



Aprenda

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

- Aprenda 1
 - Saiba mais sobre o Cloud Volumes ONTAP 1
 - Armazenamento 2
 - Pares de alta disponibilidade 12
 - A avaliar 21
 - Licenciamento 22
 - Segurança 23
 - Desempenho 26
 - Configuração padrão para Cloud Volumes ONTAP 26

Aprenda

Saiba mais sobre o Cloud Volumes ONTAP

Com o Cloud Volumes ONTAP, você otimiza seus custos e performance de storage de nuvem, além de aprimorar a proteção, a segurança e a conformidade dos dados.

O Cloud Volumes ONTAP é um dispositivo de storage somente de software que executa o software de gerenciamento de dados ONTAP na nuvem. Ele fornece storage de nível empresarial com os seguintes principais recursos:

- Eficiência de storage

Utilize deduplicação de dados incorporada, compressão, thin Provisioning e clonagem para minimizar os custos de storage.

- Alta disponibilidade

Garanta a confiabilidade empresarial e as operações contínuas em caso de falhas em seu ambiente de nuvem.

- Proteção de dados

A Cloud Volumes ONTAP utiliza o SnapMirror, a tecnologia de replicação líder do setor da NetApp para replicar dados no local para a nuvem de modo que seja fácil ter cópias secundárias disponíveis para vários casos de uso.

O Cloud Volumes ONTAP também se integra ao Cloud Backup Service para fornecer recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de nuvem.

- Categorização de dados

Alterne entre pools de armazenamento de alto e baixo desempenho sob demanda sem colocar os aplicativos offline.

- Consistência de aplicativos

Garanta a consistência das cópias Snapshot do NetApp usando o NetApp SnapCenter.

- Segurança dos dados

O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.

- Controles de conformidade de privacidade

A integração com o Cloud Compliance ajuda você a entender o contexto dos dados e identificar dados confidenciais.



As licenças para os recursos do ONTAP estão incluídas no Cloud Volumes ONTAP.

["Veja as configurações do Cloud Volumes ONTAP compatíveis"](#)

Armazenamento

Discos e agregados

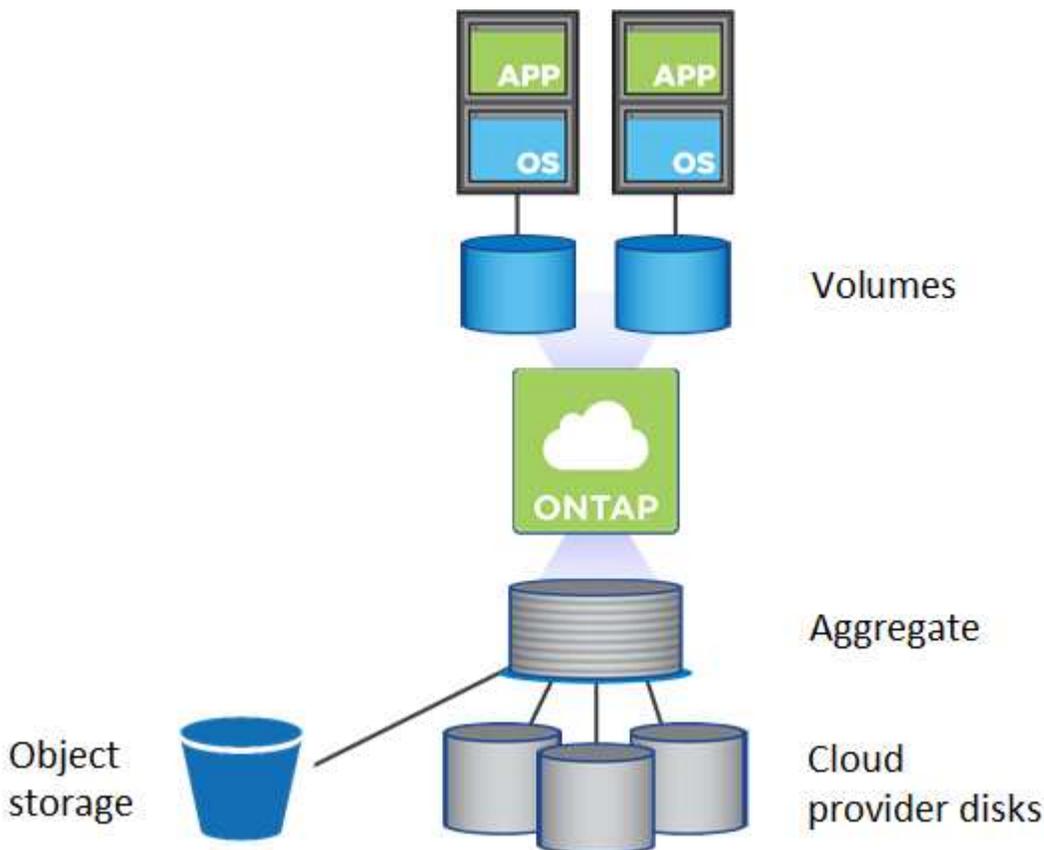
Entender como o Cloud Volumes ONTAP usa o storage de nuvem pode ajudar você a entender seus custos de storage.



Todos os discos e agregados devem ser criados e excluídos diretamente do Cloud Manager. Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Visão geral

A Cloud Volumes ONTAP usa o storage de fornecedor de nuvem como discos e os agrupa em uma ou mais agregados. Agregados fornecem storage para um ou mais volumes.



Vários tipos de discos de nuvem são suportados. Você escolhe o tipo de disco ao criar um volume e o tamanho de disco padrão ao implantar o Cloud Volumes ONTAP.



A quantidade total de storage comprada de um fornecedor de nuvem é a *capacidade bruta*. A *capacidade utilizável* é menor porque aproximadamente 12 a 14% é sobrecarga reservada para uso Cloud Volumes ONTAP. Por exemplo, se o Cloud Manager criar um agregado de 500 GB, a capacidade utilizável será de 442,94 GB.

Storage da AWS

Na AWS, o Cloud Volumes ONTAP usa o armazenamento EBS para dados de usuário e armazenamento NVMe local como Flash Cache em alguns tipos de instâncias do EC2.

Armazenamento EBS

Na AWS, um agregado pode conter até 6 discos com o mesmo tamanho. O tamanho máximo do disco é de 16 TB.

O tipo de disco EBS subjacente pode ser SSD de uso geral, SSD IOPS provisionado, HDD otimizado para taxa de transferência ou HDD frio. Você pode emparelhar um disco EBS com o Amazon S3 para "[categorize os dados inativos em storage de objetos de baixo custo](#)".

A um nível elevado, as diferenças entre os tipos de discos EBS são as seguintes:

- *Discos SSD* de uso geral equilibram custo e desempenho para uma ampla variedade de cargas de trabalho. A performance é definida em termos de IOPS.
- Os discos SSD *_IOPS* provisionados são para aplicativos críticos que exigem o mais alto desempenho a um custo mais alto.
- *Discos HDD* otimizados para taxa de transferência são para cargas de trabalho acessadas com frequência que exigem taxa de transferência rápida e consistente a um preço menor.
- *Cold HDD* discos são destinados a backups, ou dados acessados com pouca frequência, porque o desempenho é muito baixo. Assim como os discos HDD otimizados para taxa de transferência, o desempenho é definido em termos de taxa de transferência.



Discos rígidos inativos não são compatíveis com configurações de HA e com categorização de dados.

Storage NVMe local

Alguns tipos de instâncias do EC2 incluem storage NVMe local, que o Cloud Volumes ONTAP usa como "[Flash Cache](#)".

- [Ligações relacionadas*](#)
- ["Documentação da AWS: Tipos de volume do EBS"](#)
- ["Saiba como escolher tipos de disco e tamanhos de disco para seus sistemas na AWS"](#)
- ["Analisar os limites de armazenamento do Cloud Volumes ONTAP na AWS"](#)
- ["Revise as configurações compatíveis do Cloud Volumes ONTAP na AWS"](#)

Storage Azure

No Azure, um agregado pode conter até 12 discos com o mesmo tamanho. O tipo de disco e o tamanho máximo do disco dependem se você usa um sistema de nó único ou um par de HA:

Sistemas de nó único

Sistemas de nó único podem usar três tipos de discos gerenciados do Azure:

- *Discos gerenciados SSD premium* fornecem alto desempenho para cargas de trabalho com uso intenso de e/S a um custo mais alto.
- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.

- *Discos gerenciados HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

Cada tipo de disco gerenciado tem um tamanho máximo de disco de 32 TB.

É possível emparelhar um disco gerenciado com o storage Azure Blob ao ["categorize os dados inativos em storage de objetos de baixo custo"](#).

Pares HA

Os pares HA usam blobs de página Premium, que têm um tamanho máximo de disco de 8 TB.

