S3 gerenciamento de storage de objetos

ONTAP 9

NetApp
January 17, 2025

Índice

S3 gerenciamento de storage de objetos

Saiba mais sobre o suporte S3 no ONTAP 9

Saiba mais sobre a configuração do ONTAP S3

A partir do ONTAP 9.8, é possível habilitar um servidor de storage de objetos do ONTAP Simple Storage Service (S3) em um cluster ONTAP, usando ferramentas conhecidas de gerenciabilidade, como o Gerenciador de sistemas ONTAP, para provisionar rapidamente o storage de objetos de alta performance para desenvolvimento e operações no ONTAP, aproveitando as eficiências de storage e a segurança do ONTAP.

Configuração do S3 com o Gerenciador de sistemas e a CLI do ONTAP

Você pode configurar e gerenciar o ONTAP S3 com o Gerenciador de sistema e a CLI do ONTAP. Quando você ativa o S3 e cria buckets usando o Gerenciador do sistema, o ONTAP seleciona padrões de práticas recomendadas para configuração simplificada. Se você precisar especificar parâmetros de configuração, talvez queira usar a CLI do ONTAP. Se você configurar o servidor S3 e os buckets da CLI, ainda poderá gerenciá-los com o System Manager, se desejado, ou vice-versa.

Quando você cria um bucket do S3 usando o Gerenciador do sistema, o ONTAP configura um nível de serviço de desempenho padrão que é o mais alto disponível no sistema. Por exemplo, em um sistema AFF, a configuração padrão seria **Extreme**. Os níveis de serviço de performance são grupos de políticas de qualidade do serviço (QoS) adaptáveis predefinidos. Em vez de um dos níveis de serviço padrão, você pode especificar um grupo de políticas de QoS personalizado ou nenhum grupo de políticas.

Os grupos de políticas de QoS adaptáveis predefinidos são:

- **Extreme**: Usado para aplicativos que esperam a menor latência e o mais alto desempenho.
- **Desempenho**: Usado para aplicativos com necessidades de desempenho modestas e latência.
- **Valor**: Usado para aplicativos para os quais a taxa de transferência e a capacidade são mais importantes do que a latência.
- **Custom**: Especifique uma política de QoS personalizada ou nenhuma política de QoS.

Se você selecionar **Use for Tiering**, nenhum nível de serviço de desempenho será selecionado e o sistema tentará selecionar Mídia de baixo custo com desempenho ideal para os dados em camadas.

Veja também"Use grupos de políticas de QoS adaptáveis": .

A ONTAP tenta provisionar esse bucket em camadas locais que tenham os discos mais apropriados, atendendo ao nível de serviço escolhido. No entanto, se você precisar especificar quais discos incluir no bucket, considere configurar o armazenamento de objetos S3 a partir da CLI especificando os níveis locais (agregado). Se você configurar o servidor S3 a partir da CLI, ainda poderá gerenciá-lo com o System Manager, se desejado.

Se você quiser a capacidade de especificar quais agregados são usados para buckets, você só pode fazer isso usando a CLI.

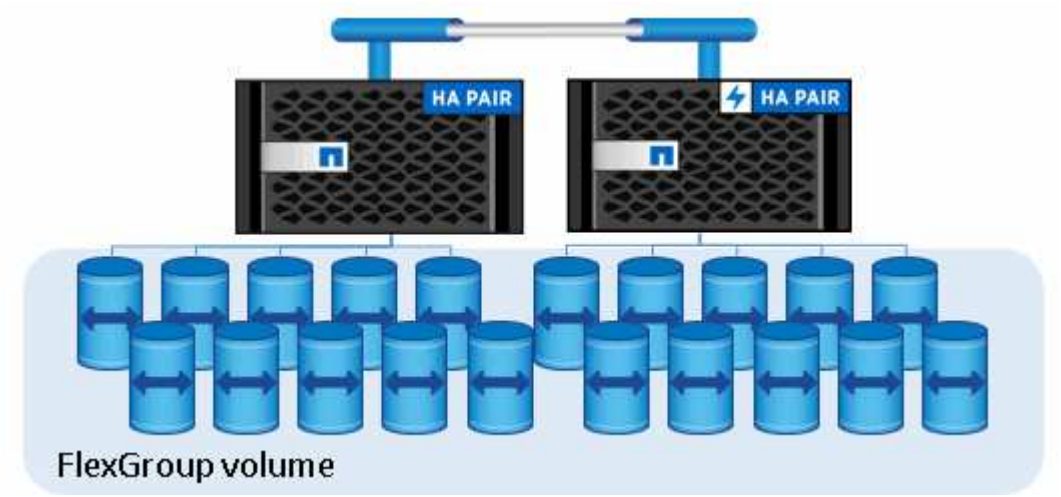
Configurando buckets do S3 no Cloud Volumes ONTAP

Se você quiser atender buckets do Cloud Volumes ONTAP, é altamente recomendável que você selecione manualmente os agregados subjacentes para garantir que eles estejam usando apenas um nó. O uso de agregados de ambos os nós pode afetar o desempenho, porque os nós estarão em zonas de disponibilidade geograficamente separadas e, portanto, suscetíveis a problemas de latência. Portanto, em ambientes Cloud Volumes ONTAP, você deve Configurar buckets do S3 a partir da CLI.

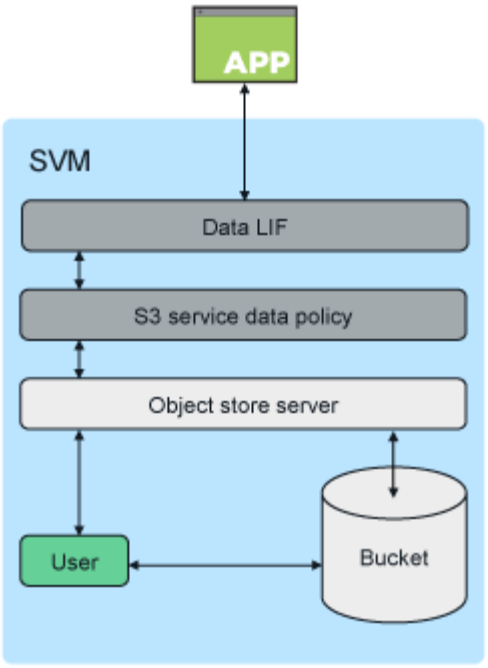
Caso contrário, os servidores S3 no Cloud Volumes ONTAP são configurados e mantidos da mesma forma no Cloud Volumes ONTAP que em ambientes locais.

Arquitetura do ONTAP S3 usando o FlexGroup volumes

No ONTAP, a arquitetura subjacente para um bucket é um "Volume FlexGroup", que é um namespace único que é composto por vários volumes de membros constituintes, mas é gerenciado como um único volume.



O acesso ao bucket é fornecido por meio de usuários autorizados e aplicativos clientes.



Quando um bucket é usado exclusivamente para aplicativos S3, incluindo o uso como um endpoint FabricPool, o volume FlexGroup subjacente só suportará o protocolo S3.

A partir do ONTAP 9.12,1, o protocolo S3 também pode ser ativado em "Volumes nas multiprotocolo" que foram pré-configurados para usar protocolos nas. Quando o protocolo S3 está habilitado em volumes nas multiprotocolo, as aplicações clientes podem ler e gravar dados usando NFS, SMB e S3.

Limites do balde

O tamanho mínimo do balde é 95GB. O tamanho máximo do balde é limitado ao tamanho máximo de FlexGroup de 60PB.

Há um limite de 1000 buckets por volume do FlexGroup ou 12.000 buckets por cluster (usando volumes do FlexGroup de 12 GB).

Dimensionamento automático de FlexGroup com ONTAP 9.14,1 e posterior

A partir do ONTAP 9.14,1, o tamanho padrão do FlexGroup é baseado no tamanho dos buckets subjacentes. O volume FlexGroup aumentará ou diminuirá automaticamente à medida que os baldes forem adicionados ou removidos.

Por exemplo, se um bucket_A inicial for provisionado para ser 100GB, o FlexGroup será thin-provisionado para ser 100GB. Se forem criados dois buckets adicionais, Bucket_B a 300GB e Bucket_C a 500GB, o volume FlexGroup aumentará para 900GB.

(Bucket_a a 100GB Bucket_B a 300GB Bucket_C a 500GB 900GB.)

Se Bucket_A for excluído, o volume FlexGroup subjacente será reduzido para 800GB.

Tamanhos de FlexGroup padrão corrigidos no ONTAP 9.13,1 e anteriores

Para fornecer capacidade para expansão do bucket, a capacidade total usada de todos os buckets no volume

FlexGroup deve ser inferior a 33% da capacidade máxima de volume FlexGroup com base em agregados de storage disponíveis no cluster. Se isso não puder ser atendido, o novo bucket que está sendo criado será provisionado em um novo volume FlexGroup criado automaticamente.

Antes do ONTAP 9.14,1, o tamanho do FlexGroup é fixado a um tamanho padrão com base em seu ambiente:

- 1,6PB em ONTAP
- 100TB em ONTAP Select

Se um cluster não tiver capacidade suficiente para provisionar um volume FlexGroup no tamanho padrão, o ONTAP reduzirá o tamanho padrão pela metade até que ele possa ser provisionado no ambiente existente.

Por exemplo, em um ambiente 300TB, um volume FlexGroup é provisionado automaticamente a 200TB TB (volumes FlexGroup de 1,6PB TB, 800TB TB e 400TB TB sendo muito grandes para o ambiente).

ONTAP S3 principais casos de uso

Estes são os principais casos de uso para acesso de cliente aos serviços do ONTAP S3:

- Usando o FabricPool para categorizar dados inativos em um bucket no ONTAP, permitindo que a ONTAP disponha em camadas do ONTAP. A disposição em camadas em um bucket no "cluster local"repositório ou a disposição em camadas em um bucket no repositório "cluster remoto"é compatível. A disposição em camadas no ONTAP S3 permite que você use sistemas ONTAP mais baratos para dados inativos e economize dinheiro com uma nova capacidade flash, sem a necessidade de licenças FabricPool adicionais ou novas tecnologias para gerenciar.
- A partir do ONTAP 9.12,1, o protocolo S3 também pode ser ativado em "Volumes nas multiprotocolo" que foram pré-configurados para usar protocolos nas. Quando o protocolo S3 está habilitado em volumes nas multiprotocolo, as aplicações clientes podem ler e gravar dados usando S3, NFS e SMB, o que abre uma variedade de casos de uso adicionais. Um dos casos de uso mais comuns são os clientes nas que gravam dados em um volume e os clientes S3 que leem os mesmos dados e executam tarefas especializadas, como análise, business intelligence, aprendizado de máquina e reconhecimento ótico de carateres.

> O ONTAP S3 é apropriado se você quiser habilitar os recursos do S3 em clusters ONTAP existentes sem hardware e gerenciamento adicionais. O NetApp StorageGRID é a principal solução da NetApp para armazenamento de objetos. O StorageGRID é recomendado para aplicações S3 nativas que precisam aproveitar toda a gama de ações S3, recursos avançados de ILM ou capacidades não alcançáveis em sistemas baseados em ONTAP. Para obter mais informações, consulte "Documentação do StorageGRID".

Informações relacionadas

"Gerenciamento de volumes do FlexGroup"

Plano

Versão do ONTAP e suporte de plataforma para storage de objetos S3

O storage de objetos do S3 é compatível com todas as plataformas AFF, FAS e ONTAP Select usando o ONTAP 9.8 e posterior.

Assim como em outros protocolos, como FC, iSCSI, NFS, NVMe_of e SMB, o S3 requer a instalação de uma licença antes que ela possa ser usada no ONTAP. A licença S3 é uma licença de custo zero, mas deve ser

instalada em sistemas que estejam atualizando para o ONTAP 9.8. A licença S3 pode ser transferida a partir do "Página chaves de licença principal"no site de suporte da NetApp.

Os novos sistemas ONTAP 9.8 e posteriores têm a licença S3 pré-instalada.

Cloud Volumes ONTAP

O ONTAP S3 é configurado e funciona da mesma forma no Cloud Volumes ONTAP que em ambientes locais, com uma exceção:

- Ao criar buckets no Cloud Volumes ONTAP, você deve usar o procedimento de CLI para garantir que o volume FlexGroup subjacente use apenas agregados de um único nó. O uso de agregados de vários nós afetará o desempenho porque os nós estarão em zonas de disponibilidade geograficamente separadas e suscetíveis a problemas de latência.

Fornecedor de nuvem	Versão de ONTAP
Azure	ONTAP 9.9,1 e posterior
AWS	ONTAP 9.11,0 e posterior
Google Cloud	ONTAP 9.12,1 e posterior

Amazon FSX para NetApp ONTAP

O armazenamento de objetos S3 é compatível com os serviços do Amazon FSX for NetApp usando o ONTAP 9.11 e posterior.

Suporte S3 com MetroCluster

A partir do ONTAP 9.14,1, é possível habilitar um servidor de storage de objetos S3 em uma SVM em um agregado espelhado em configurações IP e FC do MetroCluster.

A partir do ONTAP 9.12,1, é possível habilitar um servidor de storage de objetos S3 em uma SVM em um agregado sem espelhamento em uma configuração IP do MetroCluster. Para obter mais informações sobre as limitações de agregados sem espelhamento em configurações MetroCluster IP, "Considerações para agregados sem espelhamento"consulte .

S3 visualização pública no ONTAP 9.7

No ONTAP 9.7, o armazenamento de objetos S3 foi introduzido como uma prévia pública. Essa versão não foi destinada a ambientes de produção e não será mais atualizada a partir do ONTAP 9.8. Somente as versões do ONTAP 9.8 e posteriores são compatíveis com storage de objetos do S3 em ambientes de produção.

Os buckets do S3 criados com a visualização pública do 9,7 podem ser usados no ONTAP 9.8 e posterior, mas não podem aproveitar os aprimoramentos de recursos. Se você tiver buckets criados com a visualização pública do 9,7, migre o conteúdo desses buckets para buckets do 9,8 para oferecer suporte a recursos, segurança e melhorias de desempenho.

Ações compatíveis com o ONTAP S3

As ações do ONTAP S3 são compatíveis com APIs REST S3 padrão, exceto conforme indicado abaixo. Para obter detalhes, consulte "Referência de API do Amazon S3".

Essas S3 ações são especificamente suportadas ao usar buckets S3 nativos no ONTAP. Algumas dessas ações, como as associadas ao controle de versão, bloqueios de objetos e outros recursos, não são suportadas ao usar "S3 buckets nas (S3 em volumes nas multiprotocolo)"o .

Operações do balde

As operações a seguir são suportadas no ONTAP usando APIs AWS S3:

Funcionamento do balde	Suporte ONTAP começando com
CreateBucket	ONTAP 9.11,1
DeleteBucket	ONTAP 9.11,1
DeleteBucketPolicy	ONTAP 9.12,1
GetBucketAcl	ONTAP 9,8
GetBucketLifecycleConfiguration	ONTAP 9.13,1 * apenas ações de expiração são suportadas
GetBucketlocalização	ONTAP 9.10,1
Política de GetBucketPolicy	ONTAP 9.12,1
Balde para a cabeça	ONTAP 9,8
ListBuckets	ONTAP 9,8
ListBucketControle de versão	ONTAP 9.11,1
ListObjectVersions	ONTAP 9.11,1
PutBucket	• ONTAP 9.11,1 • ONTAP 9.8 - compatível apenas com APIs REST do ONTAP
PutBucketLifecycleConfiguration	ONTAP 9.13,1 * apenas ações de expiração são suportadas
Política de PutBucketPolicy	ONTAP 9.12,1

Operações de objetos

A partir do ONTAP 9.9,1, o ONTAP S3 oferece suporte a metadados e marcação de objetos.

