindo-os por um ponteiro para o bloco original. Outras tecnologias de eficiência de storage da ONTAP, como a compactação, também podem ser executadas em segundo plano sem intervenção.

A tecnologia de particionamento de disco da ONTAP também oferece maior eficiência de storage. A tecnologia RAID DP protege contra falhas duplas de disco sem sacrificar o desempenho ou adicionar sobrecarga de espelhamento de disco. O particionamento avançado de SSD com ONTAP 9 aumenta a capacidade utilizável em quase 20%.

O NetApp fornece os mesmos recursos de eficiência de storage disponíveis no ONTAP local na nuvem. Ao migrar dados do ONTAP no local para a nuvem, a eficiência de storage existente é preservada. Por exemplo, suponha que você tenha um banco de dados SQL contendo dados essenciais aos negócios que deseja mover de um sistema local para a nuvem. Você pode usar a replicação de dados no BlueXP para migrar seus dados

e, como parte do processo de migração, ativar a política mais recente no local para cópias Snapshot na nuvem.

Thin Provisioning

A ONTAP oferece uma ampla variedade de tecnologias de eficiência de storage, além das cópias Snapshot. As principais tecnologias incluem thin Provisioning, deduplicação, compactação e volumes, arquivos e LUNs do FlexClone. Assim como as cópias Snapshot, todas são criadas no WAFL (Write Anywhere File Layout) do ONTAP.

Um volume ou LUN *thin-provisionado* é aquele para o qual o armazenamento 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.

Suponha que sua organização precisa fornecer aos usuários do 5.000 o armazenamento para diretórios base. Você estima que os maiores diretórios base consumirão 1 GB de espaço.

Nesta situação, você pode comprar 5 TB de armazenamento físico. Para cada volume que armazena um diretório home, você reservaria espaço suficiente para satisfazer as necessidades dos maiores consumidores.

No entanto, como uma questão prática, você também sabe que os requisitos de capacidade do diretório base variam muito em toda a sua comunidade. Para cada grande usuário de armazenamento, há dez que consomem pouco ou nenhum espaço.

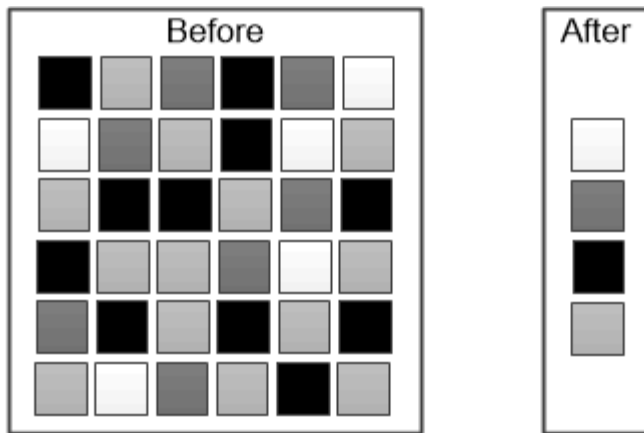
O thin Provisioning permite que você atenda às necessidades dos grandes consumidores de storage sem ter que comprar storage que você talvez nunca use. Como o espaço de armazenamento não é alocado até ser consumido, você pode "comprometer" um agregado de 2 TB, atribuindo nominalmente um tamanho de 1 GB a cada um dos 5.000 volumes que o agregado contém.

Contanto que você esteja correto que haja uma proporção de 10:1 de usuários leves para pesados, e contanto que você assuma um papel ativo no monitoramento de espaço livre no agregado, você pode ter certeza de que as gravações de volume não falharão devido à falta de espaço.

Deduplicação

Desduplicação reduz a quantidade de armazenamento físico necessária para um volume (ou todos os volumes em um agregado AFF) descartando blocos duplicados e substituindo-os por referências a um único bloco compartilhado. Leituras de dados deduplicados normalmente não implicam custos de desempenho. As gravações incorrem em uma cobrança insignificante, exceto em nós sobrecarregados.

À medida que os dados são gravados durante o uso normal, o WAFL usa um processo em lote para criar um catálogo de assinaturas de bloco. Depois que a deduplicação é iniciada, o ONTAP compara as assinaturas no catálogo para identificar blocos duplicados. Se existir uma correspondência, uma comparação byte-a-byte é feita para verificar se os blocos candidatos não foram alterados desde que o catálogo foi criado. Somente se todos os bytes corresponderem é o bloco duplicado descartado e seu espaço em disco recuperado.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

Compactação

Compression reduz a quantidade de armazenamento física necessária para um volume combinando blocos de dados em *grupos de compressão*, cada um dos quais é armazenado como um único bloco. As leituras de dados compactados são mais rápidas do que nos métodos de compactação tradicionais porque o ONTAP descompacta apenas os grupos de compactação que contêm os dados solicitados, não um arquivo inteiro ou LUN.

Você pode executar a compressão inline ou pós-processo, separadamente ou em combinação:

- *Compactação in line* compacta os dados na memória antes de serem gravados no disco, reduzindo significativamente a quantidade de e/S de gravação em um volume, mas potencialmente degradando o desempenho de gravação. Operações intensivas em desempenho são adiadas até a próxima operação de compressão pós-processo, se houver.
- *Pós-process Compression* compacta os dados depois que eles são gravados no disco, no mesmo cronograma da deduplicação.