- [Ligações relacionadas*](#)
- ["Documentação do Microsoft Azure: Introdução ao Microsoft Azure Storage"](#)
- ["Saiba como escolher tipos de disco e tamanhos de disco para seus sistemas no Azure"](#)
- ["Analisar os limites de armazenamento do Cloud Volumes ONTAP no Azure"](#)

Armazenamento do GCP

Na GCP, um agregado pode conter até 6 discos com o mesmo tamanho. O tamanho máximo do disco é de 16 TB.

O tipo de disco pode ser *Zonal SSD Persistent Disks* ou *Zonal Standard Persistent Disks*. É possível emparelhar discos persistentes com um bucket do Google Storage ao ["categorize os dados inativos em storage de objetos de baixo custo"](#).

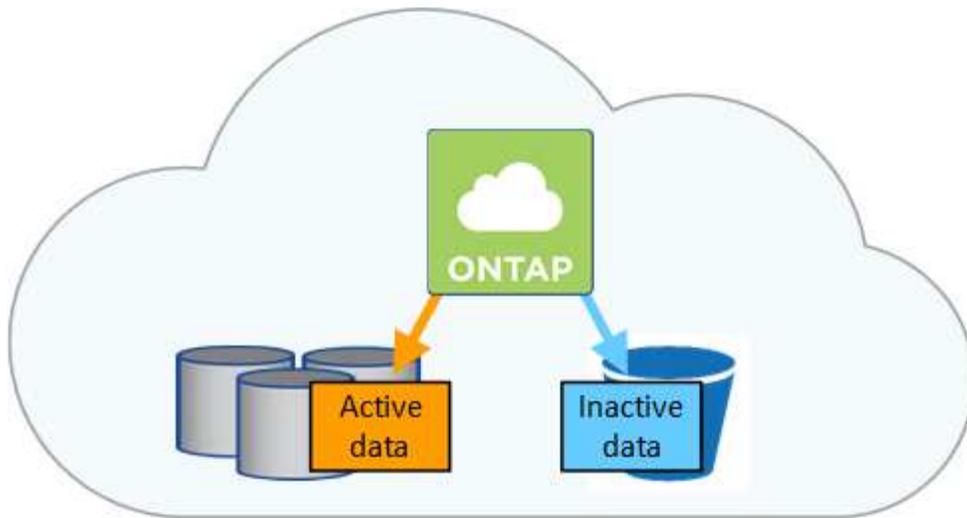
- [Ligações relacionadas*](#)
- ["Documentação do Google Cloud Platform: Opções de armazenamento"](#)
- ["Analisar os limites de armazenamento do Cloud Volumes ONTAP na GCP"](#)

Tipo de RAID

O tipo RAID para cada agregado Cloud Volumes ONTAP é RAID0 (striping). Nenhum outro tipo de RAID é suportado. A Cloud Volumes ONTAP conta com o fornecedor de nuvem para disponibilidade e durabilidade de disco.

Visão geral de categorização de dados

Reduza seus custos de storage habilitando a disposição automatizada de dados inativos em storage de objetos de baixo custo. Os dados ativos permanecem em SSDs ou HDDs de alta performance, enquanto os dados inativos são dispostos em camadas em storage de objetos de baixo custo. Isso permite recuperar espaço no storage primário e reduzir o storage secundário.



O Cloud Volumes ONTAP é compatível com categorização de dados na AWS, Azure e Google Cloud Platform. A disposição de dados em categorias é baseada na tecnologia FabricPool.



Não é necessário instalar uma licença de recurso para habilitar a disposição de dados em camadas (FabricPool).

Categorização de dados no AWS

Ao habilitar a disposição de dados em categorias na AWS, o Cloud Volumes ONTAP usa o EBS como uma camada de desempenho para dados ativos e o AWS S3 como uma camada de capacidade para dados inativos.

Camada de performance

A categoria de performance pode ser SSDs de uso geral, SSDs IOPS provisionados ou HDDs otimizados para taxa de transferência.

Camada de capacidade

Um sistema Cloud Volumes ONTAP classifica dados inativos em um único bucket do S3 usando a classe de armazenamento *Standard*. O padrão é ideal para dados acessados com frequência armazenados em várias zonas de disponibilidade.



O Cloud Manager cria um único bucket do S3 para cada ambiente de trabalho e o nomeia *Fabric-pool-cluster unique identifier*. Não é criado um bucket S3 diferente para cada volume.

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas na AWS é *Standard*. Se você não planeja acessar os dados inativos, você pode reduzir seus custos de armazenamento alterando a classe de armazenamento para um dos seguintes: *Intelligent Tiering*, *One-Zone unless Access*, ou *Standard-Unfrequent Access*. Quando você altera a classe de armazenamento, os dados inativos começam na classe de armazenamento padrão e passam para a classe de armazenamento selecionada, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de storage. ["Saiba mais sobre as classes de armazenamento do Amazon S3"](#).

Você pode selecionar uma classe de armazenamento ao criar o ambiente de trabalho e pode alterá-la a qualquer momento. Para obter detalhes sobre como alterar a classe de armazenamento, ["Disposição em](#)

[camadas dos dados inativos em storage de objetos de baixo custo](#) consulte .

A classe de storage para disposição de dados em categorias é de todo o sistema, não é por volume.

Categorização de dados no Azure

Ao habilitar a categorização de dados no Azure, o Cloud Volumes ONTAP usa discos gerenciados do Azure como uma categoria de performance para dados ativos e o storage Blob do Azure como uma categoria de capacidade para dados inativos.

Camada de performance

A camada de performance pode ser SSDs ou HDDs.

Camada de capacidade

Um sistema Cloud Volumes ONTAP categoriza dados inativos em um único contêiner de Blob usando a camada de storage *hot* do Azure. O hot Tier é ideal para dados acessados com frequência.



O Cloud Manager cria uma nova conta de storage com um único contêiner para cada ambiente de trabalho do Cloud Volumes ONTAP. O nome da conta de armazenamento é aleatório. Não é criado um recipiente diferente para cada volume.

Camadas de acesso ao storage

A camada de acesso de storage padrão para dados em camadas no Azure é o nível *hot*. Se você não planeja acessar os dados inativos, pode reduzir seus custos de storage mudando para a camada de storage *COOL*. Quando você altera a camada de storage, os dados inativos começam na camada de storage quente e passam para a camada de storage frio, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a camada de storage. ["Saiba mais sobre as camadas de acesso ao armazenamento Azure Blob"](#).

Você pode selecionar uma camada de storage ao criar o ambiente de trabalho e alterá-la a qualquer momento. Para obter detalhes sobre como alterar a camada de storage, ["Disposição em camadas dos dados inativos em storage de objetos de baixo custo"](#) consulte .

A camada de acesso a storage para categorização de dados é de todo o sistema, não é por volume.

Categorização de dados no GCP

Ao habilitar a categorização de dados no GCP, o Cloud Volumes ONTAP usa discos persistentes como uma categoria de performance para dados ativos e um bucket do Google Cloud Storage como uma categoria de capacidade para dados inativos.

Camada de performance

A camada de performance pode ser SSDs ou HDDs (discos padrão).

Camada de capacidade

Um sistema Cloud Volumes ONTAP classifica os dados inativos em um único bucket do Google Cloud Storage usando a classe de storage *Regional*.



O Cloud Manager cria um único bucket para cada ambiente de trabalho e o nomeia *Fabric-pool-cluster unique identifier*. Não é criado um intervalo diferente para cada volume.

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas é a classe *Standard Storage*. Se os dados forem acessados com pouca frequência, você poderá reduzir seus custos de armazenamento alterando para *Nearline Storage* ou *Coldline Storage*. Quando você altera a classe de armazenamento, os dados inativos começam na classe armazenamento padrão e passam para a classe de armazenamento selecionada, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de storage. ["Saiba mais sobre as classes de armazenamento para o Google Cloud Storage"](#).

Você pode selecionar uma camada de storage ao criar o ambiente de trabalho e alterá-la a qualquer momento. Para obter detalhes sobre como alterar a classe de armazenamento, ["Disposição em camadas dos dados inativos em storage de objetos de baixo custo"](#) consulte .

A classe de storage para disposição de dados em categorias é de todo o sistema, não é por volume.

Disposição de dados em categorias e limites de capacidade

Se você habilitar a disposição de dados em categorias, o limite de capacidade de um sistema permanecerá o mesmo. O limite se estende pela camada de performance e pela camada de capacidade.

Políticas de disposição em camadas de volume

Para habilitar a disposição de dados em categorias, você deve selecionar uma política de disposição em categorias de volume ao criar, modificar ou replicar um volume. Pode selecionar uma política diferente para cada volume.

Algumas políticas de disposição em categorias têm um período de resfriamento mínimo associado, que define o tempo em que os dados do usuário em um volume precisam permanecer inativos para que os dados sejam considerados "frios" e movidos para o nível de capacidade.