- PutObject e CreateMultipartUpload incluem pares de chave-valor usando `x-amz-meta-<key>`.

  Por exemplo `x-amz-meta-project: ontap_s3`: .

- GetObject. E HeadObject retornam metadados definidos pelo usuário.
- Ao contrário dos metadados, as tags podem ser lidas independentemente dos objetos usando:
  - Marcação de objetos
  - GetObjectTagging

- DeleteObjectTagging

A partir do ONTAP 9.11,1, o ONTAP S3 oferece suporte ao controle de versão de objetos e às ações associadas a essas APIs do ONTAP:

- GetBucketControle de versão
- ListBucketVersions
- PutBucketControle de versão

Operação do objeto	Suporte ONTAP começando com
AbortMultipartUpload	ONTAP 9,8
CompleteMultipartUpload	ONTAP 9,8
CopyObject	ONTAP 9.12,1
CreateMultipartUpload	ONTAP 9,8
DeleteObject	ONTAP 9,8
DeleteObjects	ONTAP 9.11,1
DeleteObjectTagging	ONTAP 9.9,1
GetBucketControle de versão	ONTAP 9.11,1
GetObject	ONTAP 9,8
GetObjectAcl	ONTAP 9,8
GetObjectRetention	ONTAP 9.14,1
GetObjectTagging	ONTAP 9.9,1
HeadObject	ONTAP 9,8
ListMultipartUpload	ONTAP 9,8
ListObjects	ONTAP 9,8
ListObjectsV2	ONTAP 9,8
ListBucketVersions	ONTAP 9.11,1
ListParts	ONTAP 9,8
PutBucketControle de versão	ONTAP 9.11,1
PutObject	ONTAP 9,8
PutObjectLockConfiguration	ONTAP 9.14,1
Retenção PutObjectRetention	ONTAP 9.14,1
Marcação de objetos	ONTAP 9.9,1
UploadPart	ONTAP 9,8
UploadPartCopy	ONTAP 9.12,1

Políticas de grupo

Essas operações não são específicas do S3 e geralmente estão associadas a processos de identidade e gerenciamento (IAM). O ONTAP é compatível com esses comandos, mas não usa as APIs REST do IAM.

- Criar política
- Política do AttachGroup

Gerenciamento de usuários

Essas operações não são específicas do S3 e geralmente estão associadas aos processos do IAM.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

S3 ações por liberação

ONTAP 9.14,1

ONTAP 9.14,1 adiciona suporte para bloqueio de objetos S3.

> Operações de retenção legal (bloqueios sem tempos de retenção definidos) não são suportadas.

- GetObjectLockConfiguration
- GetObjectRetention
- PutObjectLockConfiguration
- Retenção PutObjectRetention

ONTAP 9.13,1

O ONTAP 9.13,1 adiciona suporte ao gerenciamento do ciclo de vida do bucket.

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9.12,1

O ONTAP 9.12,1 adiciona suporte a políticas de bucket e a capacidade de copiar objetos.

- DeleteBucketPolicy
- Política de GetBucketPolicy
- Política de PutBucketPolicy
- CopyObject
- UploadPartCopy

ONTAP 9.11,1

O ONTAP 9.11,1 adiciona suporte para versionamento, URLs pré-assinados, uploads em grupo e suporte para

ações S3 comuns, como criar e excluir buckets usando APIs do S3.

- O ONTAP S3 agora suporta pedidos de assinatura de uploads em pedaços usando x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD
- O ONTAP S3 agora oferece suporte a aplicativos clientes usando URLs pré-assinados para compartilhar objetos ou permitir que outros usuários façam upload de objetos sem exigir credenciais de usuário.
- CreateBucket
- DeleteBucket
- GetBucketControle de versão
- ListBucketVersions
- PutBucket
- PutBucketControle de versão
- DeleteObjects
- ListObjectVersions

Como o FlexGroup subjacente não é criado até que o primeiro bucket seja, um bucket deve ser criado no ONTAP antes que um cliente externo possa criar um bucket usando o CreateBucket.

ONTAP 9.10,1

ONTAP 9.10,1 adiciona suporte para SnapMirror S3 e GetBucketLocation.

- GetBucketlocalização

ONTAP 9.9,1

O ONTAP 9.9,1 adiciona suporte para metadados de objetos e suporte a marcação ao ONTAP S3.

- PutObject e CreateMultipartUpload agora incluem pares de chave-valor usando 'x-amz-meta-<key>'. Por exemplo: 'X-amz-meta-project: ONTAP_S3'.
- GetObject e HeadObject agora retornam metadados definidos pelo usuário.

Tags também podem ser usadas com baldes. Ao contrário dos metadados, as tags podem ser lidas independentemente dos objetos usando:

- Marcação de objetos
- GetObjectTagging
- DeleteObjectTagging

Interoperabilidade do ONTAP S3

O servidor ONTAP S3 interage normalmente com outras funcionalidades do ONTAP, exceto conforme indicado nesta tabela.

Área da função	Suportado	Não suportado
Cloud Volumes ONTAP	• Clientes Azure no ONTAP 9.9,1 e versões posteriores • Clientes da AWS no ONTAP 9.11,0 e versões posteriores • Clientes do Google Cloud no ONTAP 9.12,1 e versões posteriores	• Cloud Volumes ONTAP para qualquer cliente no ONTAP 9.8 e versões anteriores
Proteção de dados	• Cloud Sync • Bloqueio de objetos; governança e conformidade (começando com ONTAP 9.14,1) • "Controle de versão do objeto" (Começando com ONTAP 9.11,1) • Agregados MetroCluster não espelhados (começando com ONTAP 9.12,1) • Agregados MetroCluster espelhados (começando com ONTAP 9.14,1) • "SnapMirror S3" (Começando com ONTAP 9.10,1) • SnapMirror (somente volumes nas; começando com ONTAP 9.12,1) • SnapLock (somente volumes nas; começando com ONTAP 9.14,1)	• Codificação de apagamento • NDMP • SMTape • SnapMirror • Nuvem da SnapMirror • Recuperação de desastres da SVM • SyncMirror
Criptografia	• Criptografia de agregados NetApp (NAE) • Criptografia de volume NetApp (NVE) • Criptografia de storage do NetApp (NSE) • TLS/SSL	• ESCÓRIA
Eficiência de storage	• Deduplicação • Compactação • Compactação	• Eficiências de nível de agregado • Clone de volume do volume FlexGroup que contém buckets do ONTAP S3

Área da função	Suportado	Não suportado
Virtualização de storage	-	Virtualização NetApp FlexArray
Qualidade do serviço (QoS)	• Valores máximos de QoS (tetos) • Mínimos de QoS (andares)	-
Recursos adicionais	• "Auditoria S3 eventos" (Começando com ONTAP 9.10,1) • "Gerenciamento do ciclo de vida do bucket" (Começando com ONTAP 9.13,1)	• Volumes FlexCache • FPolicy • Qtrees • Quotas

As soluções de terceiros recomendadas pela NetApp para o bucket do ONTAP S3

A NetApp validou as seguintes soluções de terceiros para uso com o ONTAP S3. Se a solução que você está procurando não estiver listada, entre em Contato com seu representante da conta do NetApp.

Soluções de terceiros validadas no ONTAP S3

A NetApp testou essas soluções em colaboração com os respetivos parceiros.

- Amazon SageMaker
- Cliente Apache Hadoop S3A
- Apache Kafka
- Kit de proteção (V11)
- Kafka fluente
- Red Hat Quay
- Rubrik
- Floco de neve
- Trino
- Kit de meia (V12)

Configurar

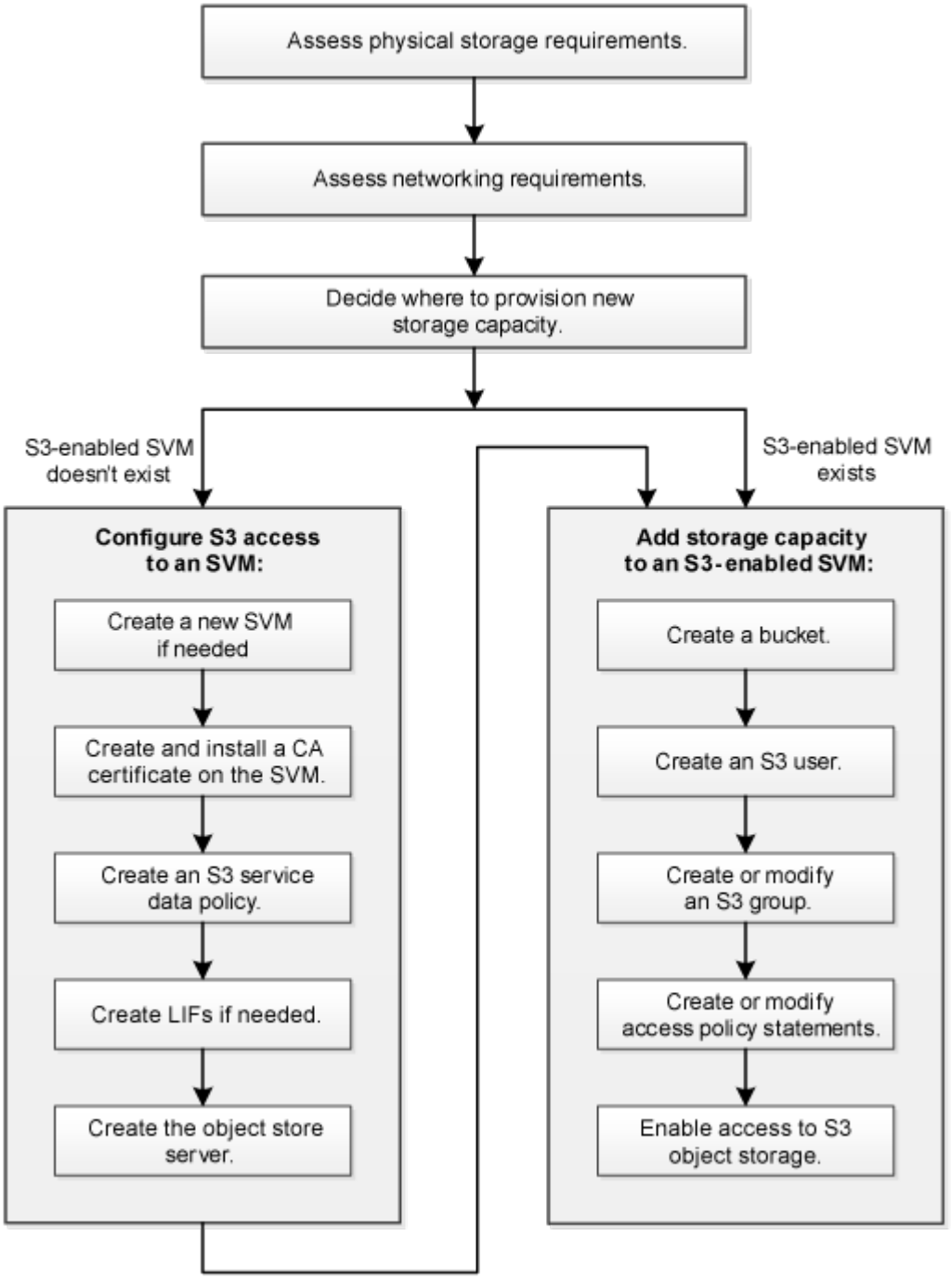
Sobre o processo de configuração do S3

Fluxo de trabalho de configuração do ONTAP S3

A configuração do S3 envolve a avaliação dos requisitos de storage físico e rede e, depois, a escolha de um fluxo de trabalho específico para sua meta: Configurar o acesso do S3 a um SVM novo ou existente, ou adicionar um bucket e usuários a um SVM

existente que já esteja totalmente configurado para o acesso S3.

Ao configurar o acesso S3 a uma nova VM de armazenamento usando o System Manager, você será solicitado a inserir informações de certificado e rede, e a VM de armazenamento e o servidor de armazenamento de objetos S3 são criados em uma única operação.



Avaliar os requisitos de storage físico do ONTAP S3

Antes de provisionar o storage S3 para clientes, você deve garantir que haja espaço suficiente em agregados existentes para o novo armazenamento de objetos. Se não houver, você poderá adicionar discos a agregados existentes ou criar novos agregados do tipo e local desejados.

Sobre esta tarefa

Quando você cria um bucket do S3 em um SVM habilitado para S3, um volume do FlexGroup é "criado automaticamente"compatível com o bucket. Você pode permitir ao ONTAP Select os agregados subjacentes e componentes do FlexGroup automaticamente (o padrão) ou selecionar os agregados subjacentes e componentes do FlexGroup você mesmo.

Se você decidir especificar os agregados e componentes do FlexGroup — por exemplo, se você tiver requisitos de desempenho específicos para os discos subjacentes — você deve garantir que sua configuração agregada esteja de acordo com as diretrizes de práticas recomendadas para o provisionamento de um volume FlexGroup. Saiba mais:

- "Gerenciamento de volumes do FlexGroup"
- "Relatório técnico da NetApp 4571-a: Melhores práticas de volume da NetApp ONTAP FlexGroup"

Se você estiver atendendo buckets do Cloud Volumes ONTAP, é altamente recomendável que você selecione manualmente os agregados subjacentes para garantir que eles estejam usando apenas um nó. O uso de agregados de ambos os nós pode afetar o desempenho, porque os nós estarão em zonas de disponibilidade geograficamente separadas e, portanto, suscetíveis a problemas de latência. Saiba mais "Criando buckets para Cloud Volumes ONTAP"sobre .

Você pode usar o servidor ONTAP S3 para criar uma camada de capacidade FabricPool local, ou seja, no mesmo cluster que a camada de performance. Isso pode ser útil, por exemplo, se você tiver discos SSD conetados a um par de HA e quiser categorizar dados *cold* em discos HDD em outro par de HA. Nesse caso de uso, o servidor S3 e o bucket que contém o nível de capacidade local devem, portanto, estar em um par de HA diferente do nível de performance. A disposição em camadas local não é compatível com clusters de um ou dois nós.