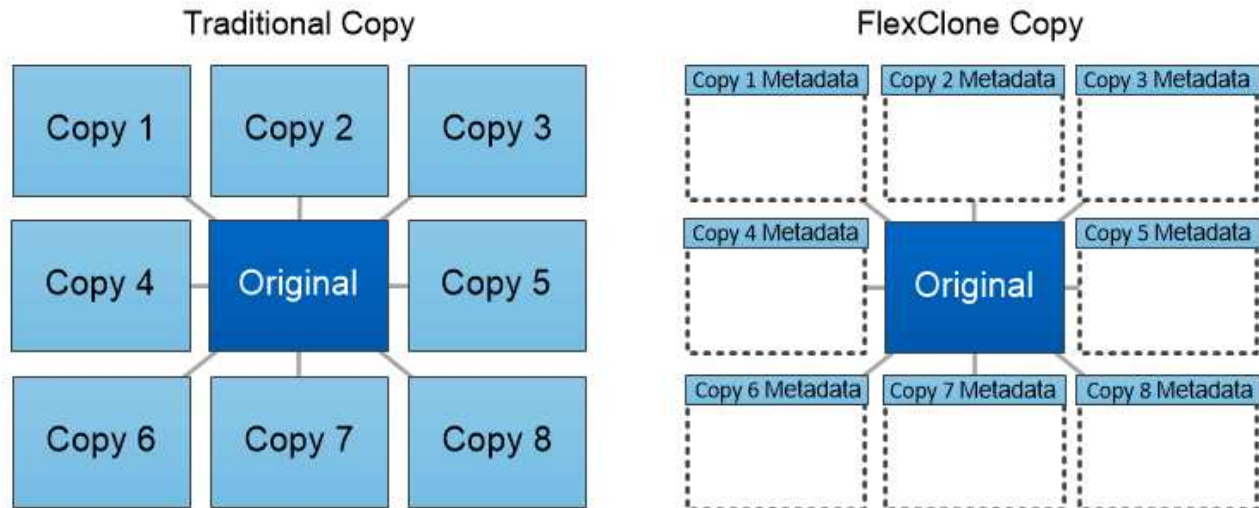
compactação de dados em linha pequenos arquivos ou e/S acolchoados com zeros são armazenados em um bloco de 4 KB, quer eles exijam ou não 4 KB de armazenamento físico. *Compactação de dados em linha* combina blocos de dados que normalmente consumiriam vários blocos de 4 KB em um único bloco de 4 KB no disco. A compactação ocorre enquanto os dados ainda estão na memória, por isso é mais adequada para controladoras mais rápidas.

Volumes, arquivos e LUNs do FlexClone

A tecnologia *FlexClone* faz referência aos metadados do Snapshot para criar cópias graváveis e pontuais de um volume. As cópias compartilham blocos de dados com os pais, não consumindo storage, exceto o necessário para os metadados até que as alterações sejam gravadas na cópia. Os arquivos FlexClone e os LUNs FlexClone usam tecnologia idêntica, exceto que uma cópia Snapshot de backup não é necessária.

Onde as cópias tradicionais podem levar minutos ou até horas para criar, o software FlexClone permite copiar até mesmo os maiores conjuntos de dados quase instantaneamente. Isso o torna ideal para situações em que você precisa de várias cópias de conjuntos de dados idênticos (uma implantação de desktop virtual, por exemplo) ou cópias temporárias de um conjunto de dados (testando uma aplicação em um conjunto de dados de produção).

Você pode clonar um volume FlexClone existente, clonar um volume contendo clones de LUN ou clonar dados espelhados e Vault. Você pode *dividir* um volume FlexClone de seu pai, caso em que a cópia é alocada seu próprio armazenamento.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

Medições de capacidade no System Manager

A capacidade do sistema pode ser medida como espaço físico ou espaço lógico. A partir do ONTAP 9.7, o Gerenciador de sistemas fornece medições de capacidade física e lógica.

As diferenças entre as duas medições são explicadas nas seguintes descrições:

- **Capacidade física:** O espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume ou nível local. O valor da capacidade física usada geralmente é menor do que o valor da capacidade lógica usada devido à redução de dados de recursos de eficiência de storage (como deduplicação e compactação).
- **Capacidade lógica:** O espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume ou nível local. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados da deduplicação ou compressão. O valor do espaço lógico usado é derivado da quantidade de espaço físico usado, além da economia com recursos de eficiência de storage (como deduplicação e compactação) configurados. Essa medição geralmente parece maior do que a capacidade física usada porque inclui cópias Snapshot, clones e outros componentes, e não reflete a compactação de dados e outras reduções no espaço físico. Assim, a capacidade lógica total poderia ser maior do que o espaço provisionado.



No System Manager, as representações de capacidade não são responsáveis pelas capacidades da camada de storage raiz (agregado).

Medições da capacidade utilizada

As medições da capacidade utilizada são apresentadas de forma diferente, dependendo da versão do System Manager que estiver a utilizar, conforme explicado na seguinte tabela:

Versão do System Manager	Termo usado para a capacidade	Tipo de capacidade referida
9.9.1 e mais tarde	Lógica utilizada	Espaço lógico utilizado se as definições de eficiência de armazenamento tiverem sido ativadas)
9,7 e 9,8	Usado	Espaço lógico utilizado (se as definições de eficiência de armazenamento tiverem sido ativadas)
9,5 e 9,6 (vista clássica)	Usado	Espaço físico utilizado

Termos de medição da capacidade

Os seguintes termos são usados ao descrever a capacidade:

- **Capacidade alocada:** A quantidade de espaço que foi alocada para volumes em uma VM de armazenamento.
- **Disponível:** A quantidade de espaço físico disponível para armazenar dados ou provisionar volumes em uma VM de storage ou em um nível local.
- **Capacidade entre volumes:** A soma do armazenamento usado e do armazenamento disponível de todos os volumes em uma VM de armazenamento.
- **Dados do cliente:** A quantidade de espaço usada pelos dados do cliente (físico ou lógico).
 - A partir do ONTAP 9.13,1, a capacidade usada pelos dados do cliente é chamada de **Logical Used**, e a capacidade usada pelas cópias Snapshot é exibida separadamente.
 - No ONTAP 9.12,1 e anterior, a capacidade usada pelos dados do cliente adicionada à capacidade usada pelas cópias Snapshot é referida como **Logical Used**.
- *** Comprometido*:** O montante da capacidade comprometida para um nível local.
- **Redução de dados:** A relação entre o tamanho dos dados ingeridos e o tamanho dos dados armazenados.
 - A partir do ONTAP 9.13,1, a redução de dados considera os resultados da maioria dos recursos de eficiência de storage, como deduplicação e compactação. No entanto, snapshots e thin Provisioning não são contados como parte da taxa de redução de dados.
 - No ONTAP 9.12,1 e anteriores, as relações de redução de dados são apresentadas da seguinte forma:
 - O valor de redução de dados exibido no painel **capacidade** é a proporção geral de todo o espaço lógico usado em comparação com o espaço físico usado, e inclui os benefícios derivados do uso de cópias Snapshot e outros recursos de eficiência de storage.
 - Quando você exibe o painel de detalhes, você vê a proporção **geral** exibida no painel de visão geral e a proporção do espaço lógico usado somente pelos dados do cliente em comparação com o espaço físico usado somente pelos dados do cliente, conhecido como **sem cópias Snapshot e clones**.