O Cloud Manager permite que você escolha uma das seguintes políticas de disposição em categorias de volume ao criar ou modificar um volume:

Apenas Snapshot

Depois que um agregado atinge a capacidade de 50%, o Cloud Volumes ONTAP classifica os dados inativos dos usuários das cópias Snapshot que não estão associados ao sistema de arquivos ativo à categoria de capacidade. O período de resfriamento é de aproximadamente 2 dias.

Se forem lidos, os blocos de dados inativos na camada de capacidade aquecem e são movidos para a categoria de performance.

Tudo

Todos os dados (não incluindo metadados) são imediatamente marcados como frios e dispostos em camadas no storage de objetos o mais rápido possível. Não há necessidade de esperar 48 horas para que novos blocos em um volume fiquem frios. Observe que os blocos localizados no volume antes da política tudo ser definida exigem 48 horas para ficarem frios.

Se lidos, os blocos de dados inativos na categoria de nuvem não são gravados de volta na categoria de performance. Esta política está disponível a partir do ONTAP 9.6.

Auto

Depois que um agregado atinge a capacidade de 50%, o Cloud Volumes ONTAP dispõe de blocos de dados inativos em um volume para uma categoria de capacidade. Os dados inativos incluem não apenas cópias Snapshot, mas também dados de usuários inativos do sistema de arquivos ativo. O período de resfriamento é de aproximadamente 31 dias.

Esta política é suportada a partir do Cloud Volumes ONTAP 9,4.

Se forem lidos por leituras aleatórias, os blocos de dados inativos na camada de capacidade aquecem e migram para a camada de performance. Se forem lidos por leituras sequenciais, como as associadas a verificações de índice e antivírus, os blocos de dados inativos permanecem inativos e não se movem para o nível de desempenho.

Nenhum

Mantém os dados de um volume na categoria de performance, impedindo que ele seja migrado para a categoria de capacidade.

Ao replicar um volume, você pode escolher se deseja categorizar os dados em storage de objetos. Se o fizer, o Cloud Manager aplica a política **Backup** ao volume de proteção de dados. A partir do Cloud Volumes ONTAP 9,6, a política de disposição em camadas **All** substitui a política de backup.

A desativação do Cloud Volumes ONTAP afeta o período de resfriamento

Os blocos de dados são resfriados por exames de resfriamento. Durante este processo, os blocos que não foram usados têm a temperatura do bloco movida (resfriada) para o próximo valor mais baixo. O tempo de resfriamento padrão depende da política de disposição em categorias de volume:

- Auto: 31 dias
- Somente snapshot: 2 dias

O Cloud Volumes ONTAP deve estar em execução para que o exame de arrefecimento funcione. Se o Cloud Volumes ONTAP estiver desligado, o resfriamento também parará. Como resultado, você pode experimentar tempos de resfriamento mais longos.

Configuração de categorização de dados

Para obter instruções e uma lista de configurações suportadas, "[Disposição em camadas dos dados inativos em storage de objetos de baixo custo](#)" consulte .

Gerenciamento de storage

O Cloud Manager oferece gerenciamento simplificado e avançado do storage Cloud Volumes ONTAP.



Todos os discos e agregados devem ser criados e excluídos diretamente do Cloud Manager. Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Provisionamento de storage

O Cloud Manager facilita o provisionamento de storage para Cloud Volumes ONTAP comprando discos e gerenciando agregados para você. Você simplesmente precisa criar volumes. Você pode usar uma opção

avançada de alocação para provisionar agregados, se desejar.

Provisionamento simplificado

Agregados fornecem storage de nuvem para volumes. O Cloud Manager cria agregados para você ao iniciar uma instância e ao provisionar volumes adicionais.

Quando você cria um volume, o Cloud Manager faz uma de três coisas:

- Ele coloca o volume em um agregado existente que tem espaço livre suficiente.
- Ele coloca o volume em um agregado existente comprando mais discos para esse agregado.
- Ele compra discos para um novo agregado e coloca o volume nesse agregado.

O Cloud Manager determina onde colocar um novo volume analisando vários fatores: O tamanho máximo de um agregado, se o thin Provisioning está habilitado e os limites de espaço livre para agregados.



O administrador da conta pode modificar limites de espaço livre a partir da página **Configurações**.

Seleção de tamanho de disco para agregados na AWS

Quando o Cloud Manager cria novos agregados para o Cloud Volumes ONTAP na AWS, ele aumenta gradualmente o tamanho do disco em um agregado, à medida que o número de agregados no sistema aumenta. O Cloud Manager faz isso para garantir que você possa utilizar a capacidade máxima do sistema antes de atingir o número máximo de discos de dados permitidos pela AWS.

Por exemplo, o Cloud Manager pode escolher os seguintes tamanhos de disco para agregados em um sistema Cloud Volumes ONTAP Premium ou BYOL:

Número agregado	Tamanho do disco	Capacidade de agregado máxima
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

Você pode escolher o tamanho do disco usando a opção de alocação avançada.

Alocação avançada

Em vez de permitir que o Cloud Manager gerencie agregados para você, você pode fazê-lo sozinho. ["Na página Alocação avançada"](#), você pode criar novos agregados que incluem um número específico de discos, adicionar discos a um agregado existente e criar volumes em agregados específicos.

Gerenciamento de capacidade

O administrador da conta pode escolher se o Cloud Manager notifica você sobre decisões de capacidade de storage ou se o Cloud Manager gerencia automaticamente os requisitos de capacidade para você. Pode ajudar você a entender como esses modos funcionam.

Gerenciamento automático de capacidade

Por padrão, o modo de gerenciamento de capacidade é definido como automático. Nesse modo, o Cloud

Manager compra automaticamente novos discos para instâncias do Cloud Volumes ONTAP quando é necessária mais capacidade, exclui coleções não usadas de discos (agregados), move volumes entre agregados quando necessário e tenta desfazer discos.

Os exemplos a seguir ilustram como esse modo funciona:

- Se um agregado com 5 ou menos discos EBS atingir o limite de capacidade, o Cloud Manager comprará automaticamente novos discos para esse agregado para que os volumes possam continuar a crescer.
- Se um agregado com 12 discos Azure atingir o limite de capacidade, o Cloud Manager moverá automaticamente um volume desse agregado para um agregado com capacidade disponível ou para um novo agregado.

Se o Cloud Manager criar um novo agregado para o volume, ele escolherá um tamanho de disco que acomoda o tamanho desse volume.

Note que o espaço livre está agora disponível no agregado original. Volumes existentes ou novos volumes podem usar esse espaço. O espaço não pode ser retornado à AWS, ao Azure ou ao GCP nesse cenário.

- Se um agregado não contiver volumes por mais de 12 horas, o Cloud Manager o excluirá.

Gerenciamento de LUNs com gerenciamento automático de capacidade

O gerenciamento automático de capacidade do Cloud Manager não se aplica a LUNs. Quando o Cloud Manager cria um LUN, ele desativa o recurso de crescimento automático.

Gestão de inodes com gestão automática de capacidade

O Cloud Manager monitora o uso de inode em um volume. Quando 85% dos inodes são usados, o Cloud Manager aumenta o tamanho do volume para aumentar o número de inodes disponíveis. O número de arquivos que um volume pode conter é determinado por quantos inodes ele tem.

Gerenciamento manual de capacidade

Se o administrador da conta definir o modo de gerenciamento de capacidade como manual, o Cloud Manager exibirá as mensagens Ação necessárias quando as decisões de capacidade devem ser tomadas. Os mesmos exemplos descritos no modo automático aplicam-se ao modo manual, mas cabe a você aceitar as ações.

Flash Cache

Algumas configurações do Cloud Volumes ONTAP na AWS e no Azure incluem o storage NVMe local, que o Cloud Volumes ONTAP usa como *Flash Cache* para melhorar a performance.

O que é Flash Cache?

O Flash Cache acelera o acesso aos dados por meio do armazenamento em cache inteligente em tempo real dos dados do usuário lidos recentemente e dos metadados do NetApp. Ele é eficaz para cargas de trabalho com uso intenso de leitura aleatória, incluindo bancos de dados, e-mail e serviços de arquivos.

Instâncias compatíveis na AWS

Selecione um dos seguintes tipos de instância do EC2 com um sistema Cloud Volumes ONTAP Premium ou BYOL novo ou existente:

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

Tipo de VM compatível no Azure

Selecione o tipo de VM Standard_L8s_v2 com um único sistema Cloud Volumes ONTAP BYOL no Azure.

Limitações

- A compactação deve ser desativada em todos os volumes para aproveitar as melhorias de desempenho do Flash Cache.

Não escolha eficiência de storage ao criar um volume no Cloud Manager ou criar um volume e, em seguida "[Desative a compressão de dados usando a CLI](#)", .

- O reaquecimento do cache após uma reinicialização não é suportado com o Cloud Volumes ONTAP.