Passos

1. Exibir espaço disponível em agregados existentes:

   ```
   storage aggregate show
   ```

   Se houver um agregado com espaço suficiente ou localização do nó necessária, Registre seu nome para sua configuração do S3.

```
cluster-1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Se não houver agregados com espaço suficiente ou localização de nó necessária, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede do ONTAP S3

Antes de fornecer armazenamento S3 para clientes, você deve verificar se a rede está corretamente configurada para atender aos requisitos de provisionamento S3.

Antes de começar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)
- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Sobre esta tarefa

Para camadas remotas de capacidade FabricPool (nuvem) e clientes S3 remotos, você precisa usar um SVM de dados e configurar LIFs de dados. Para camadas de nuvem do FabricPool, você também precisa configurar LIFs entre clusters. O peering de cluster não é necessário.

Para níveis de capacidade locais do FabricPool, você precisa usar o SVM do sistema (chamado de "'cluster'"), mas você tem duas opções de configuração de LIF:

- Você pode usar os LIFs de cluster.

Nesta opção, não é necessária nenhuma configuração de LIF adicional, mas haverá um aumento no tráfego nos LIFs de cluster. Além disso, o nível local não será acessível a outros clusters.

- Você pode usar dados e LIFs entre clusters.

  Essa opção requer configuração adicional, incluindo a ativação das LIFs para o protocolo S3, mas o nível local também estará acessível como uma camada de nuvem FabricPool remota para outros clusters.

Passos

1. Exiba as portas físicas e virtuais disponíveis:

   `network port show`

   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.
   - Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis:

   `network subnet show`

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis:

   `network ipspace show`

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster:

   `network options ipv6 show`

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decidir onde provisionar nova capacidade de storage ONTAP S3

Antes de criar um novo bucket do S3, você deve decidir se o colocará em um SVM novo ou existente. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um bucket em um novo SVM ou SVM que não esteja habilitado para S3, execute as etapas dos tópicos a seguir.

  "Criar um SVM para S3"

  "Crie um bucket para S3"

  Embora o S3 possa coexistir em uma SVM com NFS e SMB, você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

- Você está habilitando S3 em um cluster pela primeira vez.
- Você tem SVMs existentes em um cluster no qual não deseja habilitar o suporte ao S3.
- Você tem um ou mais SVMs habilitados para S3 em um cluster e deseja outro servidor S3 com caraterísticas de desempenho diferentes. Depois de ativar o S3 no SVM, prossiga com o provisionamento de um bucket.

- Se você quiser provisionar o bucket inicial ou um bucket adicional em um SVM habilitado para S3 existente, execute as etapas do tópico a seguir.

  "Crie um bucket para S3"

Configurar o acesso do S3 a uma SVM

Criar um SVM para ONTAP S3

Embora o S3 possa coexistir com outros protocolos em um SVM, você pode querer criar um novo SVM para isolar o namespace e a carga de trabalho.

Sobre esta tarefa

Se você estiver fornecendo apenas um storage de objetos S3 a partir de uma SVM, o servidor S3 não exigirá nenhuma configuração DNS. No entanto, você pode querer configurar o DNS no SVM se outros protocolos forem usados.

Ao configurar o acesso S3 a uma nova VM de armazenamento usando o System Manager, você será solicitado a inserir informações de certificado e rede, e a VM de armazenamento e o servidor de armazenamento de objetos S3 são criados em uma única operação.

Exemplo 1. Passos

System Manager

Você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN do servidor S3 não deve começar com um nome de bucket.

Você deve estar preparado para inserir endereços IP para dados de função de interface.

Se você estiver usando um certificado assinado de CA externo, será solicitado que o insira durante este procedimento; você também terá a opção de usar um certificado gerado pelo sistema.

1. Habilite o S3 em uma VM de storage.

   a. Adicionar uma nova VM de armazenamento: Clique em **armazenamento > armazenamento de VMs** e, em seguida, clique em **Adicionar**.

      Se este for um novo sistema sem VMs de armazenamento existentes: Clique em **Dashboard > Configure Protocols**.

   Se estiver adicionando um servidor S3 a uma VM de armazenamento existente: Clique em **armazenamento > armazenamento de VMs**, selecione uma VM de armazenamento, clique em **Configurações** e, em seguida, clique em **S3**.

   a. Clique em **Ativar S3** e, em seguida, introduza o nome do servidor S3.
   b. Selecione o tipo de certificado.

      Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.

   c. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Verifique se o S3 está licenciado no cluster:

   ```
   system license show -package s3
   ```

   Se não estiver, contacte o seu representante de vendas.

2. Criar um SVM:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- Utilize a definição UNIX para a `-rootvolume-security-style` opção.
- Utilize a opção C.UTF-8 predefinida `-language`.
- A `ipspace` definição é opcional.

3. Verifique a configuração e o status do SVM recém-criado:

```
vserver show -vserver <svm_name>
```

O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no ipspace ipspaceA:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação. Por padrão, a conta de usuário vsadmin é criada e está no `locked` estado. A função vsadmin é atribuída à conta de usuário padrão vsadmin.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Crie e instale um certificado de CA em um SVM habilitado para ONTAP S3

Um certificado de autoridade de certificação (CA) é necessário para habilitar o tráfego HTTPS de clientes S3 para o SVM habilitado para S3. O uso de certificados de CA cria uma relação confiável entre aplicativos clientes e o servidor de armazenamento de objetos ONTAP. Um certificado de CA deve ser instalado no ONTAP antes de usá-lo como um armazenamento de objetos acessível a clientes remotos.

Sobre esta tarefa

Embora seja possível configurar um servidor S3 para usar apenas HTTP, e embora seja possível configurar clientes sem um requisito de certificado de CA, é uma prática recomendada proteger o tráfego HTTPS para servidores ONTAP S3 com um certificado de CA.

Um certificado de CA não é necessário para um caso de uso local de disposição em camadas, em que o tráfego IP está passando apenas pelas LIFs de cluster.

As instruções neste procedimento irão criar e instalar um certificado auto-assinado ONTAP. Embora o ONTAP possa gerar certificados autoassinados, o uso de certificados assinados de uma autoridade de certificação de terceiros é a prática recomendada.; consulte a documentação de autenticação do administrador para obter mais informações.

"Autenticação de administrador e RBAC"

Consulte as `security certificate` páginas man para obter opções de configuração adicionais.

Passos

1. Crie um certificado digital autoassinado:

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   A `-type root-ca` opção cria e instala um certificado digital autoassinado para assinar outros certificados agindo como autoridade de certificação (CA).

   A `-common-name` opção cria o nome da Autoridade de Certificação (CA) do SVM e será usada ao gerar o nome completo do certificado.

   O tamanho padrão do certificado é de 2048 bits.

   Exemplo

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Quando o nome gerado do certificado for exibido; certifique-se de salvá-lo para etapas posteriores neste procedimento.

2. Gerar uma solicitação de assinatura de certificado:

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   O `-common-name` parâmetro para a solicitação de assinatura deve ser o nome do servidor S3 (FQDN).

   Você pode fornecer a localização e outras informações detalhadas sobre o SVM, se desejado.

   Você será solicitado a manter uma cópia da solicitação de certificado e da chave privada para referência futura.

3. Assine a CSR usando SVM_CA para gerar o certificado do S3 Server:

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   Insira as opções de comando que você usou nas etapas anteriores:

   - `-ca` — o nome comum da CA que você inseriu na Etapa 1.
   - `-ca-serial` — o número de série da CA a partir do passo 1. Por exemplo, se o nome do certificado CA for svm1_CA_159D1587CE21E9D4_svm1_CA, o número de série será 159D1587CE21E9D4.

Por padrão, o certificado assinado expirará em 365 dias. Você pode selecionar outro valor e especificar outros detalhes de assinatura.

Quando solicitado, copie e insira a string de solicitação de certificado que você salvou na Etapa 2.

Um certificado assinado é exibido; salve-o para uso posterior.

4. Instale o certificado assinado no SVM habilitado para S3:

   `security certificate install -type server -vserver svm_name`

   Quando solicitado, insira o certificado e a chave privada.

   Você tem a opção de inserir certificados intermediários se uma cadeia de certificados for desejada.

   Quando a chave privada e o certificado digital assinado pela CA forem exibidos, salve-os para referência futura.

5. Obtenha o certificado de chave pública:

   `security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

   Salve o certificado de chave pública para uma configuração posterior do lado do cliente.

   Exemplo

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
          FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
               Certificate Authority: svm1_ca
                 Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
             Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
              Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Crie a política de dados de serviço do ONTAP S3

Você pode criar políticas de serviço para dados e serviços de gerenciamento do S3. É necessária uma política de dados de serviço S3 para permitir o tráfego de dados S3 nos LIFs.

Sobre esta tarefa

Uma política de dados de serviço S3 é necessária se você estiver usando LIFs de dados e LIFs entre clusters. Não é necessário se você estiver usando LIFs de cluster para o caso de uso de disposição em camadas local.

Quando uma política de serviço é especificada para um LIF, a política é usada para criar uma função padrão, política de failover e lista de protocolos de dados para o LIF.

Embora vários protocolos possam ser configurados para SVMs e LIFs, é uma prática recomendada para S3 ser o único protocolo ao fornecer dados de objetos.

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Criar uma política de dados de serviço:

   `network interface service-policy create -vserver` *`svm_name`* `-policy` *`policy_name`* `-services data-core,data-s3-server`

   Os `data-core` serviços e `data-s3-server` são os únicos necessários para habilitar o ONTAP S3, embora outros serviços possam ser incluídos conforme necessário.

Criar LIFs de dados para o ONTAP S3

Se você criou um novo SVM, as LIFs dedicadas que você cria para o acesso S3 devem ser LIFs de dados.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- A política de serviço LIF já deve existir.
- Como prática recomendada, os LIFs usados para acesso a dados (data-S3-server) e LIFs usados para operações de gerenciamento (Management-https) devem ser separados. Ambos os serviços não devem ser ativados no mesmo LIF.
- Os Registros DNS devem ter apenas endereços IP dos LIFs que têm dados-S3-server associados a eles. Se endereços IP de outros LIFs forem especificados no Registro DNS, as solicitações do ONTAP S3 podem ser atendidas por outros servidores, resultando em respostas inesperadas ou perda de dados.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- Se você habilitar a disposição em camadas remota de capacidade FabricPool (nuvem), também deverá configurar LIFs entre clusters.

Passos

1. Criar um LIF:

   `network interface create -vserver` *`svm_name`* `-lif` *`lif_name`* `-service-policy` *`service_policy_names`* `-home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto-revert {true|false}`

   - `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

     Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial

com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.
- A `-service-policy` opção especifica a política de dados e serviços de gerenciamento que você criou e quaisquer outras políticas necessárias.

2. Se você quiser atribuir um endereço IPv6 na `-address` opção:

   a. Use o `network ndp prefix show` comando para visualizar a lista de prefixos RA aprendidos em várias interfaces.

      O `network ndp prefix show` comando está disponível no nível de privilégio avançado.

   b. Use o formato `prefix:id` para construir o endereço IPv6 manualmente.

      `prefix` é o prefixo aprendido em várias interfaces.

   Para derivar o `id`, escolha um número hexadecimal aleatório de 64 bits.

3. Verifique se o LIF foi criado com sucesso usando o `network interface show` comando.
4. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Exemplos

O comando a seguir mostra como criar um LIF de dados S3 atribuído com a `my-S3-policy` política de serviço:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Criar LIFs entre clusters para disposição remota de FabricPool em camadas com o ONTAP S3

Se você estiver habilitando a disposição em camadas remota de capacidade FabricPool (nuvem) usando o ONTAP S3, configure LIFs entre clusters. Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- A política de serviço LIF já deve existir.

Sobre esta tarefa

Os LIFs não são necessários para a disposição em camadas do pool de malha local ou para servir aplicações S3 externas.

Passos

1. Liste as portas no cluster:

   `network port show`

   O exemplo a seguir mostra as portas de rede no `cluster01`:

   ```
   cluster01::> network port show
                                                                 Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Criar LIFs entre clusters no sistema:

   `network interface create -vserver Cluster -lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

   O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

   `network interface show –service-policy default-intercluster -failover`

   O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` na `e0c` porta irão falhar para a `e0d` porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Crie o servidor de armazenamento de objetos ONTAP S3

O servidor de armazenamento de objetos ONTAP gerencia dados como objetos S3, em vez de armazenamento de arquivos ou blocos fornecido pelos servidores ONTAP nas e SAN.

Antes de começar

Você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN não deve começar com um nome de intervalo. Ao acessar buckets usando o estilo virtual hospedado, o nome do servidor será usado como `mydomain.com`. Por exemplo, `bucketname.mydomain.com`.

Você deve ter um certificado de CA autoassinado (criado em etapas anteriores) ou um certificado assinado por um fornecedor de CA externo. Um certificado de CA não é necessário para um caso de uso local de disposição em camadas, em que o tráfego IP está passando apenas pelas LIFs de cluster.

Sobre esta tarefa

Quando um servidor de armazenamento de objetos é criado, um usuário raiz com UID 0 é criado. Nenhuma chave de acesso ou chave secreta é gerada para este usuário raiz. O administrador do ONTAP deve executar o `object-store-server users regenerate-keys` comando para definir a chave de acesso e a chave secreta para esse usuário.

> Como uma prática recomendada do NetApp, não use esse usuário root. Qualquer aplicativo cliente que use a chave de acesso ou chave secreta do usuário raiz tem acesso total a todos os buckets e objetos no armazenamento de objetos.

Consulte as `vserver object-store-server` páginas de manual para obter opções adicionais de configuração e exibição.

Exemplo 2. Passos

System Manager

Use este procedimento se estiver adicionando um servidor S3 a uma VM de armazenamento existente. Para adicionar um servidor S3 a uma nova VM de armazenamento, "Criar um SVM de storage em S3"consulte .

Você deve estar preparado para inserir endereços IP para dados de função de interface.

1. Habilite o S3 em uma VM de storage existente.
   a. Selecione a VM de armazenamento: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento, clique em **Settings** e, em seguida, clique em **S3**.
   b. Clique em **Ativar S3** e, em seguida, introduza o nome do servidor S3.
   c. Selecione o tipo de certificado.

      Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.

   d. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Crie o servidor S3:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   Você pode especificar opções adicionais ao criar o servidor S3 ou a qualquer momento mais tarde.

   - Se você estiver configurando a disposição em categorias locais, o nome do SVM pode ser um nome de data SVM ou SVM do sistema (cluster).
   - O nome do certificado deve ser o nome do certificado do servidor (usuário final ou certificado de folha) e não o certificado de CA do servidor (certificado de CA intermediário ou raiz).
   - O HTTPS é ativado por padrão na porta 443. Pode alterar o número da porta com a `-secure -listener-port` opção.

     Quando o HTTPS está ativado, os certificados de CA são necessários para a integração correta com SSL/TLS. A partir do ONTAP 9.15,1, o TLS 1,3 é compatível com armazenamento de objetos S3.

   - O HTTP está desativado por padrão. Quando ativado, o servidor escuta na porta 80. Você pode ativá-lo com a `-is-http-enabled` opção ou alterar o número da porta com a `-listener -port` opção.

Quando o HTTP está ativado, a solicitação e as respostas são enviadas pela rede em texto não criptografado.

2. Verifique se o S3 está configurado:

```
vserver object-store-server show
```

Exemplo

Este comando verifica os valores de configuração de todos os servidores de armazenamento de objetos:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Adicionar capacidade de storage a um SVM habilitado para S3

Crie um bucket do ONTAP S3

S3 objetos são mantidos em *buckets*. Eles não são aninhados como arquivos dentro de um diretório dentro de outros diretórios.

Antes de começar

Uma VM de armazenamento contendo um servidor S3 já deve existir.

Sobre esta tarefa

- A partir do ONTAP 9.14,1, o redimensionamento automático foi ativado em volumes FlexGroup S3 quando os intervalos são criados neles. Isso elimina a alocação excessiva de capacidade durante a criação do bucket em volumes FlexGroup novos e existentes. Os volumes FlexGroup são redimensionados para um tamanho mínimo necessário com base nas diretrizes a seguir. O tamanho mínimo necessário é o tamanho total de todos os buckets do S3 em um volume FlexGroup.
  - A partir do ONTAP 9.14,1, se um volume S3 FlexGroup for criado como parte de uma nova criação de bucket, o volume FlexGroup será criado com o tamanho mínimo necessário.
  - Se um volume S3 FlexGroup foi criado antes do ONTAP 9.14,1, o primeiro bucket criado ou excluído após o ONTAP 9.14,1 redimensiona o volume FlexGroup para o tamanho mínimo necessário.
  - Se um volume S3 FlexGroup foi criado antes do ONTAP 9.14,1 e já tinha o tamanho mínimo necessário, a criação ou eliminação de um bucket subsequente ao ONTAP 9.14,1 mantém o tamanho do volume S3 FlexGroup.