- **Utilização lógica:**

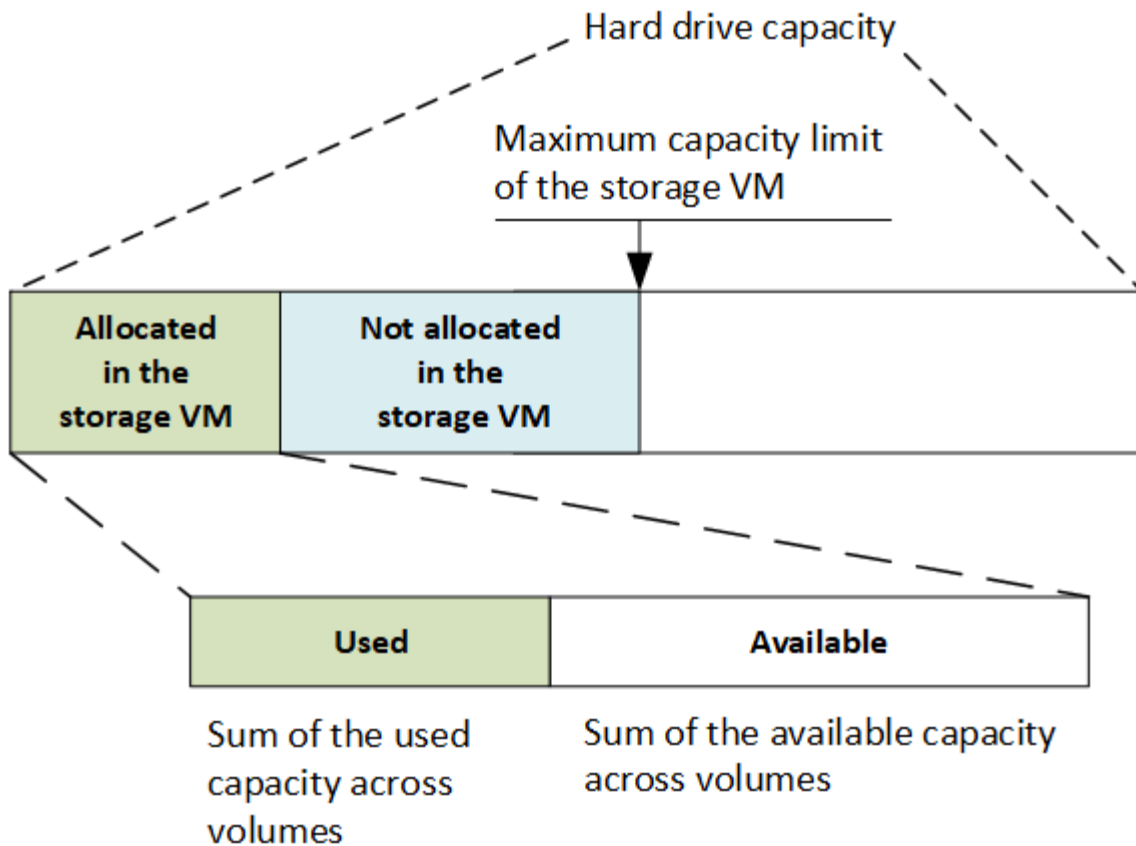
- A partir do ONTAP 9.13,1, a capacidade usada pelos dados do cliente é chamada de **Logical Used**, e a capacidade usada pelas cópias Snapshot é exibida separadamente.
- No ONTAP 9.12,1 e anterior, a capacidade usada pelos dados do cliente adicionada à capacidade usada pelas cópias Snapshot é referida como **uso lógico**.
- **% De utilização lógica:** A percentagem da capacidade lógica utilizada atual em comparação com o tamanho provisionado, excluindo reservas de instantâneos. Esse valor pode ser superior a 100%, pois inclui economia de eficiência no volume.
- **Capacidade máxima:** A quantidade máxima de espaço alocada para volumes em uma VM de armazenamento.
- **Físico usado:** A quantidade de capacidade usada nos blocos físicos de um volume ou nível local.
- *** % Física usada*:** A porcentagem de capacidade usada nos blocos físicos de um volume em comparação com o tamanho provisionado.
- **Capacidade provisionada:** Um sistema de arquivos (volume) que foi alocado de um sistema Cloud Volumes ONTAP e está pronto para armazenar dados de usuário ou aplicativo.
- **Reservado:** A quantidade de espaço reservado para volumes já provisionados em um nível local.
- **Usado:** A quantidade de espaço que contém dados.
- **Usado e reservado:** A soma do espaço físico utilizado e reservado.

Capacidade de uma VM de storage

A capacidade máxima de uma VM de armazenamento é determinada pelo espaço total alocado para volumes mais o espaço não alocado restante.

- O espaço alocado para volumes é a soma da capacidade usada e a soma da capacidade disponível dos volumes FlexVol, volumes FlexGroup e volumes FlexCache.
- A capacidade dos volumes está incluída nas somas, mesmo quando elas estão restritas, offline ou na fila de recuperação após a exclusão.
- Se os volumes estiverem configurados com crescimento automático, o valor máximo de dimensionamento automático do volume será usado nas somas. Sem crescimento automático, a capacidade real do volume é usada nas somas.

O gráfico a seguir explica como a medição da capacidade entre volumes se relaciona com o limite máximo de capacidade.



A partir do ONTAP 9.13,1, os administradores de cluster podem "[Habilite um limite máximo de capacidade para uma VM de storage](#)". No entanto, os limites de storage não podem ser definidos para uma VM de storage que contenha volumes para proteção de dados, em um relacionamento com a SnapMirror ou em uma configuração do MetroCluster. Além disso, as cotas não podem ser configuradas para exceder a capacidade máxima de uma VM de armazenamento.

Depois de definir o limite máximo de capacidade, não pode ser alterado para um tamanho inferior à capacidade atualmente alocada.

Quando uma VM de armazenamento atinge seu limite máximo de capacidade, certas operações não podem ser executadas. O System Manager fornece sugestões para as próximas etapas no "[Insights](#)".

Unidades de medição da capacidade

O System Manager calcula a capacidade de armazenamento com base em unidades binárias de 1024 (2,10) bytes.

- A partir do ONTAP 9.10,1, as unidades de capacidade de armazenamento são exibidas no System Manager como KiB, MiB, GiB, TiB e PiB.
- No ONTAP 9.10,0 e anterior, essas unidades são exibidas no Gerenciador de sistema como KB, MB, GB, TB e PB.



As unidades usadas no Gerenciador de sistemas para taxa de transferência continuam a ser KB/s, MB/s, GB/s, TB/s e PB/s para todas as versões do ONTAP.