STORAGE WORM

Você pode ativar o storage WORM (uma gravação, muitas leituras) em um sistema Cloud Volumes ONTAP para reter arquivos de forma não modificada por um período de retenção especificado. O STORAGE WORM é baseado na tecnologia SnapLock no modo empresarial, o que significa que os arquivos WORM são protegidos no nível do arquivo.

Depois que um arquivo foi comprometido com o storage WORM, ele não poderá ser modificado, mesmo depois que o período de retenção expirou. Um relógio à prova de violação determina quando o período de retenção para um arquivo WORM expirou.

Após o período de retenção ter terminado, você é responsável por excluir quaisquer arquivos que você não precisa mais.

Ativar o storage WORM

Você pode ativar o storage WORM em um sistema Cloud Volumes ONTAP ao criar um novo ambiente de trabalho. Isso inclui especificar um código de ativação e definir o período de retenção padrão para arquivos. Você pode obter um código de ativação usando o ícone de bate-papo no canto inferior direito da interface do Cloud Manager.



Não é possível ativar o storage WORM em volumes individuais—WORM deve ser ativado no nível do sistema.

A imagem a seguir mostra como ativar o storage WORM ao criar um ambiente de trabalho:

WORM | *Preview*

You can use **write once, read many (WORM)** storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level. [Learn More](#)

Disable WORM Activate WORM

Notice: If you enable WORM storage, you cannot enable data tiering to object storage.

WORM Activation Code ?

Worm-1111122222aaaaa

Retention Period

15

years

Armazenando arquivos no WORM

Você pode usar uma aplicação para vincular arquivos ao WORM em NFS ou CIFS, ou usar a CLI da ONTAP para vincular automaticamente arquivos ao WORM. Você também pode usar um arquivo anexado WORM para reter dados gravados de forma incremental, como informações de log.

Depois de ativar o storage WORM em um sistema Cloud Volumes ONTAP, você precisa usar a CLI da ONTAP para todo o gerenciamento de storage WORM. Para obter instruções, "[Documentação do ONTAP](#)" consulte .



O suporte do Cloud Volumes ONTAP para storage WORM é equivalente ao modo SnapLock Enterprise.

Limitações

- Se você excluir ou mover um disco diretamente da AWS ou do Azure, um volume poderá ser excluído antes da data de expiração.
- Quando o storage WORM é ativado, a disposição de dados em categorias para storage de objetos não pode ser habilitada.
- O backup na nuvem deve ser desativado para habilitar o storage WORM.

Pares de alta disponibilidade

Pares de alta disponibilidade na AWS

Uma configuração de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece

operações ininterruptas e tolerância de falhas. Na AWS, os dados são espelhados de forma síncrona entre os dois nós.

Visão geral

Na AWS, as configurações do Cloud Volumes ONTAP HA incluem os seguintes componentes:

- Dois nós de Cloud Volumes ONTAP cujos dados são espelhados de forma síncrona entre si.
- Uma instância de mediador que fornece um canal de comunicação entre os nós para auxiliar nos processos de takeover do storage e giveback.



A instância mediadora executa o sistema operacional Linux em uma instância T2.micro e usa um disco magnético EBS que é de aproximadamente 8 GB.

Takeover de storage e giveback

Se um nó ficar inativo, o outro nó poderá fornecer dados para que seu parceiro forneça serviços de dados contínuos. Os clientes podem acessar os mesmos dados do nó do parceiro porque os dados foram espelhados de forma síncrona para o parceiro.

Depois que o nó for reiniciado, o parceiro deverá sincronizar novamente os dados antes que ele possa retornar o armazenamento. O tempo necessário para sincronizar novamente os dados depende da quantidade de dados alterados enquanto o nó estava inativo.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos. Seus dados são consistentes transacionalmente, sem perda de dados.
- O objetivo de tempo de recuperação (rto) é de 60 segundos. Em caso de interrupção, os dados devem estar disponíveis em 60 segundos ou menos.

Modelos de IMPLANTAÇÃO DE HA

Você pode garantir a alta disponibilidade de seus dados implantando uma configuração de HA em várias zonas de disponibilidade (AZs) ou em uma única AZ. Você deve rever mais detalhes sobre cada configuração para escolher qual melhor se adapta às suas necessidades.

Cloud Volumes ONTAP HA em várias zonas de disponibilidade

A implantação de uma configuração de HA em várias zonas de disponibilidade (AZs) garante alta disponibilidade de seus dados se ocorrer uma falha com uma AZ ou uma instância que execute um nó Cloud Volumes ONTAP. Você deve entender como os endereços IP nas afetam o acesso aos dados e o failover de storage.

Acesso a dados NFS e CIFS

Quando uma configuração de HA é espalhada por várias zonas de disponibilidade, *endereços IP flutuantes* ativa o acesso do cliente nas. Os endereços IP flutuantes, que devem estar fora dos blocos CIDR para todos os VPCs na região, podem migrar entre nós quando ocorrem falhas. Eles não são acessíveis nativamente para clientes que estão fora da VPC, a menos que você "[Configure um gateway de trânsito da AWS](#)".

Se não for possível configurar um gateway de trânsito, os endereços IP privados estarão disponíveis para clientes nas que estejam fora da VPC. No entanto, esses endereços IP são estáticos – eles não podem fazer failover entre nós.

Você deve analisar os requisitos para endereços IP flutuantes e tabelas de rota antes de implantar uma configuração de HA em várias zonas de disponibilidade. Você deve especificar os endereços IP flutuantes ao implantar a configuração. Os endereços IP privados são criados automaticamente pelo Cloud Manager.

Para obter detalhes, "[Requisitos de rede da AWS para o Cloud Volumes ONTAP HA em vários AZs](#)" consulte .

Acesso a dados iSCSI

A comunicação de dados entre VPC não é um problema, uma vez que o iSCSI não usa endereços IP flutuantes.

Takeover de storage e giveback para iSCSI

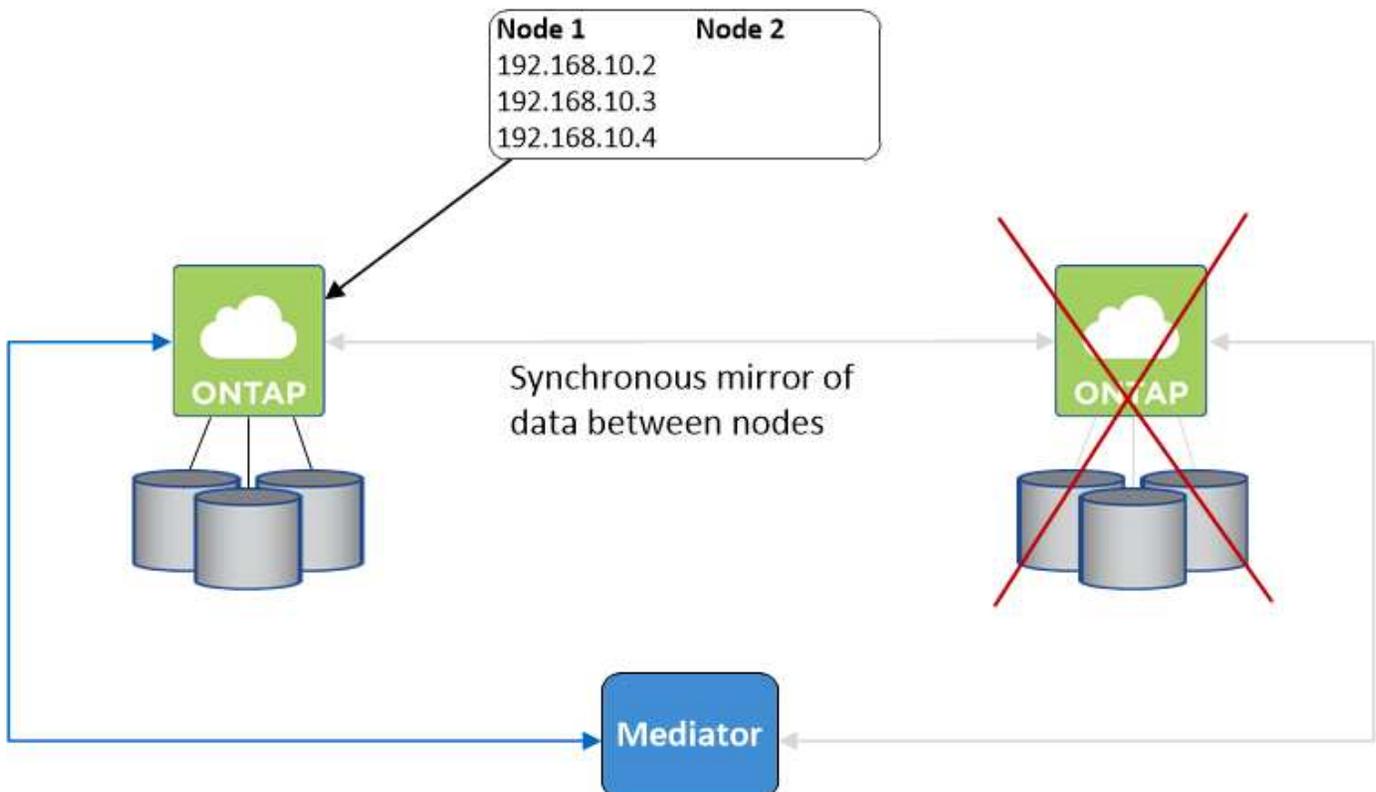
Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.



Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "[Ferramenta de Matriz de interoperabilidade do NetApp](#)" e o Guia de instalação e configuração de Utilitários de host do sistema operacional do seu host.

Takeover de storage e giveback para nas

Quando o controle ocorre em uma configuração nas usando IPs flutuantes, o endereço IP flutuante do nó que os clientes usam para acessar dados se move para o outro nó. A imagem a seguir mostra a aquisição de armazenamento em uma configuração nas usando IPs flutuantes. Se o nó 2 descer, o endereço IP flutuante do nó 2 será movido para o nó 1.



Os IPs de dados nas usados para acesso VPC externo não podem migrar entre nós se ocorrerem falhas. Se um nó ficar offline, você deverá remontar manualmente os volumes para clientes fora da VPC usando o endereço IP no outro nó.

Depois que o nó com falha voltar online, remonte os clientes para volumes usando o endereço IP original. Essa etapa é necessária para evitar a transferência de dados desnecessários entre dois nós de HA, o que pode causar impactos significativo no desempenho e na estabilidade.

Você pode identificar facilmente o endereço IP correto do Cloud Manager selecionando o volume e clicando em **Mount Command**.

Cloud Volumes ONTAP HA em uma única zona de disponibilidade

A implantação de uma configuração de HA em uma única zona de disponibilidade (AZ) pode garantir alta disponibilidade de seus dados se uma instância que executa um nó Cloud Volumes ONTAP falhar. Todos os dados podem ser acessados de forma nativa de fora da VPC.

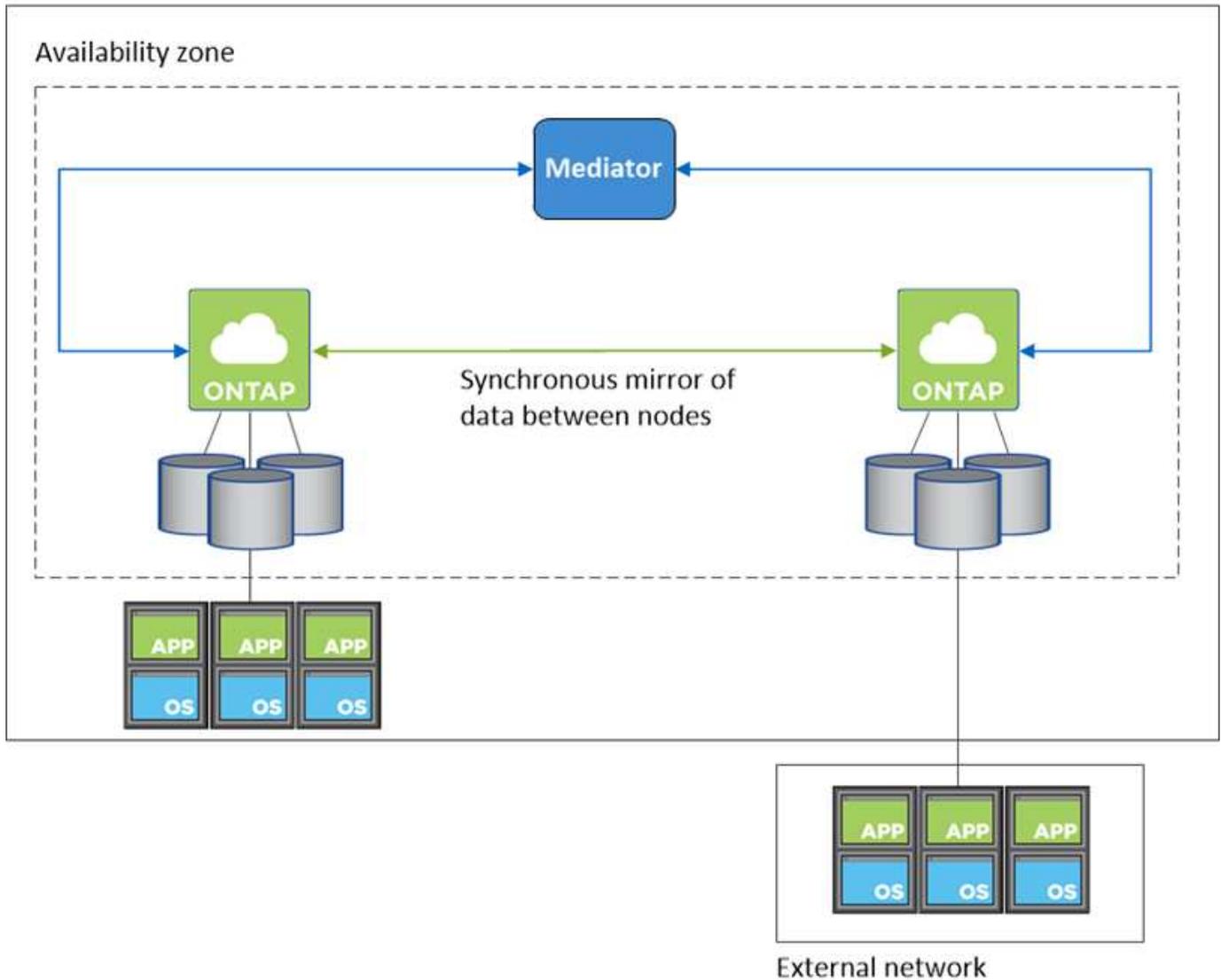


O Cloud Manager cria um "[Grupo de posicionamento do AWS Spread](#)" e lança os dois nós de HA nesse grupo de posicionamento. O grupo de posicionamento reduz o risco de falhas simultâneas, espalhando as instâncias por um hardware subjacente distinto. Esse recurso melhora a redundância do ponto de vista da computação e não do ponto de vista da falha de disco.

Acesso a dados

Como essa configuração está em uma única AZ, ela não requer endereços IP flutuantes. Você pode usar o mesmo endereço IP para acesso a dados a partir da VPC e de fora da VPC.

A imagem a seguir mostra uma configuração de HA em uma única AZ. Os dados são acessíveis a partir da VPC e de fora da VPC.



Takeover de storage e giveback

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.



Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o ["Ferramenta de Matriz de interoperabilidade do NetApp"](#) e o Guia de instalação e configuração de Utilitários de host do sistema operacional do seu host.

Para configurações nas, os endereços IP de dados podem migrar entre nós de HA se ocorrerem falhas. Isso garante o acesso do cliente ao armazenamento.

Como o storage funciona em um par de HA

Ao contrário de um cluster do ONTAP, o storage em um par de HA do Cloud Volumes ONTAP não é compartilhado entre nós. Em vez disso, os dados são espelhados de forma síncrona entre os nós para que os dados estejam disponíveis em caso de falha.

Alocação de armazenamento

Quando você cria um novo volume e são necessários discos adicionais, o Cloud Manager aloca o mesmo número de discos para ambos os nós, cria um agregado espelhado e cria o novo volume. Por exemplo, se forem necessários dois discos para o volume, o Cloud Manager aloca dois discos por nó para um total de quatro discos.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde a solicitações de dados somente se ele tiver ocupado o storage para o nó ativo.



Você só pode configurar uma configuração ativo-ativo quando usar o Cloud Manager na visualização do sistema de armazenamento.

Expectativas de performance para uma configuração de HA

Uma configuração do Cloud Volumes ONTAP HA replica sincronamente os dados entre nós, o que consome a largura de banda da rede. Como resultado, você pode esperar o seguinte desempenho em comparação com uma configuração de Cloud Volumes ONTAP de nó único:

- Para configurações de HA que atendem dados de apenas um nó, a performance de leitura é comparável à performance de leitura de uma configuração de nó único, enquanto a performance de gravação é menor.
- Para configurações de HA que atendem dados de ambos os nós, a performance de leitura é superior à performance de leitura de uma configuração de nó único, e a performance de gravação é igual ou superior.

Para obter mais detalhes sobre o desempenho do Cloud Volumes ONTAP, "[Desempenho](#)" consulte .

Acesso do cliente ao armazenamento

Os clientes devem acessar volumes NFS e CIFS usando o endereço IP de dados do nó no qual o volume reside. Se os clientes nas acessarem um volume usando o endereço IP do nó do parceiro, o tráfego vai entre os dois nós, o que reduz o desempenho.