- Os níveis de serviço de storage são grupos de políticas de qualidade do serviço (QoS) adaptáveis predefinidos, com níveis padrão *value*, *performance* e *extreme*. Em vez de um dos níveis de serviço de storage padrão, você também pode definir um grupo de políticas de QoS personalizadas e aplicá-lo a um bucket. Para obter mais informações sobre definições de serviço de armazenamento, "Definições do serviço de armazenamento"consulte . Para obter mais informações sobre gerenciamento de desempenho, "Gerenciamento de desempenho"consulte . A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.
- Se você estiver configurando a disposição em camadas de capacidade local, crie buckets e usuários em uma VM de storage de dados, não na VM de storage do sistema onde o servidor S3 está localizado.
- Para acesso remoto ao cliente, você deve configurar buckets em uma VM de storage habilitada para S3. Se você criar um bucket em uma VM de storage que não esteja habilitada para S3, ele estará disponível somente para a disposição em categorias locais.
- Começando com ONTAP 9.14,1, você pode "Crie um bucket em um agregado espelhado ou sem espelhamento em uma configuração do MetroCluster".
- Para a CLI, quando você cria um bucket, você tem duas opções de provisionamento:
  - Deixe ONTAP Select os agregados subjacentes e componentes FlexGroup (padrão)
    - O ONTAP cria e configura um volume FlexGroup para o primeiro bucket selecionando automaticamente os agregados. Ele selecionará automaticamente o nível de serviço mais alto disponível para sua plataforma ou você pode especificar o nível de serviço de storage. Quaisquer buckets adicionais adicionados posteriormente à VM de storage terão o mesmo volume FlexGroup subjacente.
    - Como alternativa, você pode especificar se o bucket será usado para disposição em camadas, caso em que o ONTAP tenta selecionar Mídia de baixo custo com desempenho ideal para os dados em camadas.
  - Você seleciona os agregados subjacentes e componentes FlexGroup (requer opções de comando de privilégios avançados): Você tem a opção de selecionar manualmente os agregados nos quais o bucket e o volume FlexGroup contendo devem ser criados e, em seguida, especificar o número de constituintes em cada agregado. Ao adicionar baldes adicionais:
    - Se você especificar agregados e componentes para um novo bucket, um novo FlexGroup será criado para o novo bucket.
    - Se você não especificar agregados e componentes para um novo bucket, o novo bucket será adicionado a um FlexGroup existente. Consulte Gerenciamento de volumes do FlexGroup para obter mais informações.

      Quando você especifica agregados e constituintes ao criar um bucket, nenhum grupo de política de QoS, padrão ou personalizado, é aplicado. Você pode fazê-lo mais tarde com o `vserver object-store-server bucket modify` comando.

  Saiba mais sobre `vserver object-store-server bucket modify` o "Referência do comando ONTAP"na .

Observação: se você estiver servindo buckets do Cloud Volumes ONTAP, você deve usar o procedimento CLI. É altamente recomendável que você selecione manualmente os agregados subjacentes para garantir que eles estejam usando apenas um nó. O uso de agregados de ambos os nós pode afetar o desempenho, porque os nós estarão em zonas de disponibilidade geograficamente separadas e, portanto, suscetíveis a problemas de latência.

Crie buckets do S3 com a CLI do ONTAP

1. Se você pretende selecionar agregados e componentes do FlexGroup você mesmo, defina o nível de privilégio como avançado (caso contrário, o nível de privilégio de administrador é suficiente): `set -privilege advanced`
2. Criar um bucket:

   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

   O nome da VM de storage pode ser uma VM de storage de dados ou `Cluster` (o nome da VM de storage do sistema) se você estiver configurando a disposição em camadas local.

   Se você não especificar nenhuma opção, o ONTAP criará um bucket do 800GB com o nível de serviço definido para o nível mais alto disponível para o sistema.

   Se você quiser que o ONTAP crie um bucket com base no desempenho ou no uso, use uma das seguintes opções:

   - nível de serviço

     Inclua a `-storage-service-level` opção com um dos seguintes valores: `value`, `performance`, Ou `extreme`.

   - disposição em camadas

     Inclua a `-used-as-capacity-tier true` opção.

     Se você quiser especificar os agregados nos quais criar o volume FlexGroup subjacente, use as seguintes opções:

   - O `-aggr-list` parâmetro especifica a lista de agregados a serem usados para componentes de volume FlexGroup.

     Cada entrada na lista cria um constituinte no agregado especificado. Você pode especificar um agregado várias vezes para ter vários constituintes criados no agregado.

   Para obter performance consistente em todo o volume FlexGroup, todos os agregados precisam usar o mesmo tipo de disco e configurações de grupo RAID.

   - O `-aggr-list-multiplier` parâmetro especifica o número de vezes a iterar sobre os agregados que são listados com o `-aggr-list` parâmetro ao criar um volume FlexGroup.

     O valor padrão do `-aggr-list-multiplier` parâmetro é 4.

3. Adicione um grupo de políticas de QoS, se necessário:

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Verificar a criação do balde:

   `vserver object-store-server bucket show [-instance]`

Exemplo

O exemplo a seguir cria um bucket para a VM de armazenamento de `vs1` tamanho `1TB` e especificando o agregado:

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Crie buckets do S3 com o System Manager

1. Adicione um novo bucket em uma VM de storage habilitada para S3.
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.
      - Se você clicar em **Salvar** neste ponto, um bucket será criado com as seguintes configurações padrão:
        - Nenhum usuário tem acesso ao bucket, a menos que as políticas de grupo já estejam em vigor.

          Você não deve usar o usuário raiz do S3 para gerenciar o armazenamento de objetos do ONTAP e compartilhar suas permissões, pois ele tem acesso ilimitado ao armazenamento de objetos. Em vez disso, crie um usuário ou grupo com Privileges administrativo que você atribuir.

        - Um nível de qualidade de serviço (desempenho) que é o mais alto disponível para o seu sistema.
      - Clique em **Salvar** para criar um bucket com esses valores padrão.

Configurar permissões e restrições adicionais

Você pode clicar em **mais Opções** para configurar as configurações de bloqueio de objetos, permissões de usuário e nível de desempenho ao configurar o bucket, ou você pode modificar essas configurações posteriormente.

Se você pretende usar o armazenamento de objetos S3 para disposição em camadas do FabricPool, considere selecionar **usar para disposição em camadas** (usar Mídia de baixo custo com desempenho ideal para os dados em camadas) em vez de um nível de serviço de desempenho.

Se você quiser habilitar o controle de versão para seus objetos para recuperação posterior, selecione **Ativar controle de versão**. O controle de versão é habilitado por padrão se você estiver habilitando o bloqueio de objetos no bucket. Para obter informações sobre o controle de versão de objetos, consulte "Usando o controle de versão em buckets do S3 para Amazon".

A partir de 9.14.1, o bloqueio de objetos é suportado em buckets do S3. O bloqueio de objetos S3 requer uma licença SnapLock padrão. Esta licença está incluída no "ONTAP One". Antes do ONTAP One, a licença SnapLock foi incluída no pacote Segurança e conformidade. O pacote de segurança e conformidade já não é oferecido, mas ainda é válido. Embora não seja necessário atualmente, os clientes existentes podem optar por "Atualize para o ONTAP One". Se você estiver habilitando o bloqueio de objetos em um bucket, deverá "Verifique se uma licença SnapLock está instalada". Se uma licença do SnapLock não estiver instalada, você deve "instale" fazê-la antes de ativar o bloqueio de objetos. Quando tiver verificado que a licença SnapLock

está instalada, para proteger os objetos no bucket de serem excluídos ou substituídos, selecione **Ativar bloqueio de objetos**. O bloqueio pode ser ativado em todas as versões específicas de objetos e apenas quando o relógio SnapLock Compliance é inicializado para os nós de cluster. Siga estes passos:

1. Se o relógio SnapLock Compliance não for inicializado em nenhum nó do cluster, o botão **Inicializar Relógio SnapLock Compliance** será exibido. Clique em **Inicializar Relógio SnapLock Compliance** para inicializar o relógio SnapLock Compliance nos nós do cluster.
2. Selecione o modo **Governance** para ativar um bloqueio baseado em tempo que permite permissões *Write Once, Read many (WORM)* nos objetos. Mesmo no modo *Governance*, os objetos podem ser excluídos por usuários administradores com permissões específicas.
3. Selecione o modo **Compliance** se quiser atribuir regras mais rigorosas de exclusão e atualização nos objetos. Neste modo de bloqueio de objetos, os objetos podem ser expirados apenas na conclusão do período de retenção especificado. A menos que um período de retenção seja especificado, os objetos permanecem bloqueados indefinidamente.
4. Especifique o período de retenção para o bloqueio em dias ou anos se você quiser que o bloqueio seja efetivo por um determinado período.

> O bloqueio é aplicável a baldes S3 com controle de versão e sem controle de versão. O bloqueio de objetos não é aplicável a objetos nas.

Você pode configurar as configurações de proteção e permissão, bem como o nível de serviço de desempenho para o bucket.

> Você já deve ter criado usuários e grupos antes de configurar as permissões.

Para obter informações, "Criar espelho para um novo balde"consulte .

Verifique o acesso ao balde

Em aplicativos cliente S3 (seja ONTAP S3 ou um aplicativo externo de terceiros), você pode verificar seu acesso ao bucket recém-criado digitando o seguinte:

- O certificado da CA do servidor S3.
- A chave de acesso e a chave secreta do usuário.
- O nome do FQDN do servidor S3 e o nome do bucket.

Aumente ou diminua o tamanho do balde ONTAP S3

Quando necessário, você pode aumentar ou diminuir o tamanho de um balde existente.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para gerenciar o tamanho do bucket.

System Manager

1. Selecione **armazenamento > baldes** e localize o balde que pretende modificar.
2. Clique ⋮ ao lado do nome do intervalo e selecione **Editar**.
3. Na janela **Edit bucket**, altere a capacidade do bucket.
4. **Guardar**.

CLI

1. Alterar a capacidade do balde:

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

Crie um bucket do ONTAP S3 em um agregado espelhado ou sem espelhamento em uma configuração do MetroCluster

A partir do ONTAP 9.14,1, você pode provisionar um bucket em um agregado espelhado ou sem espelhamento nas configurações FC e IP do MetroCluster.

Sobre esta tarefa

- Por padrão, os buckets são provisionados em agregados espelhados.
- As mesmas diretrizes de provisionamento descritas em "Crie um bucket" aplicam-se à criação de um bucket em um ambiente MetroCluster.
- Os seguintes recursos de armazenamento de objetos S3 são **não** suportados em ambientes MetroCluster:
  - SnapMirror S3
  - Gerenciamento do ciclo de vida do bucket do S3
  - S3 bloqueio de objetos no modo **Compliance**

    ⓘ O bloqueio de objetos S3D no modo **Governance** é suportado.

  - Disposição em camadas no local FabricPool

Antes de começar

Um SVM que contenha um servidor S3 já deve existir.

Processo para criar buckets

CLI

1. Se você pretende selecionar agregados e componentes do FlexGroup você mesmo, defina o nível de privilégio como avançado (caso contrário, o nível de privilégio de administrador é suficiente): `set -privilege advanced`
2. Criar um bucket:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   Defina a `-use-mirrored-aggregates` opção como `true` ou `false` dependendo se você deseja usar um agregado espelhado ou sem espelhamento.

   Por padrão, a `-use-mirrored-aggregates` opção é definida como `true`.

   - O nome do SVM deve ser um data SVM.
   - Se você não especificar nenhuma opção, o ONTAP criará um bucket do 800GB com o nível de serviço definido para o nível mais alto disponível para o sistema.
   - Se você quiser que o ONTAP crie um bucket com base no desempenho ou no uso, use uma das seguintes opções:
     - nível de serviço

       Inclua a `-storage-service-level` opção com um dos seguintes valores: `value`, `performance`, Ou `extreme`.

     - disposição em camadas

       Inclua a `-used-as-capacity-tier true` opção.
   - Se você quiser especificar os agregados nos quais criar o volume FlexGroup subjacente, use as seguintes opções:
     - O `-aggr-list` parâmetro especifica a lista de agregados a serem usados para componentes de volume FlexGroup.

       Cada entrada na lista cria um constituinte no agregado especificado. Você pode especificar um agregado várias vezes para ter vários constituintes criados no agregado.

   Para obter performance consistente em todo o volume FlexGroup, todos os agregados precisam usar o mesmo tipo de disco e configurações de grupo RAID.

   - O `-aggr-list-multiplier` parâmetro especifica o número de vezes a iterar sobre os agregados que são listados com o `-aggr-list` parâmetro ao criar um volume FlexGroup.

     O valor padrão do `-aggr-list-multiplier` parâmetro é 4.
3. Adicione um grupo de políticas de QoS, se necessário:

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. Verificar a criação do balde:

```
vserver object-store-server bucket show [-instance]
```

Exemplo

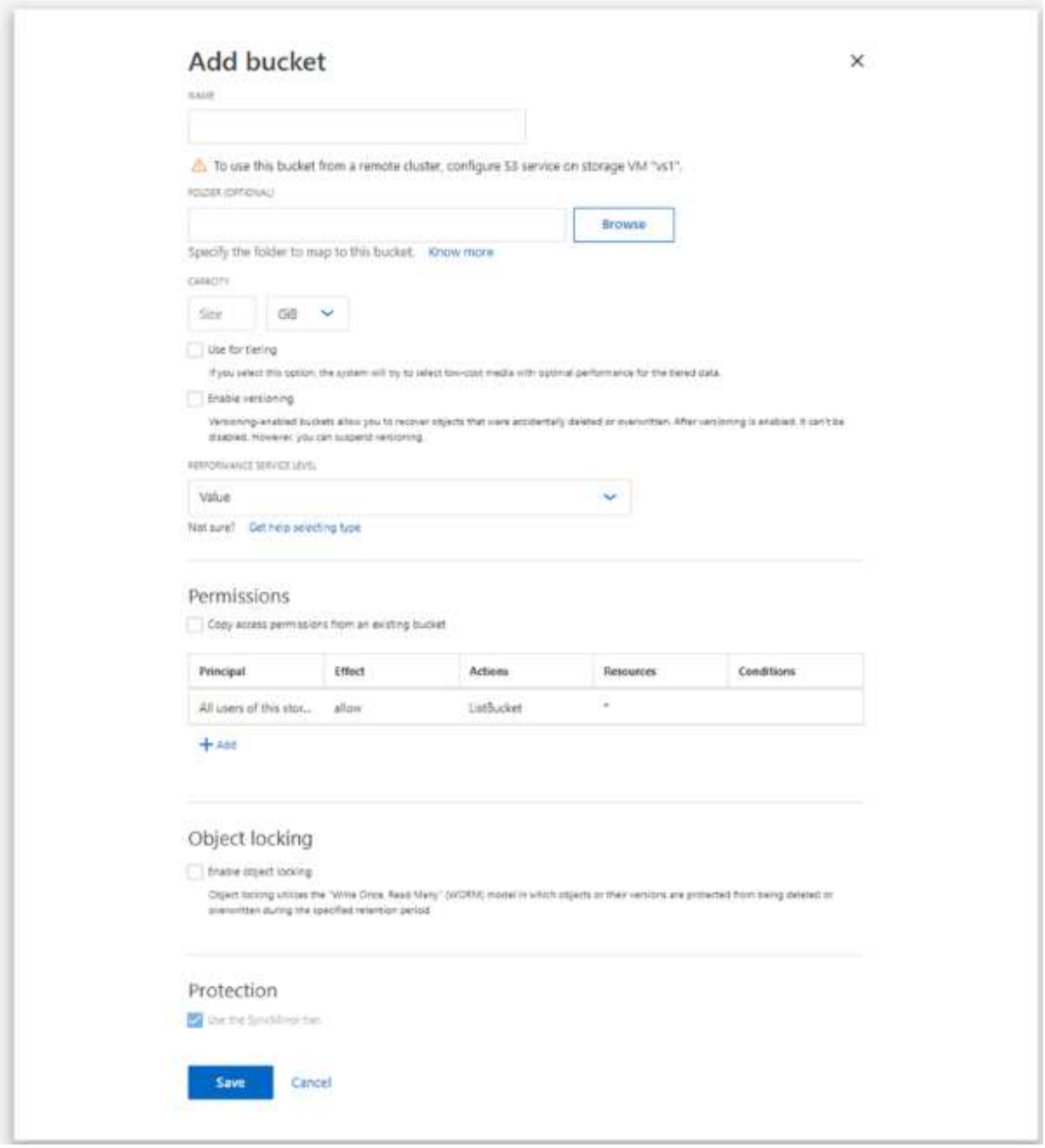
O exemplo a seguir cria um bucket do SVM VS1 de tamanho 1TB em um agregado espelhado:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Adicione um novo bucket em uma VM de storage habilitada para S3.
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Por padrão, o bucket é provisionado em um agregado espelhado. Se você quiser criar um bucket em um agregado sem espelhamento, selecione **mais opções** e desmarque a caixa **Use the SyncMirror Tier** sob **proteção** conforme mostrado na imagem a seguir:



- Se você clicar em **Salvar** neste ponto, um bucket será criado com as seguintes configurações padrão:
  - Nenhum usuário tem acesso ao bucket, a menos que as políticas de grupo já estejam em vigor.