Unidade de capacidade exibida no Gerenciador do sistema para ONTAP 9.10,0 e anterior	Unidade de capacidade exibida no Gerenciador do sistema para ONTAP 9.10,1 e posterior	Cálculo	Valor em bytes
KB	KiB	1024	1024 bytes
MB	MiB	1024 * 1024	1.048.576 bytes
GB	GiB	1024 * 1024 * 1024	1.073.741.824 bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1.125.899.906.842.624 bytes

Informações relacionadas

["Monitorar a capacidade no System Manager"](#)

["Relatórios de espaço lógico e imposição para volumes"](#)

Visão geral da eficiência de storage sensível à temperatura

O ONTAP fornece benefícios de eficiência de storage sensíveis à temperatura ao avaliar a frequência com que os dados do volume são acessados e mapear essa frequência para o nível de compressão aplicado a esses dados. Para dados inativos acessados com pouca frequência, blocos de dados maiores são compactados e, para dados ativos, acessados com frequência e substituídos com mais frequência, blocos de dados menores são compactados, tornando o processo mais eficiente.

A eficiência de storage sensível à temperatura (SSE) é introduzida no ONTAP 9.8 e é ativada automaticamente em volumes AFF recém-criados com provisionamento reduzido. Você pode ativar a eficiência de storage sensível à temperatura em volumes AFF existentes e em volumes DP não AFF provisionados de forma fina.



A eficiência de storage sensível à temperatura não é aplicada nas plataformas AFF A70, AFF A90 e AFF A1K. A compactação não se baseia em dados ativos ou inativos nessas plataformas. Portanto, a compactação começa sem esperar que os dados fiquem inativos.

Introdução dos modos "padrão" e "eficiente"

A partir do ONTAP 9.10,1, os modos de eficiência de storage no nível de volume *default* e *efficient* são introduzidos apenas para sistemas AFF. Os dois modos oferecem a opção entre compactação de arquivos (padrão), que é o modo padrão ao criar novos volumes AFF ou eficiência de storage sensível à temperatura (eficiente), que permite a eficiência de storage sensível à temperatura. Com o ONTAP 9.10,1, ["a eficiência de storage sensível à temperatura deve ser definida explicitamente"](#) para ativar a compressão adaptável automática. No entanto, outros recursos de eficiência de storage, como compactação de dados, cronograma de deduplicação automática, deduplicação in-line entre volumes e deduplicação em segundo plano entre

volumes, são habilitados por padrão nas plataformas AFF para os modos padrão e eficiente.

Ambos os modos de eficiência de storage (padrão e eficiente) são compatíveis com agregados habilitados para FabricPool e com todos os tipos de política de disposição em camadas.

Eficiência de storage sensível à temperatura ativada nas plataformas C-Series

A eficiência de storage sensível à temperatura é habilitada por padrão nas plataformas AFF C-Series e ao migrar volumes de uma plataforma que não seja TSSE para uma plataforma C-Series habilitada para TSSE usando a movimentação de volume ou SnapMirror com as seguintes versões instaladas no destino:

- ONTAP 9.12.1P4 e posterior
- ONTAP 9.13,1 e posterior

Para obter mais informações, "[Comportamento de eficiência de storage com movimentação de volume e operações de SnapMirror](#)" consulte .

No caso dos volumes existentes, a eficiência de storage sensível à temperatura não é ativada automaticamente. No entanto, é possível "[modificar o modo de eficiência de storage](#)" alterar manualmente para o modo eficiente.



Depois de alterar o modo de eficiência de storage para eficiente, você não poderá alterá-lo novamente.

Eficiência de storage aprimorada com embalagem sequencial de blocos físicos contíguos

A partir do ONTAP 9.13,1, a eficiência de storage sensível à temperatura adiciona empacotamento sequencial de blocos físicos contíguos para aprimorar ainda mais a eficiência de storage. Os volumes que têm a eficiência de storage sensível à temperatura ativada automaticamente têm o empacotamento sequencial habilitado quando você atualiza os sistemas para o ONTAP 9.13,1. Depois que a embalagem sequencial estiver ativada, é "[reembalar manualmente os dados existentes](#)" necessário .

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1 e posterior, os volumes existentes recebem um modo de eficiência de storage com base no tipo de compactação atualmente habilitado nos volumes. Durante uma atualização, os volumes com compressão ativada recebem o modo padrão e os volumes com eficiência de storage sensível à temperatura ativada recebem o modo eficiente. Se a compactação não estiver ativada, o modo de eficiência de storage permanecerá em branco.

CPU ou eficiência de storage do processador de descarga dedicado

A partir do ONTAP 9.15,1, o ONTAP oferece eficiência de storage e compactação de dados nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90.

Dependendo da plataforma, o seguinte se aplica ao atualizar:

- A compactação é realizada usando a CPU principal ou com um processador de descarga dedicado.
- A eficiência de storage é habilitada por padrão em todos os volumes com thin Provisioning ou apenas volumes existentes.

Para uma plataforma FF A70, AFF A90 ou AFF A1K, a eficiência de storage é ativada automaticamente e não requer configuração. Isso se aplica a todos os volumes thin Provisioning e dados existentes recentemente criados, incluindo volumes movidos de outras plataformas para uma plataforma AFF A70,

AFF A90 ou AFF A1K.

Para uma plataforma FAS70 ou FAS90, a eficiência de storage é habilitada por padrão somente nos volumes thin Provisioning existentes que tiveram a eficiência de storage habilitada antes da atualização. Você pode ativar a eficiência de storage em volumes criados recentemente usando o método de CLI ou API REST.

- Os dados migrados usando a tecnologia de movimentação de volume ou SnapMirror são convertidos automaticamente para compactação in-line de 32k TB:

Para uma plataforma AFF A70, AFF A90 ou AFF A1K, os dados são convertidos automaticamente.

Para uma plataforma FAS70 ou FAS90, os dados são convertidos somente se a compactação foi ativada na plataforma original.

A eficiência de storage sensível à temperatura não é aplicada nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90. A compactação não se baseia em dados ativos ou inativos nessas plataformas. Portanto, a compactação começa sem esperar que os dados fiquem inativos.

A eficiência de storage nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90 usa a embalagem sequencial de blocos físicos contíguos para aprimorar ainda mais a eficiência de storage para dados compactados.

Para obter informações sobre como atualizar uma controladora para um AFF A70, AFF A90, AFF A1K, FAS70 ou FAS90, consulte "[Documentação de atualização de hardware da ONTAP](#)".