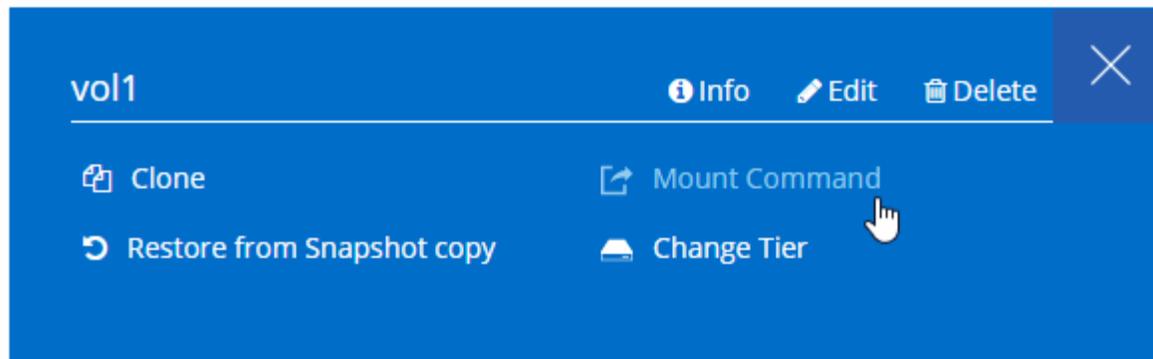


Se você mover um volume entre nós em um par de HA, remonte o volume usando o endereço IP do outro nó. Caso contrário, você pode experimentar desempenho reduzido. Se os clientes suportarem referências NFSv4 ou redirecionamento de pastas para CIFS, você pode habilitar esses recursos nos sistemas Cloud Volumes ONTAP para evitar a reinstalação do volume. Para obter detalhes, consulte a documentação do ONTAP.

Você pode identificar facilmente o endereço IP correto do Cloud Manager:

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)

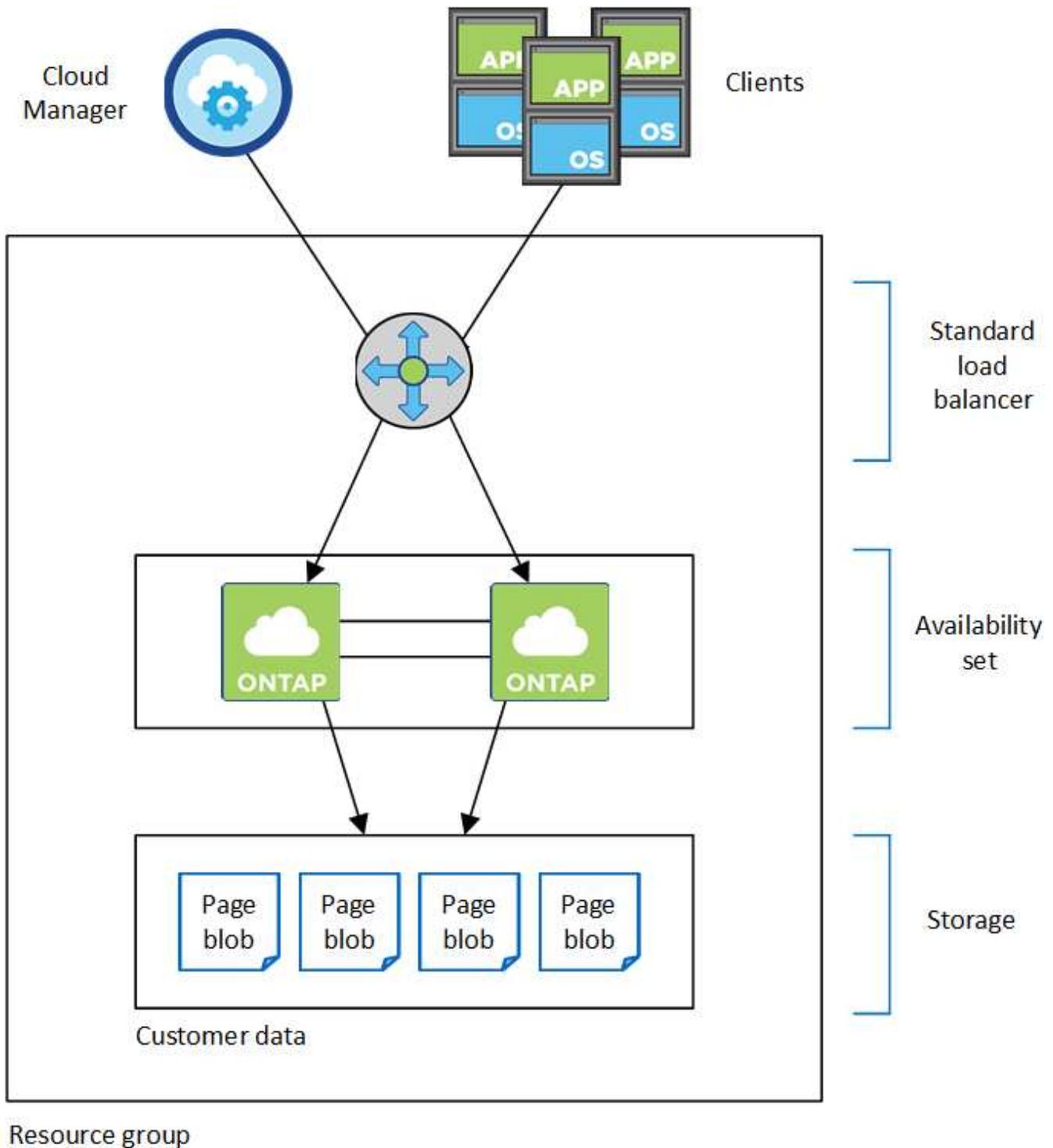


Pares de alta disponibilidade no Azure

Um par de alta disponibilidade (HA) da Cloud Volumes ONTAP fornece confiabilidade empresarial e operações contínuas em caso de falhas em seu ambiente de nuvem. No Azure, o storage é compartilhado entre os dois nós.

Componentes HA

Uma configuração do Cloud Volumes ONTAP HA no Azure inclui os seguintes componentes:



Resource group

Observe o seguinte sobre os componentes do Azure que o Cloud Manager implanta para você:

Azure Standard Load Balancer

O balanceador de carga gerencia o tráfego de entrada para o par de HA do Cloud Volumes ONTAP.

Disponibilidade definida

O conjunto de disponibilidade garante que os nós estejam em diferentes domínios de falha e atualização.

Discos

Os dados do cliente residem nos blobs da página do Premium Storage. Cada nó tem acesso ao storage do outro nó. Também é necessário armazenamento adicional para "[dados de inicialização, raiz e núcleo](#)"o .

Contas de armazenamento

- Uma conta de armazenamento é necessária para discos gerenciados.
- Uma ou mais contas de armazenamento são necessárias para os blobs de página de armazenamento Premium, uma vez que o limite de capacidade de disco por conta de armazenamento é atingido.

["Documentação do Azure: Escalabilidade do Azure Storage e metas de desempenho para contas de storage"](#).

- Uma conta de storage é necessária para a disposição de dados em categorias no storage Azure Blob.
- A partir do Cloud Volumes ONTAP 9,7, as contas de storage criadas pelo Cloud Manager para pares de HA são contas de storage v2 de uso geral.
- Você pode habilitar uma conexão HTTPS de um par de HA do Cloud Volumes ONTAP 9,7 para contas de storage do Azure ao criar um ambiente de trabalho. Observe que ativar essa opção pode afetar o desempenho de gravação. Não é possível alterar a configuração depois de criar o ambiente de trabalho.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos. Seus dados são consistentes transacionalmente, sem perda de dados.
- O objetivo de tempo de recuperação (rto) é de 60 segundos. Em caso de interrupção, os dados devem estar disponíveis em 60 segundos ou menos.

Takeover de storage e giveback

Semelhante a um cluster físico do ONTAP, o storage em um par de HA do Azure é compartilhado entre nós. As conexões com o armazenamento do parceiro permitem que cada nó acesse o armazenamento do outro no caso de um *takeover*. Os mecanismos de failover de caminho de rede garantem que os clientes e hosts continuem a se comunicar com o nó sobrevivente. O parceiro *devolve* armazenamento quando o nó é colocado de volta na linha.

Para configurações nas, os endereços IP de dados são migrados automaticamente entre nós de HA se ocorrerem falhas.

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.



Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "[Ferramenta de Matriz de interoperabilidade do NetApp](#)" e o Guia de instalação e configuração de Utilitários de host do sistema operacional do seu host.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde a solicitações de dados somente se ele tiver ocupado o storage para o nó ativo.

Limitações DE HA

As limitações a seguir afetam os pares de HA do Cloud Volumes ONTAP no Azure:

- Os pares DE HA são compatíveis com o padrão Cloud Volumes ONTAP, Premium e BYOL. Explorar não é suportado.
- NFSv4 não é suportado. NFSv3 é suportado.
- Pares HA não são suportados em algumas regiões.

["Consulte a lista de regiões do Azure suportadas"](#).