> Você não deve usar o usuário raiz do S3 para gerenciar o armazenamento de objetos do ONTAP e compartilhar suas permissões, pois ele tem acesso ilimitado ao armazenamento de objetos. Em vez disso, crie um usuário ou grupo com Privileges administrativo que você atribuir.

  - Um nível de qualidade de serviço (desempenho) que é o mais alto disponível para o seu sistema.
- Você pode clicar em **mais Opções** para configurar permissões de usuário e nível de desempenho ao configurar o bucket, ou você pode modificar essas configurações

posteriormente.

- Você já deve ter criado usuários e grupos antes de usar **mais Opções** para configurar suas permissões.
- Se você pretende usar o armazenamento de objetos S3 para disposição em camadas do FabricPool, considere selecionar **usar para disposição em camadas** (usar Mídia de baixo custo com desempenho ideal para os dados em camadas) em vez de um nível de serviço de desempenho.

2. Em aplicativos cliente S3 (outro sistema ONTAP ou um aplicativo externo de 3rd parceiros), verifique o acesso ao novo bucket inserindo o seguinte:
   - O certificado da CA do servidor S3.
   - A chave de acesso e a chave secreta do usuário.
   - O nome do FQDN do servidor S3 e o nome do bucket.

Criar uma regra de gerenciamento do ciclo de vida do bucket do ONTAP S3

A partir do ONTAP 9.13,1, é possível criar regras de gerenciamento de ciclo de vida para gerenciar os ciclos de vida dos objetos nos buckets do S3. Você pode definir regras de exclusão para objetos específicos em um bucket e, por meio dessas regras, expirar esses objetos de bucket. Isso permite que você atenda aos requisitos de retenção e gerencie o storage geral de objetos do S3 com eficiência.

Se o bloqueio de objetos estiver ativado para os objetos de bucket, as regras de gerenciamento de ciclo de vida para expiração de objetos não serão aplicadas em objetos bloqueados. Para obter informações sobre o bloqueio de objetos, "Crie um bucket"consulte .

Antes de começar

- Um SVM habilitado para S3 que contenha um servidor S3 e um bucket já deve existir. Consulte "Criar um SVM para S3" para obter mais informações.
- Você deve estar ciente de que as regras de gerenciamento do ciclo de vida do bucket não são compatíveis com configurações do MetroCluster.

Sobre esta tarefa

Ao criar suas regras de gerenciamento de ciclo de vida, você pode aplicar as seguintes ações de exclusão aos objetos bucket:

- Exclusão de versões atuais - esta ação expira objetos identificados pela regra. Se o controle de versão estiver habilitado no bucket, o S3 tornará todos os objetos expirados indisponíveis. Se o controle de versão não estiver habilitado, essa regra excluirá os objetos permanentemente. A ação CLI é `Expiration`.
- Exclusão de versões não-atuais - esta ação especifica quando S3 pode remover permanentemente objetos não-atuais. A ação CLI é `NoncurrentVersionExpiration`.

Uma versão não atual é baseada no tempo de criação ou modificação da versão atual. A remoção atrasada de objetos não atuais pode ser útil quando você exclui ou sobrescreve acidentalmente um objeto. Por exemplo, você pode configurar uma regra de expiração para excluir versões não-atuais cinco dias após elas se tornarem não-atuais. Por exemplo, suponha que em 1/1/2014 às 10:30 UTC (horário de Brasília) você crie um objeto chamado `photo.gif` (ID da versão `111111`). Em 1/2/2014 às 11:30 UTC (horário de Brasília), você exclui acidentalmente `photo.gif` (ID da versão `111111`), o que cria um marcador de exclusão com um novo ID de versão (como ID da versão `4857693`). Agora você tem cinco dias para recuperar a versão original `photo.gif` do (ID da versão `111111`) antes que a exclusão seja permanente. Em 1/8/2014 às 00:00 UTC, a regra de ciclo de vida para expiração é executada e exclui permanentemente `photo.gif` (ID da versão `111111`), cinco dias depois que se tornou uma versão não atual.

- Eliminação de marcadores de eliminação expirados - esta ação elimina marcadores de eliminação de objetos expirados. Em buckets habilitados para versionamento, objetos com marcadores de exclusão se tornam as versões atuais dos objetos. Os objetos não são excluídos e nenhuma ação pode ser executada neles. Esses objetos expiram quando não há versões atuais associadas a eles. A ação CLI é `Expiration`.
- Eliminação de carregamentos de várias partes incompletos - esta ação define um tempo máximo (em dias) que pretende permitir que os carregamentos de várias partes permaneçam em curso. Depois disso, eles são excluídos. A ação CLI é `AbortIncompleteMultipartUpload`.

O procedimento que você segue depende da interface que você usa. Com o ONTAP 9.13,1, você precisa usar o CLI. A partir do ONTAP 9.14,1, você também pode usar o Gerenciador do sistema.

Gerencie regras de gerenciamento de ciclo de vida com a CLI

A partir do ONTAP 9.13,1, você pode usar a CLI do ONTAP para criar regras de gerenciamento de ciclo de vida para expirar objetos nos buckets do S3.

Antes de começar

Para a CLI, você precisa definir os campos obrigatórios para cada tipo de ação de expiração ao criar uma regra de gerenciamento do ciclo de vida do bucket. Esses campos podem ser modificados após a criação inicial. A tabela a seguir exibe os campos exclusivos para cada tipo de ação.

Tipo de ação	Campos únicos
Não CurrentVersionExpiration	• `-non-curr-days` - Número de dias após os quais as versões não atuais serão excluídas • `-new-non-curr-versions` - Número de versões não atuais mais recentes a reter
Expiração	• `-obj-age-days` - Número de dias desde a criação, após o qual a versão atual dos objetos pode ser excluída • `-obj-exp-date` - Data específica em que os objetos devem expirar • `-expired-obj-del-markers` - Limpar marcadores de exclusão de objeto

AbortIncompleteMultipartUpload	• `-after-initiation-days` - Número de dias de início, após o qual o upload pode ser abortado

Para que a regra de gerenciamento do ciclo de vida do bucket seja aplicada somente a um subconjunto específico de objetos, os administradores devem definir cada filtro ao criar a regra. Se esses filtros não forem definidos ao criar a regra, a regra será aplicada a todos os objetos dentro do intervalo.

Todos os filtros podem ser modificados após a criação inicial *exceto* para o seguinte

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Passos

1. Use o `vserver object-store-server bucket lifecycle-management-rule create` comando com campos obrigatórios para o seu tipo de ação de expiração para criar a regra de gerenciamento do ciclo de vida do bucket.

Exemplo

O comando a seguir cria uma regra de gerenciamento do ciclo de vida do bucket NonCurrentVersionExpiration:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Exemplo

O comando a seguir cria uma regra de gerenciamento do ciclo de vida do bucket Expiration:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Exemplo

O comando a seguir cria uma regra de gerenciamento do ciclo de vida do bucket do

AbortIncompleteMultipartUpload:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Gerencie regras de gerenciamento de ciclo de vida com o System Manager

A partir do ONTAP 9.14,1, você pode expirar S3 objetos usando o Gerenciador de sistema. Você pode adicionar, editar e excluir regras de gerenciamento de ciclo de vida para seus objetos S3D. Além disso, você pode importar uma regra de ciclo de vida criada para um bucket e utilizá-la para os objetos em outro bucket. Você pode desativar uma regra ativa e ativá-la mais tarde.

Adicionar uma regra de gerenciamento de ciclo de vida

1. Clique em **armazenamento > baldes**.
2. Selecione o intervalo para o qual você deseja especificar a regra de expiração.
3. Clique no ⋮ ícone e selecione **Gerenciar regras de ciclo de vida**.
4. Clique em **Add > Lifecycle rule**.
5. Na página Adicionar uma regra de ciclo de vida, adicione o nome da regra.
6. Defina o escopo da regra, se você deseja que ela seja aplicada a todos os objetos no bucket ou em objetos específicos. Se você quiser especificar objetos, adicione pelo menos um dos seguintes critérios de filtro:
   a. Prefixo: Especifique um prefixo dos nomes das chaves do objeto aos quais a regra deve ser aplicada. Normalmente, é o caminho ou pasta do objeto. Você pode inserir um prefixo por regra. A menos que um prefixo válido seja fornecido, a regra se aplica a todos os objetos em um bucket.
   b. Tags: Especifique até três pares de chaves e valores (tags) para os objetos aos quais a regra deve ser aplicada. Somente chaves válidas são usadas para filtragem. O valor é opcional. No entanto, se você adicionar valores, certifique-se de adicionar apenas valores válidos para as chaves correspondentes.
   c. Tamanho: Você pode limitar o escopo entre os tamanhos mínimo e máximo dos objetos. Pode introduzir um ou ambos os valores. A unidade padrão é MIB.
7. Especifique a ação:
   a. **Expire a versão atual dos objetos**: Defina uma regra para tornar todos os objetos atuais permanentemente indisponíveis após um número específico de dias desde a sua criação ou em uma data específica. Esta opção não estará disponível se a opção **Excluir marcadores de exclusão de objetos expirados** estiver selecionada.
   b. **Excluir permanentemente versões não atuais**: Especifique o número de dias após os quais a versão não atual é excluída e o número de versões a serem mantidas.
   c. **Excluir marcadores de exclusão de objetos expirados**: Selecione esta ação para excluir objetos com marcadores de exclusão expirados, ou seja, excluir marcadores sem um objeto atual associado.

Essa opção fica indisponível quando você seleciona a opção **expire a versão atual dos objetos** que exclui automaticamente todos os objetos após o período de retenção. Essa opção também fica indisponível quando tags de objeto são usadas para filtragem.

d. **Excluir carregamentos de várias partes incompletos**: Defina o número de dias após os quais os uploads de várias partes incompletos serão excluídos. Se os uploads de várias partes que estão em andamento falharem dentro do período de retenção especificado, você poderá excluir os uploads de várias partes incompletos. Esta opção fica indisponível quando as tags de objeto são usadas para filtragem.

e. Clique em **Salvar**.

Importar uma regra de ciclo de vida

1. Clique em **armazenamento > baldes**.
2. Selecione o intervalo para o qual você deseja importar a regra de expiração.
3. Clique no ⋮ ícone e selecione **Gerenciar regras de ciclo de vida**.
4. Clique em **Adicionar > Importar uma regra**.
5. Selecione o intervalo a partir do qual você deseja importar a regra. As regras de gerenciamento de ciclo de vida definidas para o bucket selecionado são exibidas.
6. Selecione a regra que pretende importar. Você tem a opção de selecionar uma regra de cada vez, sendo a seleção padrão a primeira regra.
7. Clique em **Importar**.

Edite, exclua ou desative uma regra

Você só pode editar as ações de gerenciamento de ciclo de vida associadas à regra. Se a regra foi filtrada com tags de objeto, as opções **Excluir marcadores de exclusão de objeto expirados** e **Excluir carregamentos de várias partes incompletos** não estarão disponíveis.

Quando você exclui uma regra, essa regra não se aplicará mais a objetos associados anteriormente.

1. Clique em **armazenamento > baldes**.
2. Selecione o intervalo para o qual deseja editar, excluir ou desativar a regra de gerenciamento de ciclo de vida.
3. Clique no ⋮ ícone e selecione **Gerenciar regras de ciclo de vida**.
4. Selecione a regra pretendida. Você pode editar e desativar uma regra de cada vez. Você pode excluir várias regras de uma só vez.
5. Selecione **Edit**, **Delete** ou **Disable** e conclua o procedimento.

Crie um usuário do ONTAP S3

Crie um usuário S3 com permissões específicas. A autorização do usuário é necessária em todos os armazenamentos de objetos ONTAP para restringir a conetividade a clientes autorizados.

Antes de começar.

Uma VM de storage habilitada para S3 já deve existir.

Sobre esta tarefa

Um usuário S3 pode ter acesso a qualquer bucket em uma VM de armazenamento. Quando você cria um usuário S3, uma chave de acesso e uma chave secreta também são gerados para o usuário. Eles devem ser compartilhados com o usuário juntamente com o FQDN do armazenamento de objetos e o nome do bucket.

Para maior segurança, a partir de ONTAP 9.15,1, as chaves de acesso e as chaves secretas só são exibidas no momento em que o usuário S3 é criado e não podem ser exibidas novamente. Se as chaves forem perdidas, "novas chaves devem ser regeneradas".

Você pode conceder permissões de acesso específicas a usuários do S3 em uma política de bucket ou uma diretiva de servidor de objetos.

Quando você cria um novo servidor de armazenamento de objetos, o ONTAP cria um usuário raiz (UID 0), que é um usuário privilegiado com acesso a todos os buckets. Em vez de administrar o ONTAP S3 como usuário raiz, o NetApp recomenda que uma função de usuário de administrador seja criada com Privileges específicos.

CLI

1. Criar um usuário S3:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - Adicionar um comentário é opcional.
   - A partir de ONTAP 9.14,1, pode definir o período de tempo para o qual a chave será válida no `-key-time-to-live` parâmetro. Você pode adicionar o período de retenção neste formato para indicar o período após o qual a chave de acesso expira: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Por exemplo, se você quiser inserir um período de retenção de um dia, duas horas, três minutos e quatro segundos, digite o valor como `P1DT2H3M4S`. A menos que especificado, a chave é válida por um período de tempo indefinido.

     O exemplo abaixo cria um usuário com nome `sm_user1` na VM de armazenamento `vs0` , com um período de retenção de chave de uma semana.

```
vserver object-store-server user create -vserver vs0 -user sm_user1
-key-time-to-live P1W
```

2. Certifique-se de salvar a chave de acesso e a chave secreta. Eles serão necessários para acesso de clientes S3.

System Manager

1. Clique em **Storage > Storage VMs**. Selecione a VM de armazenamento à qual você precisa adicionar um usuário, selecione **Configurações** e clique em S3.
2. Para adicionar um usuário, clique em **usuários > Adicionar**.
3. Introduza um nome para o utilizador.
4. A partir do ONTAP 9.14,1, você pode especificar o período de retenção das chaves de acesso que são criadas para o usuário. Você pode especificar o período de retenção em dias, horas, minutos ou segundos, após o qual as chaves expiram automaticamente. Por padrão, o valor é definido como `0` que indica que a chave é válida indefinidamente.
5. Clique em **Salvar**. O usuário é criado e uma chave de acesso e uma chave secreta são geradas para o usuário.
6. Transfira ou guarde a chave de acesso e a chave secreta. Eles serão necessários para acesso de clientes S3.

Próximas etapas

- Criar ou modificar grupos S3

Crie ou modifique grupos de usuários do ONTAP S3 para controlar o acesso aos buckets

Você pode simplificar o acesso ao bucket criando grupos de usuários com autorizações de acesso apropriadas.

Antes de começar

S3 usuários em um SVM habilitado para S3 já devem existir.