Segurança

Autenticação e autorização do cliente

O ONTAP usa métodos padrão para proteger o acesso do cliente e do administrador ao armazenamento e para proteger contra vírus. Tecnologias avançadas estão disponíveis para criptografia de dados em repouso e para storage WORM.

O ONTAP autentica uma máquina cliente e um usuário verificando suas identidades com uma fonte confiável. O ONTAP autoriza um usuário a acessar um arquivo ou diretório comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório.

Autenticação

Você pode criar contas de usuário locais ou remotas:

- Uma conta local é aquela em que as informações da conta residem no sistema de armazenamento.
- Uma conta remota é aquela em que as informações de conta são armazenadas em um controlador de domínio do Active Directory, um servidor LDAP ou um servidor NIS.

O ONTAP usa serviços de nomes locais ou externos para procurar informações de mapeamento de nome, usuário, grupo, grupo netgroup e nome do host. O ONTAP oferece suporte aos seguintes serviços de nomes:

- Usuários locais
- DNS

- Domínios NIS externos
- Domínios LDAP externos

Uma tabela *name Service switch* especifica as fontes para procurar informações de rede e a ordem na qual pesquisá-las (fornecendo a funcionalidade equivalente do arquivo `/etc/nsswitch.conf` em sistemas UNIX). Quando um cliente nas se conecta ao SVM, o ONTAP verifica os serviços de nome especificados para obter as informações necessárias.

Kerberos support Kerberos é um protocolo de autenticação de rede que fornece "autenticação de conexão", criptografando senhas de usuário em implementações cliente-servidor. O ONTAP suporta autenticação Kerberos 5 com verificação de integridade (krb5i) e autenticação Kerberos 5 com verificação de privacidade (krb5p).

Autorização

O ONTAP avalia três níveis de segurança para determinar se uma entidade está autorizada a executar uma ação solicitada em arquivos e diretórios localizados em um SVM. O acesso é determinado pelas permissões efetivas após a avaliação dos níveis de segurança:

- Segurança de exportação (NFS) e compartilhamento (SMB)

A segurança de exportação e compartilhamento se aplica ao acesso do cliente a uma determinada exportação NFS ou compartilhamento SMB. Os usuários com Privileges administrativo podem gerenciar a segurança de exportação e compartilhamento a partir de clientes SMB e NFS.

- Segurança de arquivo e diretório do Access Guard no nível de armazenamento

A segurança do Access Guard no nível de storage se aplica ao acesso de clientes SMB e NFS aos volumes SVM. Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

- Segurança nativa em nível de arquivo NTFS, UNIX e NFSv4

A segurança de nível de arquivo nativo existe no arquivo ou diretório que representa o objeto de storage. Você pode definir a segurança no nível do arquivo de um cliente. As permissões de arquivo são efetivas independentemente de SMB ou NFS serem usados para acessar os dados.

Autenticação com SAML

O ONTAP suporta a linguagem de marcação de asserção de Segurança (SAML) para autenticação de usuários remotos. Vários provedores de identidade populares (IDPs) são suportados. Para obter mais informações sobre IDPs suportados e instruções para ativar a autenticação SAML, ["Configurar a autenticação SAML"](#) consulte .

OAuth 2,0 com clientes API REST do ONTAP

O suporte para a estrutura de autorização aberta (OAuth 2,0) está disponível a partir do ONTAP 9.14. Você só pode usar o OAuth 2,0 para tomar decisões de autorização e controle de acesso quando o cliente usa a API REST para acessar o ONTAP. No entanto, você pode configurar e ativar o recurso com qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI, o Gerenciador de sistema e a API REST.

Os recursos padrão do OAuth 2,0 são suportados juntamente com vários servidores de autorização populares. Você pode aprimorar ainda mais a segurança do ONTAP usando tokens de acesso restritos ao remetente baseados no TLS mútuo. E há uma ampla variedade de opções de autorização disponíveis, incluindo escopos autônomos, bem como integração com as funções REST do ONTAP e definições de usuário local. Consulte ["Visão geral da implementação do ONTAP OAuth 2,0"](#) para obter mais informações.

Autenticação de administrador e RBAC

Os administradores usam contas de login locais ou remotas para se autenticar no cluster e na SVM. O controle de acesso baseado em função (RBAC) determina os comandos aos quais um administrador tem acesso.

Autenticação

Você pode criar contas de administrador de cluster local ou remoto e SVM:

- Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento.
- Uma conta remota é aquela em que as informações de conta são armazenadas em um controlador de domínio do Active Directory, um servidor LDAP ou um servidor NIS.

Exceto o DNS, o ONTAP usa os mesmos serviços de nome para autenticar contas de administrador que ele usa para autenticar clientes.

RBAC

A *função* atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Verificação de vírus

Você pode usar a funcionalidade de antivírus integrada no sistema de armazenamento para proteger os dados contra o comprometimento por vírus ou outros códigos maliciosos. A verificação de vírus do ONTAP, chamada *Vscan*, combina o melhor software antivírus de terceiros com recursos do ONTAP que oferecem a flexibilidade necessária para controlar quais arquivos são verificados e quando.

Os sistemas de storage descarregam as operações de verificação para servidores externos que hospedam softwares antivírus de terceiros. O *ONTAP Antivirus Connector*, fornecido pelo NetApp e instalado no servidor externo, lida com as comunicações entre o sistema de armazenamento e o software antivírus.

- Você pode usar *verificação no acesso* para verificar se há vírus quando os clientes abrem, leem, renomeiam ou fecham arquivos pelo SMB. A operação do arquivo é suspensa até que o servidor externo comunique o status da digitalização do arquivo. Se o ficheiro já tiver sido lido, o ONTAP permite a operação do ficheiro. Caso contrário, ele solicita uma verificação do servidor.

A verificação no acesso não é suportada para NFS.