["Saiba como implantar um sistema HA no Azure"](#).

A avaliar

Você pode avaliar o Cloud Volumes ONTAP antes de pagar pelo software. A maneira mais comum é lançar a versão PAYGO do seu primeiro sistema Cloud Volumes ONTAP para obter uma avaliação gratuita de 30 dias. Uma licença BYOL de avaliação também é uma opção.

Se você precisar de ajuda com sua prova de conceito, entre em Contato ["A equipa de vendas"](#) ou entre em Contato com a opção de bate-papo disponível ["Centro de nuvem da NetApp"](#) de e no Cloud Manager.

Avaliações gratuitas de 30 dias para PAYGO

Uma avaliação gratuita de 30 dias está disponível se você planeja pagar pelo Cloud Volumes ONTAP conforme você for. Você pode iniciar uma avaliação gratuita de 30 dias do Cloud Volumes ONTAP usando o Cloud Manager criando seu primeiro sistema Cloud Volumes ONTAP na conta de um pagador.

Não há cobranças de licença de software por hora para a instância, mas as cobranças de infraestrutura do seu provedor de nuvem ainda se aplicam.

Uma avaliação gratuita se converte automaticamente em uma assinatura paga por hora quando expira. Se você encerrar a instância dentro do limite de tempo, a próxima instância que você implantar não faz parte da avaliação gratuita (mesmo que ela seja implantada dentro desses 30 dias).

Os testes de pagamento conforme o uso são concedidos por meio de um fornecedor de nuvem e não podem ser estendidos de forma alguma.

Licenças de avaliação para BYOL

Uma licença BYOL de avaliação é uma opção para clientes que esperam pagar pelo Cloud Volumes ONTAP comprando uma licença denominada da NetApp. Você pode obter uma licença de avaliação de sua equipe de conta, seu engenheiro de vendas ou seu parceiro.

A chave de avaliação é boa por 30 dias, e pode ser usada várias vezes, cada uma por 30 dias (independentemente do dia de criação).

No final de 30 dias, desligamentos diários ocorrerão, por isso é melhor Planejar com antecedência. Você pode aplicar uma nova licença BYOL em cima da licença de avaliação para uma atualização no local (isso requer uma reinicialização de sistemas de nó único). Seus dados hospedados são **não** excluídos no final do período de teste.



Não é possível atualizar o software Cloud Volumes ONTAP ao usar uma licença de avaliação.

Licenciamento

Cada sistema BYOL do Cloud Volumes ONTAP deve ter uma licença de sistema instalada com uma assinatura ativa. O Cloud Manager simplifica o processo gerenciando licenças para você e notificando-o antes que elas expirem. As licenças BYOL também estão disponíveis para o Backup to Cloud.

Licenças de sistema BYOL

Você pode comprar várias licenças para um sistema BYOL da Cloud Volumes ONTAP para alocar mais de 368 TB de capacidade. Por exemplo, você pode comprar duas licenças para alocar até 736 TB de capacidade para o Cloud Volumes ONTAP. Ou você pode comprar quatro licenças para obter até 1,4 PB.

O número de licenças que você pode comprar para um único sistema de nó ou par de HA é ilimitado.

Esteja ciente de que os limites de disco podem impedir que você alcance o limite de capacidade usando discos sozinhos. Você pode ir além do limite de disco pelo ["disposição em camadas dos dados inativos no storage de objetos"](#). Para obter informações sobre limites de disco, ["Limites de armazenamento nas Notas de versão do Cloud Volumes ONTAP"](#) consulte .

Gerenciamento de licenças para um novo sistema

Quando você cria um sistema BYOL, o Cloud Manager solicita o número de série da licença e da conta do site de suporte da NetApp. O Cloud Manager usa a conta para baixar o arquivo de licença do NetApp e instalá-lo no sistema Cloud Volumes ONTAP.

["Saiba como adicionar contas do site de suporte da NetApp ao Cloud Manager"](#).

Se o Cloud Manager não puder acessar o arquivo de licença pela conexão segura à Internet, você poderá obter o arquivo sozinho e, em seguida, fazer o upload manual do arquivo para o Cloud Manager. Para obter instruções, ["Gerenciamento de licenças BYOL para Cloud Volumes ONTAP"](#) consulte .

Aviso de expiração da licença

O Cloud Manager avisa-o 30 dias antes de uma licença expirar e novamente quando a licença expirar. A imagem a seguir mostra um aviso de expiração de 30 dias:



Pode selecionar o ambiente de trabalho para rever a mensagem.

Se não renovar a licença a tempo, o sistema Cloud Volumes ONTAP desliga-se. Se você reiniciá-lo, ele se desliga novamente.



O Cloud Volumes ONTAP também pode notificá-lo por e-mail, um trapost SNMP ou servidor syslog usando notificações de eventos do EMS (sistema de Gerenciamento de Eventos). Para obter instruções, consulte "[Guia expresso de configuração de EMS do ONTAP 9](#)".

Renovação da licença

Quando você renova uma assinatura BYOL entrando em Contato com um representante da NetApp, o Cloud Manager obtém automaticamente a nova licença do NetApp e a instala no sistema Cloud Volumes ONTAP.

Se o Cloud Manager não puder acessar o arquivo de licença pela conexão segura à Internet, você poderá obter o arquivo sozinho e, em seguida, fazer o upload manual do arquivo para o Cloud Manager. Para obter instruções, "[Gerenciamento de licenças BYOL para Cloud Volumes ONTAP](#)" consulte .

Licenças de backup BYOL

Uma licença de backup BYOL permite que você compre uma licença da NetApp para usar o backup na nuvem por um determinado período de tempo e por um espaço máximo de backup. Quando um dos limites for atingido, você precisará renovar a licença.

"[Saiba mais sobre a licença BYOL do Backup to Cloud](#)".

Segurança

O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.

Criptografia de dados em repouso

O Cloud Volumes ONTAP oferece suporte às seguintes tecnologias de criptografia:

- Soluções de criptografia NetApp (NVE e NAE)
- AWS Key Management Service
- Criptografia do Serviço de storage do Azure
- Criptografia padrão do Google Cloud Platform

Você pode usar as soluções de criptografia NetApp com criptografia nativa da AWS, Azure ou GCP, que criptografam dados no nível do hipervisor. Fazer isso forneceria criptografia dupla, que pode ser desejada para dados muito confidenciais. Quando os dados criptografados são acessados, eles não são criptografados duas vezes, uma no nível do hipervisor (usando chaves do provedor de nuvem) e outra vez usando soluções de criptografia NetApp (usando chaves de um gerenciador de chaves externo).

Soluções de criptografia NetApp (NVE e NAE)

O Cloud Volumes ONTAP é compatível com criptografia de volume NetApp (NVE) e criptografia agregada NetApp (NAE) com um gerenciador de chaves externo. NVE e NAE são soluções baseadas em software que permitem a criptografia de volumes em repouso compatível com FIPS (140-2) em conformidade com dados em repouso de volumes.

- O NVE criptografa os dados em repouso um volume por vez. Cada volume de dados tem sua própria chave de criptografia exclusiva.

- O NVE é uma extensão do NVE - ele criptografa os dados para cada volume e os volumes compartilham uma chave no agregado. O NAE também permite que blocos comuns em todos os volumes do agregado sejam desduplicados.

Tanto o NVE quanto o NAE usam criptografia AES de 256 bits.

["Saiba mais sobre criptografia de volume NetApp e criptografia agregada NetApp"](#).

A partir do Cloud Volumes ONTAP 9,7, os novos agregados terão a encriptação agregada NetApp (NAE) ativada por predefinição depois de configurar um gestor de chaves externo. Novos volumes que não fazem parte de um agregado NAE terão a criptografia de volume NetApp (NVE) ativada por padrão (por exemplo, se você tiver agregados existentes que foram criados antes de configurar um gerenciador de chaves externo).

Configurar um gerenciador de chaves suportado é o único passo necessário. Para obter instruções de configuração, ["Criptografando volumes com soluções de criptografia NetApp"](#) consulte .

AWS Key Management Service

Ao iniciar um sistema Cloud Volumes ONTAP na AWS, é possível ativar a criptografia de dados usando o ["AWS Key Management Service \(KMS\)"](#). O Cloud Manager solicita chaves de dados usando uma chave mestra do cliente (CMK).



Não é possível alterar o método de criptografia de dados da AWS depois de criar um sistema Cloud Volumes ONTAP.

Se você quiser usar essa opção de criptografia, certifique-se de que o AWS KMS esteja configurado adequadamente. Para obter detalhes, ["Configurando o AWS KMS"](#) consulte .

Criptografia do Serviço de storage do Azure

["Criptografia do Serviço de storage do Azure"](#) Para dados em repouso é habilitado por padrão para dados do Cloud Volumes ONTAP no Azure. Nenhuma configuração é necessária.