Sobre esta tarefa

Os usuários de um grupo S3 podem ter acesso a qualquer bucket em um SVM, mas não em vários SVMs. As permissões de acesso de grupo podem ser configuradas de duas maneiras:

- Ao nível do balde

  Depois de criar um grupo de usuários do S3, você especifica permissões de grupo em declarações de política de bucket e elas se aplicam somente a esse bucket.

- No nível da SVM

  Depois de criar um grupo de usuários S3, você especifica nomes de diretiva de servidor de objetos na definição de grupo. Essas políticas determinam os buckets e o acesso dos membros do grupo.

System Manager

1. Edite a VM de armazenamento: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.
2. Adicionar um grupo: Selecione **grupos** e, em seguida, selecione **Adicionar**.
3. Introduza um nome de grupo e selecione a partir de uma lista de utilizadores.
4. Você pode selecionar uma política de grupo existente ou adicionar uma agora, ou pode adicionar uma política mais tarde.

CLI

1. Criar um grupo S3:
   `vserver object-store-server group create -vserver` *`svm_name`* `-name` *`group_name`* `-users` *`user_name\(s\)`* `[-policies` *`policy_names`*`] [-comment` *`text`*`\]` A `-policies` opção pode ser omitida em configurações com apenas um bucket em um armazenamento de objetos; o nome do grupo pode ser adicionado à política de bucket. A `-policies` opção pode ser adicionada mais tarde com o `vserver object-store-server group modify` comando após a criação de políticas de servidor de armazenamento de objetos.

Regenere as chaves ONTAP S3 e modifique seu período de retenção

Chaves de acesso e chaves secretas são geradas automaticamente durante a criação do usuário para habilitar o acesso do cliente S3. Você pode regenerar chaves para um usuário se uma chave estiver expirada ou comprometida.

Para obter informações sobre a geração de chaves de acesso, "Crie um usuário S3"consulte .

System Manager

1. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
2. Na guia **Settings**, clique no mosaico **S3**.
3. Na guia **usuários**, verifique se não há nenhuma chave de acesso ou se a chave expirou para o usuário.
4. Se você precisar regenerar a chave, clique ao lado do usuário e clique em **regenerar chave**.
5. Por padrão, as chaves geradas são válidas por um período de tempo indefinido. A partir de 9.14.1, você pode modificar seu período de retenção, após o qual as chaves expiram automaticamente. Insira o período de retenção em dias, horas, minutos ou segundos.
6. Clique em **Salvar**. A chave é regenerada. Qualquer alteração no período de retenção da chave entra em vigor imediatamente.
7. Transfira ou guarde a chave de acesso e a chave secreta. Eles serão necessários para acesso de clientes S3.

CLI

1. Regenere o acesso e as chaves secretas para um usuário executando o `vserver object-store-server user regenerate-keys` comando.
2. Por padrão, as chaves geradas são válidas indefinidamente. A partir de 9.14.1, você pode modificar seu período de retenção, após o qual as chaves expiram automaticamente. Você pode adicionar o período de retenção neste formato: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Por exemplo, se quiser inserir um período de retenção de um dia, duas horas, três minutos e quatro segundos, digite o valor como `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. Guarde as chaves de acesso e secretas. Eles serão necessários para acesso de clientes S3.

Criar ou modificar instruções de política de acesso

Saiba mais sobre as políticas de servidor de armazenamento de objetos e bucket do ONTAP S3

O acesso de usuário e grupo a recursos do S3 é controlado por políticas de servidor de armazenamento de objetos e bucket. Se você tem um pequeno número de usuários ou grupos, controlar o acesso no nível do bucket provavelmente é suficiente, mas se você tiver muitos usuários e grupos, é mais fácil controlar o acesso no nível do servidor do armazenamento de objetos.

Adicione regras de acesso à política de bucket do ONTAP S3 padrão

Você pode adicionar regras de acesso à política de bucket padrão. O escopo de seu controle de acesso é o balde contendo, portanto, é mais apropriado quando há um único balde.

Antes de começar

Uma VM de armazenamento habilitada para S3 contendo um servidor S3 e um bucket já deve existir.

Você já deve ter criado usuários ou grupos antes de conceder permissões.

Sobre esta tarefa

Você pode adicionar novas instruções para novos usuários e grupos ou modificar os atributos de instruções existentes. Para obter mais opções, consulte as `vserver object-store-server bucket policy` páginas de manual.

Permissões de usuário e grupo podem ser concedidas quando o bucket é criado ou conforme necessário mais tarde. Você também pode modificar a capacidade do bucket e a atribuição do grupo de políticas de QoS.

A partir do ONTAP 9.9,1, se você planeja oferecer suporte à funcionalidade de marcação de objetos cliente AWS com o servidor ONTAP S3, as ações `GetObjectTagging` `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Passos

1. Edite o bucket: Clique em **Storage > Buckets**, clique no bucket desejado e clique em **Edit**. Ao adicionar ou modificar permissões, você pode especificar os seguintes parâmetros:
   - **Principal**: O usuário ou grupo a quem o acesso é concedido.
   - **Efeito**: Permite ou nega o acesso a um usuário ou grupo.
   - **Ações**: Ações permitidas no intervalo para um determinado usuário ou grupo.
   - **Recursos**: Caminhos e nomes de objetos dentro do intervalo para o qual o acesso é concedido ou negado.

     Os padrões ***bucketname*** e ***bucketname/**** concedem acesso a todos os objetos no bucket. Você também pode conceder acesso a objetos únicos; por exemplo, ***bucketname/*_readme.txt**.

   - **Condições** (opcional): Expressões que são avaliadas quando o acesso é tentado. Por exemplo, você pode especificar uma lista de endereços IP para os quais o acesso será permitido ou negado.

> A partir do ONTAP 9.14,1, você pode especificar variáveis para a política de bucket no campo **Resources**. Essas variáveis são marcadores de posição que são substituídos por valores contextuais quando a política é avaliada. Por exemplo, se `${aws:username}` for especificado como uma variável para uma política, essa variável será substituída pelo nome de usuário do contexto de solicitação e a ação da política pode ser executada como configurada para esse usuário.

CLI

Passos

1. Adicione uma instrução a uma política de bucket:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   Os seguintes parâmetros definem permissões de acesso:

`-effect`	A declaração pode permitir ou negar acesso
`-action`	Você pode especificar `*` para indicar todas as ações ou uma lista de uma ou mais das seguintes opções: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` E `ListMultipartUploadParts`.

`-principal`	Uma lista de um ou mais S3 usuários ou grupos. • Um máximo de 10 usuários ou grupos podem ser especificados. • Se um grupo S3 for especificado, ele deverá estar no formulário `group/group_name`. • `*` pode ser especificado para significar acesso público; ou seja, acesso sem uma chave de acesso e chave secreta. • Se nenhum principal for especificado, todos os usuários do S3 na VM de armazenamento terão acesso.
`-resource`	O balde e qualquer objeto que ele contém. Os carateres curinga `*` e `?` podem ser usados para formar uma expressão regular para especificar um recurso. Para um recurso, você pode especificar variáveis em uma política. Estas são variáveis de política são marcadores de posição que são substituídos pelos valores contextuais quando a política é avaliada.

Opcionalmente, você pode especificar uma cadeia de texto como comentário com a `-sid` opção.

Exemplos

O exemplo a seguir cria uma declaração de política de bucket do servidor de armazenamento de objetos para a VM de armazenamento svm1.example.com e bucket1 que especifica o acesso permitido a uma pasta readme para o usuário do servidor de armazenamento de objetos user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

O exemplo a seguir cria uma declaração de política de bucket do servidor de armazenamento de objetos para a VM de armazenamento svm1.example.com e bucket1 que especifica o acesso permitido a todos os objetos para o grupo de servidores de armazenamento de objetos group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partir do ONTAP 9.14,1, você pode especificar variáveis para uma política de bucket. O exemplo a seguir cria uma declaração de política de bucket do servidor para a VM de armazenamento `svm1` e `bucket1` especifica `${aws:username}` como uma variável para um recurso de diretiva. Quando a política é avaliada, a variável de política é substituída pelo nome de usuário de contexto de solicitação e a ação de política pode ser executada como configurada para esse usuário. Por exemplo, quando a seguinte declaração de política é avaliada, `${aws:username}` é substituída pelo usuário que executa a operação S3. Se um usuário `user1` executar a operação, esse usuário terá acesso ao `bucket1` as `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Criar ou modificar uma política de servidor de armazenamento de objetos ONTAP S3

Você pode criar políticas que podem ser aplicadas a um ou mais buckets em um armazenamento de objetos. As políticas de servidor de armazenamento de objetos podem ser anexadas a grupos de usuários, simplificando assim o gerenciamento do acesso a recursos em vários buckets.

Antes de começar

Um SVM habilitado para S3 que contenha um servidor S3 e um bucket já deve existir.

Sobre esta tarefa

É possível habilitar políticas de acesso no nível SVM especificando uma política padrão ou personalizada em um grupo de servidores de storage de objetos. As políticas não entram em vigor até que sejam especificadas na definição de grupo.

> Quando você usa políticas de servidor de armazenamento de objetos, você especifica princípios (ou seja, usuários e grupos) na definição de grupo, não na própria política.

Há três políticas padrão somente leitura para acesso aos recursos do ONTAP S3:

- FullAccess
- NoS3Access
- ReadOnlyAccess

Você também pode criar novas políticas personalizadas, adicionar novas instruções para novos usuários e grupos ou modificar os atributos de instruções existentes. Saiba mais sobre `vserver object-store-server policy` o "Referência do comando ONTAP"na .

A partir do ONTAP 9.9,1, se você planeja oferecer suporte à funcionalidade de marcação de objetos cliente AWS com o servidor ONTAP S3, as ações `GetObjectTagging` `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar ou modificar uma política de servidor de armazenamento de objetos

Passos

1. Edite a VM de armazenamento: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.
2. Adicionar um usuário: Clique em **políticas** e, em seguida, clique em **Adicionar**.
   a. Introduza um nome de política e selecione a partir de uma lista de grupos.
   b. Selecione uma política padrão existente ou adicione uma nova.

      Ao adicionar ou modificar uma política de grupo, você pode especificar os seguintes parâmetros:

      - Grupo: Os grupos a quem o acesso é concedido.
      - Efeito: Permite ou nega o acesso a um ou mais grupos.
      - Ações: Ações permitidas em um ou mais buckets para um determinado grupo.
      - Recursos: Caminhos e nomes de objetos dentro de um ou mais buckets para os quais o acesso é concedido ou negado. Por exemplo:
        - ***** Concede acesso a todos os buckets na VM de armazenamento.
        - **bucketname** e **bucketname/*** concedem acesso a todos os objetos em um bucket específico.
        - **bucketname/readme.txt** concede acesso a um objeto em um intervalo específico.
   c. Se desejar, adicione instruções às políticas existentes.

CLI

Use a CLI para criar ou modificar uma política de servidor de armazenamento de objetos

Passos

1. Criar uma política de servidor de armazenamento de objetos:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Crie uma declaração para a política:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Os seguintes parâmetros definem permissões de acesso:

`-effect`	A declaração pode permitir ou negar acesso

`-action`	Você pode especificar `*` para indicar todas as ações ou uma lista de uma ou mais das seguintes opções: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, E `ListMultipartUploadParts`.
`-resource`	O balde e qualquer objeto que ele contém. Os carateres curinga `*` e `?` podem ser usados para formar uma expressão regular para especificar um recurso.

Opcionalmente, você pode especificar uma cadeia de texto como comentário com a `-sid` opção.

Por padrão, novas instruções são adicionadas ao final da lista de instruções, que são processadas em ordem. Quando você adiciona ou modifica instruções mais tarde, você tem a opção de modificar a configuração da instrução `-index` para alterar a ordem de processamento.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Configurar serviços de diretório externo para acesso ao ONTAP S3

A partir do ONTAP 9.14,1, os serviços para diretórios externos foram integrados ao armazenamento de objetos ONTAP S3. Essa integração simplifica o gerenciamento de usuários e acessos por meio de serviços de diretório externos.

Você pode fornecer grupos de usuários pertencentes a um serviço de diretório externo com acesso ao ambiente de storage de objetos do ONTAP. O LDAP (Lightweight Directory Access Protocol) é uma interface para comunicação com serviços de diretório, como o ative Directory, que fornece um banco de dados e serviços para gerenciamento de identidade e acesso (IAM). Para fornecer acesso, é necessário configurar grupos LDAP no ambiente do ONTAP S3. Depois de configurar o acesso, os membros do grupo têm permissões para buckets do ONTAP S3. Para obter informações sobre LDAP, "Visão geral do uso do LDAP"consulte .

Você também pode configurar grupos de usuários do ative Directory para o modo de vinculação rápida, para que as credenciais de usuário possam ser validadas e aplicativos S3 de terceiros e de código aberto possam ser autenticados por conexões LDAP.

Antes de começar

Antes de configurar grupos LDAP e ativar o modo de ligação rápida para acesso a grupos, certifique-se de que o seguinte é:

1. Uma VM de armazenamento habilitada para S3 contendo um servidor S3 foi criada. "Criar um SVM para S3"Consulte .
2. Um bucket foi criado nessa VM de storage. "Crie um bucket"Consulte .
3. O DNS está configurado na VM de armazenamento. "Configurar serviços DNS"Consulte .

4. Um certificado de autoridade de certificação raiz (CA) autoassinado do servidor LDAP é instalado na VM de armazenamento. "Instale o certificado de CA raiz autoassinado no SVM"Consulte .
5. Um cliente LDAP é configurado com TLS habilitado no SVM. "Crie uma configuração de cliente LDAP"Consulte e "Associe a configuração do cliente LDAP a SVMs para obter informações".

Configurar o acesso S3 para serviços de diretório externo

1. Especifique LDAP como o banco de dados *name Service* do SVM para o grupo e a senha para LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Crie uma declaração de política de bucket do armazenamento de objetos com o `principal` conjunto para o grupo LDAP ao qual você deseja conceder acesso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Exemplo: O exemplo a seguir cria uma declaração de política de bucket para `buck1`. A política permite o acesso do grupo LDAP `group1` ao recurso (bucket e seus objetos `buck1`) .

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verifique se um usuário do grupo LDAP `group1` é capaz de executar operações S3 do cliente S3.

Use o modo LDAP fast bind para autenticação

1. Especifique LDAP como o banco de dados *name Service* do SVM para o grupo e a senha para LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Certifique-se de que um usuário LDAP acessando o bucket do S3 tenha permissões definidas nas políticas de bucket. Para obter mais informações, "Modificar uma política de bucket"consulte .
3. Verifique se um usuário do grupo LDAP pode executar as seguintes operações:
   a. Configure a chave de acesso no cliente S3 neste formato: `"NTAPFASTBIND" + base64-encode(user-name:password)` Exemplo `"NTAPFASTBIND"`: base64-encode(ldapuser:password), o que resulta em `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      O cliente S3 pode pedir uma chave secreta. Na ausência de uma chave secreta, qualquer senha de pelo menos 16 carateres pode ser inserida.

   b. Execute operações S3 básicas do cliente S3 para o qual o usuário tem permissões.

Autenticação de recursos para o ative Directory para usuários sem UID e GID

Se o nasgroup especificado na declaração bucket-policy ou os usuários que fazem parte do nasgroup não tiverem UID e GID definidos, as pesquisas falharão quando esses atributos não forem encontrados.