- Você pode usar *On-demand scanning* para verificar arquivos para vírus imediatamente ou em uma programação. Por exemplo, você pode querer executar digitalizações apenas em horas fora de pico. O servidor externo atualiza o status de verificação dos arquivos verificados, de modo que a latência de

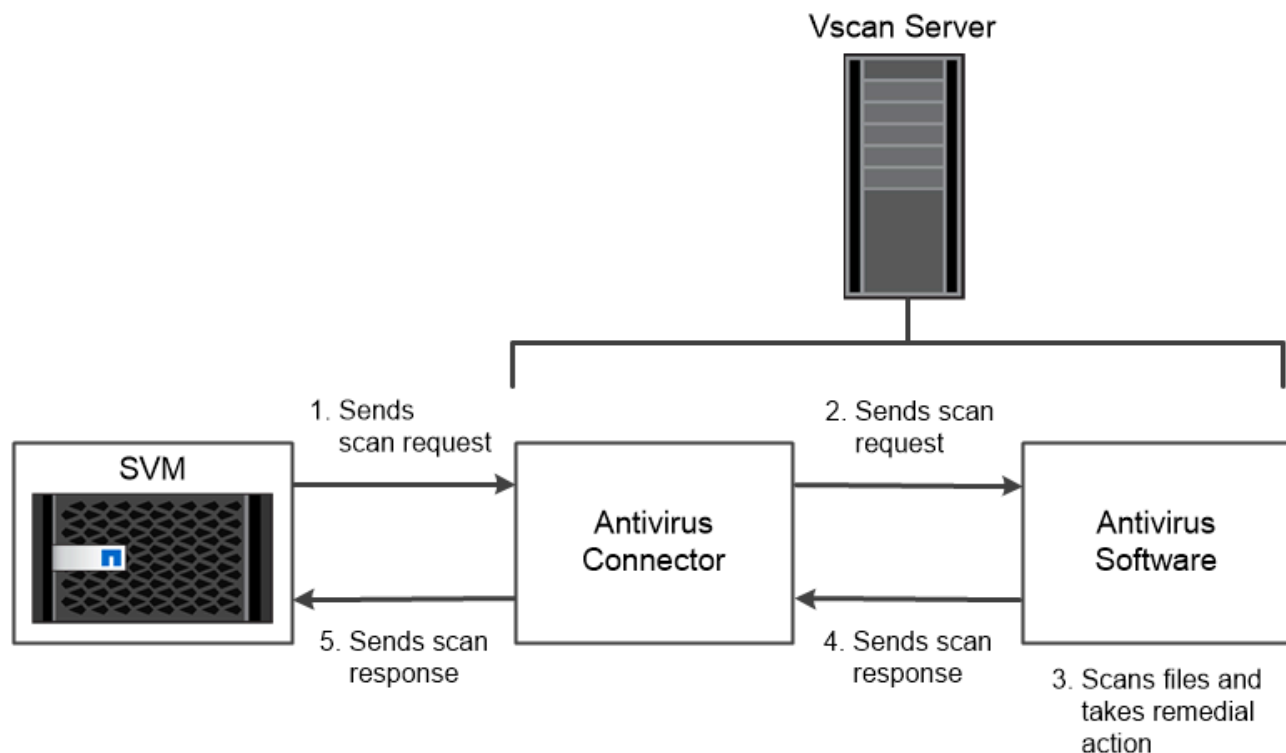
acesso ao arquivo desses arquivos (supondo que eles não tenham sido modificados) seja normalmente reduzida quando forem acessados pela próxima vez por SMB.

Você pode usar a verificação sob demanda para qualquer caminho no namespace SVM, até mesmo para volumes exportados somente por NFS.

Normalmente, você ativa ambos os modos de digitalização em um SVM. Em ambos os modos, o software antivírus toma medidas corretivas em arquivos infectados com base em suas configurações no software.

Verificação de vírus na recuperação de desastres e configurações do MetroCluster

Para a recuperação de desastres e configurações do MetroCluster, é necessário configurar servidores Vscan separados para os clusters locais e parceiros.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Criptografia

A ONTAP oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode usar as seguintes soluções de criptografia:

- Soluções de hardware:
 - Criptografia de storage do NetApp (NSE)

O NSE é uma solução de hardware que usa unidades de autcriptografia (SEDs).

- SEDs NVMe

O ONTAP fornece criptografia completa de disco para SEDs NVMe que não têm a certificação FIPS 140-2-2.

- Soluções de software:

- Criptografia de agregados NetApp (NAE)

NAE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele é habilitado com chaves exclusivas para cada agregado.

- Criptografia de volume NetApp (NVE)

O NVE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade em que ele esteja habilitado com uma chave exclusiva para cada volume.

Use as soluções de criptografia de software (NAE ou NVE) e hardware (NSE ou NVMe SED) para obter criptografia dupla em repouso. A eficiência de storage não é afetada pela criptografia NVE ou NAE.

Criptografia de storage do NetApp

O NetApp Storage Encryption (NSE) é compatível com SEDs que criptografam dados à medida que são gravados. Os dados não podem ser lidos sem uma chave de criptografia armazenada no disco. A chave de criptografia, por sua vez, é acessível apenas para um nó autenticado.

Em uma solicitação de e/S, um nó se autentica em uma SED usando uma chave de autenticação recuperada de um servidor de gerenciamento de chaves externo ou Gerenciador de chaves integrado:

- O servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que fornece chaves de autenticação para nós que usam o Key Management Interoperability Protocol (KMIP).
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados.

O NSE é compatível com HDDs e SSDs com autcriptografia. Você pode usar a criptografia de volume NetApp com NSE para criptografar dados duas vezes em unidades NSE.



Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Unidades com autcriptografia NVMe

No entanto, esses discos usam a criptografia de disco transparente AES de 256 bits para proteger os dados em repouso 140-2.

As operações de criptografia de dados, como a geração de uma chave de autenticação, são realizadas internamente. A chave de autenticação é gerada na primeira vez que o disco é acessado pelo sistema de armazenamento. Depois disso, os discos protegem os dados em repouso exigindo autenticação do sistema de storage sempre que as operações de dados forem solicitadas.

Criptografia de agregados NetApp

O NetApp Aggregate Encryption (NAE) é uma tecnologia baseada em software para criptografar todos os dados em um agregado. Um benefício do NAE é que os volumes estão incluídos na deduplicação de nível agregado, enquanto os volumes NVE são excluídos.

Com o NAE ativado, os volumes dentro do agregado podem ser criptografados com chaves agregadas.

A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você tem o ["Licença NVE"](#) e gerenciamento de chaves externas ou integradas.

Criptografia de volume do NetApp

O NetApp volume Encryption (NVE) é uma tecnologia baseada em software para criptografar dados em repouso, um volume de cada vez. Uma chave de criptografia acessível apenas para o sistema de armazenamento garante que os dados de volume não possam ser lidos se o dispositivo subjacente for separado do sistema.

Os dados, incluindo cópias Snapshot, e metadados, são criptografados. O acesso aos dados é dado por uma chave exclusiva XTS-AES-256, uma por volume. Um Gerenciador de chaves integrado protege as chaves no mesmo sistema com seus dados.