Você pode criptografar discos gerenciados do Azure em sistemas Cloud Volumes ONTAP de nó único usando chaves externas de outra conta. Esse recurso é compatível com APIs do Cloud Manager.

Você só precisa adicionar o seguinte à solicitação de API ao criar o sistema de nó único:

```
"azureEncryptionParameters": {  
  "key": <azure id of encryptionset>  
}
```



Chaves gerenciadas pelo cliente não são compatíveis com pares de HA do Cloud Volumes ONTAP.

Criptografia padrão do Google Cloud Platform

["Criptografia de dados em repouso do Google Cloud Platform"](#) É ativado por padrão para o Cloud Volumes ONTAP. Nenhuma configuração é necessária.

Embora o Google Cloud Storage sempre criptografe seus dados antes de serem gravados no disco, você pode usar as APIs do Cloud Manager para criar um sistema Cloud Volumes ONTAP que use *chaves de*

criptografia gerenciadas pelo cliente. Essas são as chaves que você gera e gerencia no GCP usando o Cloud Key Management Service. "[Saiba mais](#)".

Verificação de vírus ONTAP

Você pode usar a funcionalidade de antivírus integrada em sistemas ONTAP 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.

Para obter informações sobre fornecedores, software e versões compatíveis com o Vscan, consulte "[Matriz de interoperabilidade do NetApp](#)".

Para obter informações sobre como configurar e gerenciar a funcionalidade antivírus em sistemas ONTAP, consulte "[Guia de configuração do antivírus do ONTAP 9](#)".

Proteção contra ransomware

Os ataques de ransomware podem custar tempo, recursos e reputação aos negócios. Com o Cloud Manager, você implementa a solução NetApp para ransomware, que fornece ferramentas eficazes de visibilidade, detecção e correção.

- O Cloud Manager identifica volumes que não estão protegidos por uma política do Snapshot e permite ativar a política padrão do Snapshot nesses volumes.

As cópias snapshot são somente leitura, o que impede a corrupção de ransomware. Eles também podem fornecer a granularidade para criar imagens de uma única cópia de arquivo ou uma solução completa de recuperação de desastres.

- O Cloud Manager também permite bloquear extensões comuns de arquivos de ransomware habilitando a solução FPolicy da ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection



50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

"[Saiba como implementar a solução NetApp para ransomware](#)".

Desempenho

Você pode analisar os resultados de performance para decidir quais workloads são apropriados para o Cloud Volumes ONTAP.

- Cloud Volumes ONTAP para AWS

["Relatório Técnico da NetApp 4383: Caracterização de desempenho do Cloud Volumes ONTAP em Serviços Web da Amazon com cargas de trabalho de aplicativos"](#).

- Cloud Volumes ONTAP para Microsoft Azure

["Relatório técnico da NetApp 4671: Caracterização de desempenho do Cloud Volumes ONTAP no Azure com cargas de trabalho de aplicação"](#).

- Cloud Volumes ONTAP para Google Cloud

["Relatório técnico da NetApp 4816: Caracterização de desempenho do Cloud Volumes ONTAP para o Google Cloud"](#).

Configuração padrão para Cloud Volumes ONTAP

Entender como o Cloud Volumes ONTAP é configurado por padrão pode ajudá-lo a configurar e administrar seus sistemas, especialmente se você estiver familiarizado com o ONTAP porque a configuração padrão do Cloud Volumes ONTAP é diferente do ONTAP.

Predefinições

- O Cloud Volumes ONTAP está disponível como um sistema de nó único na AWS, Azure e GCP, além de par de HA na AWS e no Azure.
- O Cloud Manager cria uma VM de storage de fornecimento de dados quando implanta o Cloud Volumes ONTAP. Algumas configurações suportam VMs de storage adicionais. ["Saiba mais sobre como gerenciar VMs de armazenamento"](#).
- O Cloud Manager instala automaticamente as seguintes licenças de recurso do ONTAP no Cloud Volumes ONTAP:
 - CIFS
 - FlexCache
 - FlexClone
 - ISCSI
 - Criptografia de volume NetApp (somente para sistemas BYOL ou PAYGO registrados)
 - NFS
 - SnapMirror
 - SnapRestore
 - SnapVault
- Várias interfaces de rede são criadas por padrão:

- Um LIF de gerenciamento de clusters
- Um LIF entre clusters
- LIF de gerenciamento de SVM em sistemas de HA no Azure, sistemas de nó único na AWS e, opcionalmente, em sistemas de HA em várias zonas de disponibilidade da AWS
- Um LIF de gerenciamento de nós
- Um iSCSI data LIF
- LIF de dados CIFS e NFS



O failover de LIF é desativado por padrão para o Cloud Volumes ONTAP devido aos requisitos do EC2. A migração de um LIF para uma porta diferente rompe o mapeamento externo entre endereços IP e interfaces de rede na instância, tornando o LIF inacessível.

- O Cloud Volumes ONTAP envia backups de configuração para o conector usando HTTPS.

Os backups são acessíveis de <https://ipaddress/occm/offboxconfig/> onde *ipaddress* é o endereço IP do host do conector.

- O Cloud Manager define alguns atributos de volume de maneira diferente de outras ferramentas de gerenciamento (System Manager ou CLI, por exemplo).

A tabela a seguir lista os atributos de volume que o Cloud Manager define de forma diferente dos padrões:

Atributo	Valor definido pelo Cloud Manager
Modo de tamanho automático	crescer
Dimensionamento automático máximo	1.000 por cento  O Administrador da conta pode modificar este valor a partir da página Configurações.
Estilo de segurança	NTFS para volumes CIFS UNIX para volumes NFS
Estilo de garantia de espaço	nenhum
Permissões UNIX (somente NFS)	777

Consulte a página *man volume create* para obter informações sobre esses atributos.

Dados de inicialização e raiz para Cloud Volumes ONTAP

Além do storage para dados de usuário, o Cloud Manager também compra storage de nuvem para dados de

inicialização e raiz em cada sistema Cloud Volumes ONTAP.

AWS

- Dois discos por nó para dados de inicialização e raiz:
 - 9,7: Disco IO1 de 160 gb para dados de inicialização e um disco GP2 de 220 gb para dados de raiz
 - 9,6: Disco IO1 de 93 gb para dados de inicialização e um disco GP2 de 140 gb para dados de raiz
 - 9,5: Disco IO1 de 45 gb para dados de inicialização e um disco GP2 de 140 gb para dados de raiz
- Um instantâneo EBS para cada disco de arranque e disco raiz
- Para pares HA, um volume EBS para a instância Mediator, que é de aproximadamente 8 GB

Azure (nó único)

- Três discos SSD premium:
 - Um disco de 10 GB para dados de inicialização
 - Um disco de 140 GB para dados de raiz
 - Um disco de 128 GB para NVRAM

Se a máquina virtual que você escolheu para o Cloud Volumes ONTAP oferecer suporte a SSDs Ultra, o sistema usará um SSD Ultra para NVRAM, em vez de um SSD Premium.
- Um disco rígido padrão de 1024 GB para guardar núcleos
- Um snapshot do Azure para cada disco de inicialização e disco raiz

Azure (pares de HA)

- Dois discos SSD premium de 10 GB para o volume de inicialização (um por nó)
- Dois blobs de página de armazenamento Premium de 140 GB para o volume raiz (um por nó)
- Dois discos HDD padrão de 1024 GB para guardar núcleos (um por nó)
- Dois discos SSD premium de 128 GB para NVRAM (um por nó)
- Um snapshot do Azure para cada disco de inicialização e disco raiz

GCP

- Um disco persistente padrão de 10 GB para dados de inicialização
- Um disco persistente padrão de 64 GB para dados de raiz
- Um disco persistente padrão de 500 GB para NVRAM
- Um disco persistente padrão de 216 GB para guardar núcleos
- Um snapshot do GCP para o disco de inicialização e o disco raiz

Onde residem os discos

O Cloud Manager estabelece o storage da seguinte forma:

- Os dados de inicialização residem em um disco conectado à instância ou à máquina virtual.

Este disco, que contém a imagem de arranque, não está disponível para o Cloud Volumes ONTAP.

- Os dados de raiz, que contêm a configuração e os logs do sistema, residem no aggr0.
- O volume raiz da máquina virtual de storage (SVM) reside no aggr1.
- Os volumes de dados também residem em aggr1.

Criptografia

Os discos de inicialização e raiz são sempre criptografados no Azure e no Google Cloud Platform porque a criptografia é habilitada por padrão nesses provedores de nuvem.

Quando você ativa a criptografia de dados na AWS usando o Serviço de Gerenciamento de chaves (KMS), os discos de inicialização e raiz do Cloud Volumes ONTAP também são criptografados. Isso inclui o disco de inicialização da instância de mediador em um par de HA. Os discos são criptografados usando o CMK selecionado quando você cria o ambiente de trabalho.

Informações sobre direitos autorais

Copyright © 2024 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 INTERRUPÇÃO 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.