Para evitar falhas de pesquisa, o NetApp recomenda o uso de domínios confiáveis para autorização de recursos no formato UPN: Nasgroup/group@trusted_domain.com

Para gerar as chaves de acesso do usuário para usuários de domínio confiáveis quando o LDAP fast bind não é usado

Use o `s3/services/<svm_uuid>/users` endpoint com usuários especificados no formato UPN. Exemplo:

```
$curl -siku FQDN\\user:<user_name> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn](https://github.com/fqdn)>,"<key_time_to_live>":"PT6H3M
"}'
```

Habilite os usuários LDAP ou de domínio para gerar suas próprias chaves de acesso ONTAP S3

A partir do ONTAP 9.14,1, como administrador do ONTAP, você pode criar funções personalizadas e concedê-las a grupos locais ou de domínio ou a grupos LDAP (Lightweight Directory Access Protocol), de modo que os usuários pertencentes a esses grupos possam gerar seu próprio acesso e chaves secretas para acesso ao cliente S3.

Você precisa executar algumas etapas de configuração em sua VM de armazenamento, para que a função personalizada possa ser criada e atribuída ao usuário que invoca a API para geração de chaves de acesso.

Antes de começar

Certifique-se de que:

1. Uma VM de armazenamento habilitada para S3 contendo um servidor S3 foi criada. "Criar um SVM para S3"Consulte .
2. Um bucket foi criado nessa VM de storage. "Crie um bucket"Consulte .
3. O DNS está configurado na VM de armazenamento. "Configurar serviços DNS"Consulte .
4. Um certificado de autoridade de certificação raiz (CA) autoassinado do servidor LDAP é instalado na VM de armazenamento. "Instale o certificado de CA raiz autoassinado no SVM"Consulte .
5. Um cliente LDAP é configurado com TLS ativado na VM de armazenamento. "Crie uma configuração de cliente LDAP"Consulte .
6. Associe a configuração do cliente ao SVM. "Associe a configuração do cliente LDAP a SVMs"Consulte . Saiba mais sobre `vserver services name-service ldap create` o "Referência do comando ONTAP"na .
7. Se você estiver usando uma VM de armazenamento de dados, crie uma interface de rede de gerenciamento (LIF) e na VM e também uma política de serviço para o LIF. Saiba mais sobre os[`network interface create`[`network interface service-policy create` comandos em ONTAP.

Configurar usuários para geração de chaves de acesso

1. Especifique LDAP como o banco de dados *name Service* da VM de armazenamento para o grupo e a senha para LDAP:

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Saiba mais sobre `vserver services name-service ns-switch modify` o "Referência do comando ONTAP"na .

2. Criar uma função personalizada com acesso ao endpoint da API REST do usuário S3: `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>` Neste exemplo, a `s3-role` função é gerada para usuários na VM de armazenamento `svm-1` , à qual todos os direitos de acesso, leitura, criação e atualização são concedidos.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

   Saiba mais sobre `security login rest-role create` o "Referência do comando ONTAP"na .

3. Crie um grupo de usuários LDAP com o comando de login de segurança e adicione a nova função personalizada para acessar o endpoint da API REST do usuário S3. Saiba mais sobre `security login`

`create` o "Referência do comando ONTAP"na .

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

Neste exemplo, o grupo LDAP `ldap-group-1` é criado no `svm-1`, e a função personalizada `s3role` é adicionada a ele para acessar o endpoint da API, juntamente com a habilitação do acesso LDAP no modo de vinculação rápida.

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Para obter mais informações, "Use LDAP fast bind para autenticação nsswitch"consulte .

A adição da função personalizada ao domínio ou grupo LDAP permite aos usuários desse grupo um acesso limitado ao endpoint do ONTAP `/api/protocols/s3/services/{svm.uuid}/users`. Ao invocar a API, os usuários do domínio ou grupo LDAP podem gerar seu próprio acesso e chaves secretas para acessar o cliente S3. Eles podem gerar as chaves apenas para si mesmos e não para outros usuários.

Como um usuário S3 ou LDAP, gere suas próprias chaves de acesso

A partir do ONTAP 9.14,1, você pode gerar seu próprio acesso e chaves secretas para acessar clientes S3, se o administrador lhe concedeu a função de gerar suas próprias chaves. Você pode gerar chaves somente para si mesmo usando o seguinte endpoint da API REST do ONTAP.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir. Para obter informações sobre os outros métodos deste endpoint, consulte a "Documentação do API" referência .

Método HTTP	Caminho
POST	/api/protocols/s3/services/(svm.uuid)/users

Curl exemplo

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Exemplo de saída JSON


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```


Ative o acesso do cliente ao armazenamento de objetos S3

Habilite o acesso ao ONTAP S3 para disposição remota de FabricPool em camadas

Para que o ONTAP S3 seja usado como um nível de capacidade remota de FabricPool (nuvem), o administrador do ONTAP S3 deve fornecer informações sobre a configuração do servidor S3 para o administrador remoto do cluster do ONTAP.

Sobre esta tarefa

As seguintes informações do servidor S3 são necessárias para configurar as camadas de nuvem do FabricPool:

- Nome do servidor (FQDN)
- nome do intervalo
- Certificado CA
- chave de acesso
- palavra-passe (chave de acesso secreta)

Além disso, é necessária a seguinte configuração de rede:

- Deve haver uma entrada para o nome do host do servidor ONTAP S3 remoto no servidor DNS configurado para o SVM admin, incluindo o nome FQDN do servidor S3 e os endereços IP em seus LIFs.

- As LIFs de clusters devem ser configuradas no cluster local, embora o peering de cluster não seja necessário.

Consulte a documentação do FabricPool sobre como configurar o ONTAP S3 como uma camada de nuvem.

"Gerenciamento de camadas de storage usando o FabricPool"

Habilite o acesso ao ONTAP S3 para disposição em camadas local do FabricPool

Para que o ONTAP S3 seja usado como uma categoria de capacidade FabricPool local, você precisa definir um armazenamento de objetos com base no bucket criado e anexá-lo a um agregado de categoria de performance para criar um FabricPool.

Antes de começar

Você deve ter o nome do servidor ONTAP S3 e um nome de bucket, e o servidor S3 deve ter sido criado usando LIFs de cluster (com o `-vserver Cluster` parâmetro).

Sobre esta tarefa

A configuração de armazenamento de objetos contém informações sobre o nível de capacidade local, incluindo os nomes de servidor e bucket do S3 e requisitos de autenticação.

Uma configuração de armazenamento de objetos depois de criada não deve ser reatribuída a um repositório de objetos ou bucket diferente. Você pode criar vários buckets para camadas locais, mas não pode criar vários armazenamentos de objetos em um único bucket.

Não é necessária uma licença FabricPool para um nível de capacidade local.

Passos

1. Crie o armazenamento de objetos para o nível de capacidade local:

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - `-container-name`O é o bucket do S3 que você criou.
   - O `-access-key` parâmetro autoriza solicitações ao servidor ONTAP S3.
   - `-secret-password`O parâmetro (chave de acesso secreto) autentica solicitações ao servidor ONTAP S3.
   - Você pode definir o `-is-certificate-validation-enabled` parâmetro como `false` para desativar a verificação de certificados para o ONTAP S3.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Exiba e verifique as informações de configuração do armazenamento de objetos:

   ```
   storage aggregate object-store config show
   ```

3. Opcional: "Determine a quantidade de dados em um volume estão inativos usando relatórios de dados inativos".

   Ver quantos dados em um volume estão inativos pode ajudar você a decidir qual agregado usar para a disposição em camadas local do FabricPool.

4. Anexe o armazenamento de objetos a um agregado:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Você pode usar a `allow-flexgroup` **`true`** opção para anexar agregados que contêm componentes de volume FlexGroup.

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. Exiba as informações do armazenamento de objetos e verifique se o armazenamento de objetos anexado está disponível:

   `storage aggregate object-store show`

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

Ative os aplicativos cliente S3 para acessar um servidor ONTAP S3

Para que os aplicativos cliente S3 acessem o servidor ONTAP S3, o administrador do ONTAP S3 deve fornecer informações de configuração ao usuário S3.

Antes de começar

O aplicativo cliente S3 deve ser capaz de autenticar com o servidor ONTAP S3 usando as seguintes versões de assinatura da AWS:

- Assinatura versão 4, ONTAP 9 .8 e posterior
- Assinatura versão 2, ONTAP 9.11,1 e posterior

Outras versões de assinatura não são suportadas pelo ONTAP S3.

O administrador do ONTAP S3 deve ter criado S3 usuários e concedido permissões de acesso a eles, como usuários individuais ou como membro do grupo, na política de bucket ou na diretiva do servidor de storage de objetos.

O aplicativo cliente S3 deve ser capaz de resolver o nome do servidor ONTAP S3, o que requer que o administrador do ONTAP S3 forneça o nome do servidor S3 (FQDN) e os endereços IP para LIFs do servidor S3.

Sobre esta tarefa

Para acessar um bucket do ONTAP S3, um usuário no aplicativo cliente S3 insere informações fornecidas pelo administrador do ONTAP S3.

A partir do ONTAP 9.9,1, o servidor ONTAP S3 suporta a seguinte funcionalidade de cliente AWS:

- metadados de objetos definidos pelo usuário

  Um conjunto de pares de chave-valor pode ser atribuído a objetos como metadados quando eles são criados usando put (ou POST). Quando uma OPERAÇÃO GET/HEAD é executada no objeto, os metadados definidos pelo usuário são retornados juntamente com os metadados do sistema.

- marcação de objetos

  Um conjunto separado de pares de chave-valor pode ser atribuído como tags para categorizar objetos. Ao contrário dos metadados, as tags são criadas e lidas com APIs REST independentemente do objeto e implementadas quando os objetos são criados ou a qualquer momento depois.

> Para permitir que os clientes obtenham e coloquem informações de marcação, as ações `GetObjectTagging`, `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

Para obter mais informações, consulte a documentação do AWS S3.

Passos

1. Autentique o aplicativo cliente S3 com o servidor ONTAP S3 inserindo o nome do servidor S3 e o certificado da CA.
2. Autentique um usuário no aplicativo cliente S3 inserindo as seguintes informações:
   - Nome do servidor S3 (FQDN) e nome do bucket
   - a chave de acesso e a chave secreta do usuário

Níveis de serviço de storage do ONTAP S3

O ONTAP inclui serviços de storage predefinidos, mapeados para os fatores mínimos de desempenho correspondentes.

O conjunto real de serviços de storage disponíveis em um cluster ou SVM é determinado pelo tipo de storage que compõe o SVM.

A tabela a seguir mostra como os fatores mínimos de desempenho são mapeados para os serviços de storage predefinidos:

Serviço de storage	IOPS esperado (SLA)	IOPS de pico (SLO)	Volume mínimo de IOPS	Latência estimada	As IOPS esperadas são aplicadas?
valor	128 por TB	512 por TB	75	17 ms	No AFF: Sim Caso contrário: Não

Serviço de storage	IOPS esperado (SLA)	IOPS de pico (SLO)	Volume mínimo de IOPS	Latência estimada	As IOPS esperadas são aplicadas?
desempenho	2048 por TB	4096 por TB	500	2 ms	Sim
extremo	6144 por TB	12288 por TB	1000	1 ms	Sim

A tabela a seguir define o nível de serviço de storage disponível para cada tipo de Mídia ou nó:

Mídia ou nó	Nível de serviço de storage disponível
Disco	valor
Disco da máquina virtual	valor
LUN de FlexArray	valor
Híbrida	valor
Flash otimizado para capacidade	valor
Unidade de estado sólido (SSD) - não-AFF	valor
Flash otimizado para desempenho - SSD (AFF)	extremo, desempenho, valor

Configure o compartilhamento de recursos entre origens (CORS) para buckets do ONTAP S3

A partir do ONTAP 9.16,1, você pode configurar o compartilhamento de recursos entre origens (CORS) para permitir que aplicativos da Web clientes de diferentes domínios acessem seus buckets do ONTAP. Isso fornece acesso seguro aos objetos bucket usando um navegador da Web.

CORS é uma estrutura construída em HTTP que permite que scripts definidos em uma página da Web acessem recursos em um servidor em um domínio diferente. O framework é usado para ignorar com segurança a política *same-origin*, que é uma base inicial para a segurança da web. Os principais conceitos e terminologia são descritos abaixo.

Origem

Uma origem define com precisão a localização e a identidade de um recurso. É representado como uma combinação dos seguintes valores:

- Esquema URI (protocolo)
- Nome de host (nome de domínio ou endereço IP)
- Número da porta

Aqui está um exemplo simples de uma origem: `https://www.mycompany.com:8001`. Quando uma origem é usada com o CORS, ele identifica o cliente que faz a solicitação.

Política da mesma origem

A política de mesma origem (SOP) é um conceito de segurança e restrição aplicados a scripts baseados em navegador. A política permite que scripts carregados inicialmente de uma página da Web acessem dados em outra página, desde que ambas as páginas estejam na mesma origem. Esta limitação impede que scripts maliciosos acessem dados nas páginas de uma origem diferente.

Casos comuns de uso de CORS

Existem vários casos de uso geral para CORS. A maioria envolve instâncias bem definidas de acesso entre domínios, como solicitações AJAX, carregamento de fontes, folhas de estilo e scripts, bem como autenticação entre domínios. O CORS também pode ser implementado como parte de um aplicativo de página única (SPA).

Cabeçalhos HTTP

O CORS é implementado usando cabeçalhos que são inseridos nas solicitações e respostas HTTP. Por exemplo, existem vários cabeçalhos de resposta que implementam o controle de acesso e indicam quais operações, incluindo métodos e cabeçalhos, são permitidas. A presença do cabeçalho *origin* em uma solicitação HTTP o define como uma solicitação de domínio cruzado. O valor de origem é usado pelo servidor CORS para localizar uma configuração CORS válida.

Solicitação HTTP preflight

Esta é uma solicitação opcional para determinar inicialmente se um servidor suporta CORS, incluindo os métodos e cabeçalhos específicos. Com base na resposta, a solicitação do CORS pode ser concluída ou não.

Buckets do ONTAP

Um bucket é um contentor de objetos armazenados e acessados com base em um namespace bem definido. Existem dois tipos de buckets do ONTAP:

- Buckets do nas acessíveis pelos protocolos nas e S3
- Buckets do S3 que só são acessíveis através do protocolo S3

Implementação do CORS em ONTAP

O CORS é ativado por padrão com o ONTAP 9.16,1 e versões posteriores. Você precisa configurar o CORS em cada SVM onde ele estará ativo.

> Não há opção administrativa para desativar o CORS para um cluster ONTAP. No entanto, você pode efetivamente desativá-lo não definindo nenhuma regra ou excluindo todas as regras existentes.