Você pode usar o NVE em qualquer tipo de agregado (HDD, SSD, híbrido, LUN de array), com qualquer tipo de RAID e em qualquer implementação de ONTAP com suporte, incluindo ONTAP Select. Você também pode usar o NVE com criptografia de storage NetApp (NSE) para criptografar dados duas vezes em unidades NSE.

quando usar servidores KMIP embora seja menos caro e normalmente mais conveniente usar o Gerenciador de chaves integrado, você deve configurar servidores KMIP se qualquer uma das seguintes situações for verdadeira:

- Sua solução de gerenciamento de chaves de criptografia precisa estar em conformidade com Federal Information Processing Standards (FIPS) 140-2 ou com o padrão OASIS KMIP.
- Você precisa de uma solução de vários clusters. Os servidores KMIP são compatíveis com vários clusters com gerenciamento centralizado de chaves de criptografia.

Os servidores KMIP são compatíveis com vários clusters com gerenciamento centralizado de chaves de criptografia.

- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

Os servidores KMIP armazenam as chaves de autenticação separadamente dos dados.

Informações relacionadas

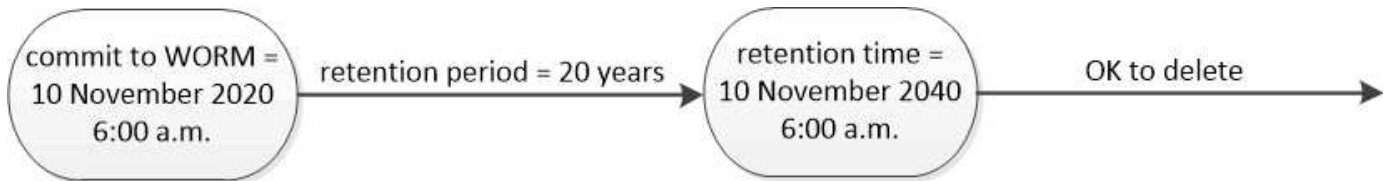
["Perguntas frequentes - encriptação de volume NetApp e encriptação agregada NetApp"](#)

STORAGE WORM

O *SnapLock* é uma solução de conformidade de alto desempenho para organizações que usam o armazenamento *write once, read many (WORM)* para reter arquivos críticos de forma não modificada para fins regulatórios e de governança.

Uma única licença permite que você use o SnapLock no estrito modo *Compliance*, para satisfazer mandatos externos, como a regra SEC 17a-4(f), e um modo *Enterprise mais solto*, para atender aos regulamentos internos exigidos para a proteção de ativos digitais. O SnapLock usa um *ComplianceClock* à prova de violação para determinar quando o período de retenção de um arquivo WORM tiver decorrido.

Use o *SnapLock for SnapVault* para proteger cópias Snapshot WORM no storage secundário. Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres e outros fins.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAP e VMware vSphere

Você pode integrar o ONTAP e os produtos relacionados do NetApp com o VMware vSphere. Existem várias opções disponíveis, dependendo do ambiente de tecnologia e das necessidades do seu negócio.

Conceitos e terminologia selecionados

À medida que você começa a explorar o uso do ONTAP e de produtos NetApp relacionados em um ambiente VMware, é útil primeiro conhecer alguns dos principais conceitos e terminologia.

Número de unidade lógica

Um LUN é um número usado para identificar uma *unidade lógica* dentro de uma SAN (Storage Area Network). Esses dispositivos endereçáveis são normalmente discos lógicos acessados através do protocolo SCSI (Small Computer System Interface) ou de um de seus derivados encapsulados.

Volume virtual do VMware vSphere

Um volume virtual (vVol) fornece uma abstração em nível de volume para o storage usado por uma máquina virtual. Ele inclui vários benefícios e fornece uma alternativa ao uso de um LUN tradicional.

Reservas persistentes

As reservas persistentes são suportadas com SCSI-3 e uma melhoria em relação às reservas SCSI-2 anteriores. Eles permitem que vários iniciadores de cliente se comuniquem com um único destino enquanto bloqueiam outros nós. As reservas podem persistir mesmo que o barramento seja redefinido para recuperação de erros.



A partir do ONTAP 9.15,1, você pode criar uma reserva persistente para um volume virtual usando SCSI-3. Esse recurso só é compatível com o uso das Ferramentas do ONTAP para VMware vSphere 9 com um cluster de failover de servidor do Windows (WSFC).

Cluster de failover do Windows Server

O Microsoft WSFC é um recurso do sistema operacional Windows Server que fornece tolerância a falhas e

alta disponibilidade. Um conjunto de nós de servidor (físicos ou virtuais) é Unido como um cluster para fornecer resiliência em caso de falha. O WSFC é comumente usado para implantar serviços de infraestrutura, incluindo servidores de banco de dados, arquivos e namespaces.

VMware vSphere Storage APIs - Storage Awareness

O VASA é um conjunto de APIs que fornecem integração dos storage arrays com o vCenter para gerenciamento e administração. A arquitetura é baseada em vários componentes, incluindo o *VASA Provider*, que lida com a comunicação entre o VMware vSphere e os sistemas de armazenamento. Com o ONTAP, o provedor é implementado como parte das ferramentas do ONTAP para o VMware vSphere.

VMware vSphere Storage APIs - Array Integration

O VAAI é um conjunto de APIs que permitem a comunicação entre os hosts do VMware vSphere ESXi e os dispositivos de armazenamento. A API inclui um conjunto de operações primitivas usadas pelos hosts para descarregar operações de storage para o array. O VAAI pode fornecer melhorias significativas de desempenho para tarefas com uso intenso de storage.

NetApp SnapCenter

O SnapCenter é uma plataforma centralizada e dimensionável que fornece proteção de dados para aplicações, bancos de dados, sistemas de arquivos host e máquinas virtuais que usam sistemas de storage ONTAP. Ele utiliza as tecnologias nativas da ONTAP, incluindo Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault.

Plug-ins do NetApp e tecnologias relacionadas

O NetApp fornece suporte robusto para a integração do ONTAP e produtos relacionados com as tecnologias VMware vSphere.

Ferramentas do ONTAP para VMware vSphere

As ferramentas do ONTAP para VMware vSphere são um conjunto de ferramentas para integrar o ONTAP e o vSphere. Ele implementa a funcionalidade do provedor da estrutura da API VASA. As ferramentas do ONTAP também incluem o plug-in do vCenter, um adaptador de replicação de storage (SRA) para o VMware Site Recovery Manager e um servidor de API REST que você pode usar para criar aplicativos de automação.

Plug-in NFS para VMware VAAI

O plug-in NFS do NetApp para VMware VAAI fornece acesso aos recursos do VAAI. O plug-in pode ser instalado em hosts ESXi e permite que os hosts aproveitem o VAAI com os datastores NFS no ONTAP. Ele fornece várias operações, incluindo clonagem, reservas de espaço e descarregamento de snapshot.

VMware Site Recovery Manager

O VMware Site Recovery Manager (SRM) fornece uma capacidade de recuperação de desastres. O SRM se integra às ferramentas do ONTAP para o VMware vSphere acessar e aproveitar a funcionalidade de gerenciamento de dados do ONTAP.

Cluster de armazenamento vSphere Metro

O vSphere Metro Storage Cluster (vmsc) é uma tecnologia que permite e suporta o vSphere em uma implantação de cluster *estendido*. As soluções vmsc são compatíveis com o NetApp MetroCluster e o SnapMirror ativo Sync (anteriormente SMBC). Essas soluções fornecem continuidade de negócios aprimorada em caso de falha de domínio. O modelo de resiliência é baseado em suas escolhas de configuração específicas.

Plug-in do SnapCenter para VMware vSphere

O plug-in do SnapCenter para VMware vSphere (SCV) é um dispositivo virtual baseado em Linux que você pode implantar em conjunto com o servidor SnapCenter ou como um aplicativo autônomo. Em ambos os casos, o SCV fornece operações de backup e restauração de VMs, armazenamentos de dados e VMDKs. As operações são rápidas, com uso eficiente de espaço, consistentes com falhas e consistentes com VM.

Obtenha mais informações

Há vários recursos adicionais disponíveis para ajudá-lo a se preparar para implantar o ONTAP em um ambiente VMware vSphere.

- ["Ferramentas do ONTAP para documentação do VMware vSphere"](#)
- ["Aplicações empresariais: VMware vSphere com ONTAP"](#)
- ["NetApp KB: O que são Reservas SCSI e Reservas persistentes SCSI?"](#)
- ["Plug-in do SnapCenter para documentação do VMware vSphere"](#)

Gerenciamento de dados com reconhecimento de aplicações

O gerenciamento de dados com reconhecimento de aplicações permite descrever o aplicativo que você deseja implantar no ONTAP em termos de aplicativo, em vez de em termos de storage. O aplicativo pode ser configurado e pronto para servir dados rapidamente com o mínimo de entradas usando o System Manager e as APIs REST.

O recurso de gerenciamento de dados com reconhecimento de aplicações fornece uma maneira de configurar, gerenciar e monitorar o storage no nível de aplicativos individuais. Esse recurso incorpora práticas recomendadas relevantes da ONTAP para provisionar aplicações de forma otimizada, com posicionamento equilibrado de objetos de storage com base nos níveis de serviço de performance desejados e nos recursos do sistema disponíveis.

O recurso de gerenciamento de dados com reconhecimento de aplicativo inclui um conjunto de modelos de aplicativo, com cada modelo composto por um conjunto de parâmetros que descrevem coletivamente a configuração de um aplicativo. Esses parâmetros, que geralmente são predefinidos com valores padrão, definem as características que um administrador de aplicativos poderia especificar para provisionar armazenamento em um sistema ONTAP, como tamanhos de banco de dados, níveis de serviço, elementos de acesso de protocolo, como LIFs, bem como critérios de proteção locais e critérios de proteção remota. Com base nos parâmetros especificados, o ONTAP configura entidades de storage, como LUNs e volumes, com tamanhos e níveis de serviço apropriados para a aplicação.

Você pode executar as seguintes tarefas para seus aplicativos:

- Crie aplicativos usando os modelos de aplicativo
- Gerenciar o armazenamento associado aos aplicativos
- Modificar ou eliminar as aplicações
- Ver aplicações
- Gerenciar cópias Snapshot das aplicações
- Crie [grupos de consistência](#) para fornecer funcionalidades de proteção de dados selecionando vários LUNs nos mesmos volumes ou em volumes diferentes

FabricPool

Muitos clientes da NetApp têm quantidades significativas de dados armazenados que raramente são acessados. Chamamos isso de *cold* dados. Os clientes também têm dados que são acessados com frequência, que chamamos de *hot* data. Idealmente, você deseja manter seus dados ativos em seu storage mais rápido para obter a melhor performance. Os dados inativos podem se mover para um armazenamento mais lento, desde que estejam imediatamente disponíveis, se necessário. Mas como você sabe quais partes de seus dados estão quentes e quais são frios?

O FabricPool é um recurso do ONTAP que move dados automaticamente entre uma camada local (agregado) de alta performance e uma camada de nuvem com base em padrões de acesso. A disposição em categorias libera espaço no storage local caro para os dados ativos enquanto mantém os dados inativos prontamente disponíveis no storage de objetos de baixo custo na nuvem. O FabricPool monitora constantemente o acesso aos dados e migra os dados entre as camadas para melhor performance e máxima economia.

Usar o FabricPool para categorizar dados pouco acessados na nuvem é uma das maneiras mais fáceis de ganhar eficiência e criar uma configuração de nuvem híbrida. O FabricPool trabalha em nível de bloco de storage, portanto, trabalha com dados LUN e de arquivo.

No entanto, o FabricPool não se destina apenas a separar os dados on-premises para a nuvem. Muitos clientes usam o FabricPool em Cloud Volumes ONTAP para categorizar dados inativos de storage de nuvem mais caro para storage de objetos de baixo custo dentro do fornecedor de nuvem. A partir do ONTAP 9.8, é possível capturar análises em volumes habilitados para FabricPool com ["Análise do sistema de arquivos"](#) ou ["eficiência de storage sensível à temperatura"](#).

As aplicações que usam os dados não sabem que eles estão dispostos em categorias, portanto, não são necessárias alterações nas aplicações. A disposição em camadas é totalmente automática, portanto, não é necessária administração contínua.

Você pode armazenar dados inativos no storage de objetos de um dos principais fornecedores de nuvem. Ou escolha a NetApp StorageGRID para manter seus dados inativos na sua própria nuvem privada, proporcionando a melhor performance e controle total sobre seus dados.

Informações relacionadas

["Doc do Gestor de sistema FabricPool"](#)

["Disposição em camadas do BlueXP"](#)

["Lista de reprodução do FabricPool na NetApp TechComm TV"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.