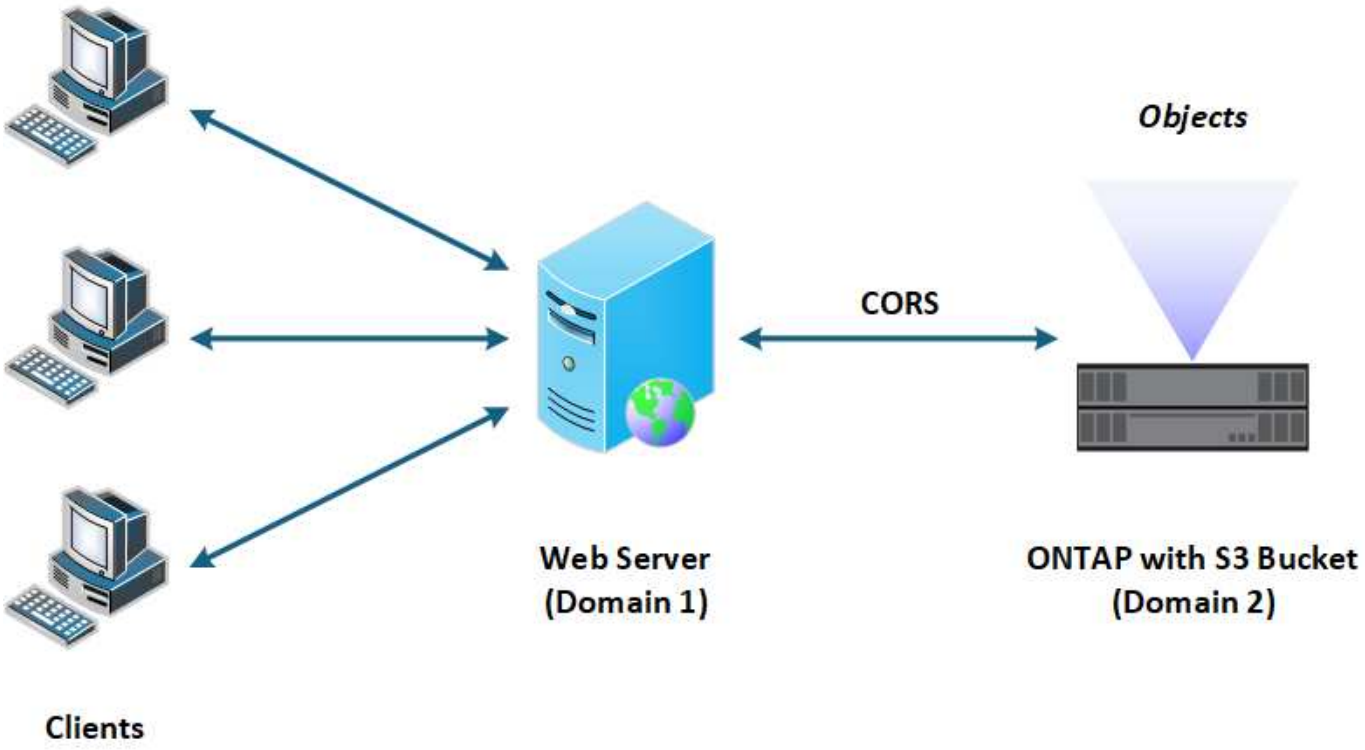
Possíveis casos de uso

A implementação do ONTAP CORS permite várias topologias possíveis para acesso a recursos entre domínios, incluindo:

- Buckets do ONTAP S3 (no mesmo ou diferente SVM ou cluster)
- Buckets do ONTAP nas (no mesmo ou diferente SVM ou cluster)
- Buckets do ONTAP S3 e nas (no mesmo ou diferente SVM ou cluster)
- Buckets do ONTAP e buckets externos de fornecedor
- Baldes em diferentes fusos horários

Vista de alto nível

O seguinte ilustra em alto nível como o CORS permite o acesso aos buckets do ONTAP S3.



Definindo regras CORS

Você precisa definir regras CORS no ONTAP para ativar e usar o recurso.

Ações de configuração

Há três ações principais de regra de configuração suportadas no ONTAP:

- Mostrar
- Criar
- Eliminar

Uma regra CORS definida no ONTAP tem várias propriedades, incluindo o SVM e bucket, bem como as origens, métodos e cabeçalhos permitidos.

Opções de administração

Você tem várias opções disponíveis ao administrar o CORS no cluster do ONTAP.

Interface de linha de comando ONTAP

Você pode configurar o CORS usando a interface de linha de comando. Consulte Administrando CORS usando a CLI para obter mais informações.

API REST do ONTAP

Você pode configurar o CORS usando a API REST do ONTAP. Não foram adicionados novos endpoints para suportar o recurso CORS. Em vez disso, você pode usar o seguinte endpoint existente:

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

Saiba mais no "Documentação de automação do ONTAP".

S3 API

Você pode usar a API S3 para criar e excluir uma configuração CORS em um bucket do ONTAP. Um administrador de cliente S3 requer Privileges suficiente, incluindo:

- Acesso ou credenciais de chave secreta
- Política configurada no bucket para permitir acesso através do s3api

Atualizando e revertendo

Se você planeja usar o CORS para acessar os buckets do ONTAP S3, você deve estar ciente de vários problemas administrativos.

A atualizar

O recurso CORS é suportado quando todos os nós são atualizados para 9.16.1. Em clusters de modo misto, o recurso só estará disponível quando a versão de cluster efetiva (ECV) for 9.16.1 ou posterior.

Reverter

Do ponto de vista do usuário, toda a configuração do CORS deve ser removida antes que a reversão do cluster possa prosseguir. Internamente, a operação excluirá todas as bases de dados CORS. Você será solicitado a executar um comando para limpar e reverter essas estruturas de dados.

Administrando CORS usando a CLI

Você pode usar a CLI do ONTAP para administrar regras do CORS. As operações principais são descritas abaixo. Você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos CORS.

Criar

Você pode definir uma regra CORS usando o `vserver object-store-server bucket cors-rule create` comando.

Parâmetros

Os parâmetros usados para criar uma regra são descritos abaixo.

Parâmetro	Descrição
`vserver`	Especifica o nome do SVM (vserver) que hospeda o bucket do servidor de armazenamento de objetos onde a regra é criada.
`bucket`	O nome do bucket no servidor de armazenamento de objetos para o qual a regra é criada.
`index`	Um parâmetro opcional que indica o índice do bucket do servidor de armazenamento de objetos onde a regra é criada.
`rule id`	Um identificador exclusivo para a regra de bucket do servidor de armazenamento de objetos.
`allowed-origins`	Uma lista das origens das quais os pedidos de origem cruzada são autorizados a ter origem.
`allowed-methods`	Uma lista dos métodos HTTP permitidos em uma solicitação de origem cruzada.
`allowed-headers`	Uma lista dos métodos HTTP permitidos nas solicitações de origem cruzada.
`expose-headers`	Uma lista dos cabeçalhos extras envia nas respostas do CORS que os clientes podem acessar de seus aplicativos.
`max-age-in-seconds`	Um parâmetro opcional especificando a quantidade de tempo que seu navegador deve armazenar em cache uma resposta de pré-voo para um recurso específico.

Exemplo

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

Mostrar

Você pode usar o comando `vserver object-store-server bucket cors-rule show` para exibir uma lista das regras atuais e seu conteúdo.

Incluir o parâmetro `-instance` expande os dados apresentados para cada uma das regras. Você também pode especificar quais campos deseja.

Exemplo

```
server object-store-server bucket cors-rule show -instance
```

Eliminar

Você pode usar o comando delete para remover uma instância de uma regra CORS. Você precisa do `index` valor da regra e, portanto, esta operação é executada em duas etapas:

1. Emita um `show` comando para exibir a regra e recuperar seu índice.
2. Emita a exclusão usando o valor do índice.

Exemplo

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

Modificar

Não há nenhum comando CLI disponível para modificar uma regra CORS existente. Para modificar uma regra, você precisa fazer o seguinte:

1. Exclua a regra existente.
2. Crie uma nova regra com as opções desejadas.

Proteja buckets com o SnapMirror S3

Visão geral do SnapMirror S3

A partir do ONTAP 9.10,1, você pode proteger buckets em armazenamentos de objetos do ONTAP S3 usando a funcionalidade de espelhamento e backup do SnapMirror. Ao contrário do SnapMirror padrão, o SnapMirror S3 permite o espelhamento e os backups para destinos que não sejam NetApp, como o AWS S3.

O SnapMirror S3 é compatível com espelhos ativos e categorias de backup dos buckets do ONTAP S3 nos seguintes destinos:

Alvo	É compatível com espelhos ativos e takeover?	É compatível com backup e restauração?
ONTAP S3 • Buckets no mesmo SVM • Buckets em diferentes SVMs no mesmo cluster • Buckets em SVMs em diferentes clusters	Sim	Sim
StorageGRID	Não	Sim
AWS S3	Não	Sim
Cloud Volumes ONTAP para Azure	Sim	Sim
Cloud Volumes ONTAP para AWS	Sim	Sim

Alvo	É compatível com espelhos ativos e takeover?	É compatível com backup e restauração?
Cloud Volumes ONTAP para Google Cloud	Sim	Sim

Você pode proteger buckets existentes nos servidores do ONTAP S3 ou criar novos buckets com a proteção de dados ativada imediatamente.

Requisitos do SnapMirror S3

- Versão de ONTAP

  O ONTAP 9.10,1 ou posterior deve estar em execução nos clusters de origem e destino.

- Licenciamento

  As seguintes licenças estão disponíveis no "ONTAP One"pacote de software são necessárias em sistemas de origem e destino ONTAP para fornecer acesso a:

  - Protocolo e storage ONTAP S3
  - SnapMirror S3 para segmentar outros destinos de armazenamento de objetos NetApp (ONTAP S3, StorageGRID e Cloud Volumes ONTAP)
  - SnapMirror S3 para segmentar armazenamentos de objetos de terceiros, incluindo AWS S3 (disponível no "Pacote de compatibilidade ONTAP One")

- ONTAP S3
  - Os servidores ONTAP S3 devem estar executando SVMs de origem e destino.
  - Recomenda-se, mas não é necessário, que os certificados de CA para acesso TLS sejam instalados em sistemas que hospedem servidores S3.
    - Os certificados de CA usados para assinar os certificados dos servidores S3 devem ser instalados na VM de armazenamento de administrador dos clusters que hospedam os servidores S3.
    - Você pode usar um certificado de CA autoassinado ou um certificado assinado por um fornecedor de CA externo.
    - Se as VMs de armazenamento de origem ou destino não estiverem escutando em HTTPS, não será necessário instalar certificados de CA.
- Peering (para alvos ONTAP S3)
  - Os LIFs entre clusters devem ser configurados (para destinos ONTAP remotos) e os LIFs entre clusters do cluster de origem e destino podem se conetar às LIFs de dados do servidor S3 de origem e destino.
  - Os clusters de origem e destino são direcionados (para destinos ONTAP remotos).
  - As VMs de armazenamento de origem e destino são direcionadas (para todos os destinos do ONTAP).
- Política de SnapMirror
  - Uma política SnapMirror específica para S3 é necessária para todos os relacionamentos do SnapMirror S3, mas você pode usar a mesma política para vários relacionamentos.
  - Você pode criar sua própria política ou aceitar a política padrão **contínua**, que inclui os seguintes valores:
    - Acelerador (limite superior em taxa de transferência/largura de banda) - ilimitado.

- Tempo para objetivo do ponto de recuperação: 1 hora (3600 segundos).

> Você deve estar ciente de que quando dois buckets do S3 estiverem em um relacionamento do SnapMirror, se houver políticas de ciclo de vida configuradas para que a versão atual de um objeto expire (seja excluída), a mesma ação será replicada para o bucket do parceiro. Isso é verdade mesmo que o intervalo do parceiro seja somente leitura ou passivo.

- Chaves de usuário raiz armazenamento VM chaves de acesso de usuário raiz são necessárias para relacionamentos do SnapMirror S3; o ONTAP não as atribui por padrão. Na primeira vez que você criar uma relação do SnapMirror S3, você deve verificar se as chaves existem nas VMs de armazenamento de origem e destino e regenerá-las se não o fizerem. Se você precisar regenerá-los, você deve garantir que todos os clientes e todas as configurações de armazenamento de objetos do SnapMirror usando o par de chaves secretas e de acesso sejam atualizados com as novas chaves.

Para obter informações sobre a configuração do servidor S3, consulte os seguintes tópicos:

- "Ative um servidor S3 em uma VM de armazenamento"
- "Sobre o processo de configuração do ONTAP S3"

Para obter informações sobre peering de VM de cluster e armazenamento, consulte o seguinte tópico:

- "Prepare-se para espelhamento e cofre (System Manager, passos 1-6)"
- "Peering de cluster e SVM (CLI)"

Relacionamentos SnapMirror compatíveis

O SnapMirror S3 é compatível com relações em fan-out e cascata. Para obter uma visão geral,"Implantações de proteção de dados em cascata e fan-out"consulte .

O SnapMirror S3 não é compatível com implantações fan-in (relacionamentos de proteção de dados entre vários buckets de origem e um único bucket de destino). O SnapMirror S3 é compatível com vários espelhos de bucket de vários clusters para um único cluster secundário, mas cada bucket do origem deve ter seu próprio bucket do destino no cluster secundário.

Controle o acesso aos buckets do S3

Ao criar novos buckets, você pode controlar o acesso criando usuários e grupos. Para obter mais informações, consulte os seguintes tópicos:

- "Adicionar S3 usuários e grupos (System Manager)"
- "Criar um usuário S3 (CLI)"
- "Criar ou modificar S3 grupos (CLI)"

Proteção de espelho e backup em um cluster remoto

Criar uma relação de espelhamento para um novo bucket (cluster remoto)

Ao criar novos buckets do S3, você pode protegê-los imediatamente em um destino do SnapMirror S3 em um cluster remoto.

Sobre esta tarefa

Você precisará executar tarefas em sistemas de origem e destino.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre clusters de origem e destino, e existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma.
2. Edite a VM de storage para adicionar usuários e adicionar usuários a grupos, nas VMs de armazenamento de origem e destino:

   Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. No cluster de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações**- Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Use os padrões (*bucketname, bucketname/**) ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.

d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**. Em seguida, introduza os seguintes valores:

- Destino
  - **ALVO: Sistema ONTAP**
  - **CLUSTER**: Selecione o cluster remoto.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster remoto.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3:** Copie e cole o conteúdo do certificado *destination*.

5. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
6. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
7. Clique em **Salvar**. Um novo bucket é criado na VM de storage de origem e é espelhado em um novo bucket que é criado a VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:

   ```
   vserver object-store-server user show
   ```

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   Não regenere a chave se já existir uma.

2. Crie buckets nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   ```

`[additional_options]`

3. Adicione regras de acesso às políticas de bucket padrão nas SVMs de origem e de destino:

   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. No SVM de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros:

   - Tipo `continuous` - o único tipo de política para relacionamentos SnapMirror S3 (obrigatório).
   - `-rpo` - especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` - especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

     Exemplo

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instalar certificados de servidor CA nas SVMs administrativas dos clusters de origem e destino:

   a. No cluster de origem, instale o certificado da CA que assinou o certificado do servidor *Destination* S3:
      `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. No cluster de destino, instale o certificado da CA que assinou o certificado do servidor *source* S3:
      `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

      Se você estiver usando um certificado assinado por um fornecedor de CA externo, instale o mesmo certificado na SVM do administrador de origem e destino.

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Na fonte SVM, crie uma relação do SnapMirror S3:

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   Você pode usar uma política criada ou aceitar o padrão.

   Exemplo

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
   test-policy
   ```

7. Verifique se o espelhamento está ativo:
   `snapmirror show -policy-type continuous -fields status`

Criar uma relação de espelhamento para um bucket existente (cluster remoto)

Você pode começar a proteger os buckets existentes do S3 a qualquer momento; por exemplo, se você atualizou uma configuração do S3 de uma versão anterior ao ONTAP 9.10,1.

Sobre esta tarefa

Você precisa executar tarefas nos clusters de origem e destino.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre clusters de origem e destino, e existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

Passos

Você pode criar uma relação de espelhamento usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Selecione **Storage > Storage VMs** e, em seguida, selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key.** Não regenere a chave se já existir uma.
2. Verifique se os usuários e grupos existentes estão presentes e têm o acesso correto nas VMs de armazenamento de origem e destino: Selecione **armazenamento > VMs de armazenamento** e, em seguida, selecione a VM de armazenamento e, em seguida, a guia **Configurações**. Por fim, localize o bloco **S3**, selecione e selecione a guia **usuários** e, em seguida, a guia **grupos** para exibir as configurações de acesso de usuário e grupo.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. No cluster de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Selecione **proteção > Visão geral** e clique em **Configurações de política local**.
   b. Selecione ao lado de **políticas de proteção** e clique em **Adicionar**.
   c. Introduza o nome e a descrição da política.
   d. Selecione o escopo da política, cluster ou SVM.
   e. Selecione **contínuo** para relações SnapMirror S3.
   f. Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Verifique se a política de acesso ao bucket do bucket existente ainda atende às suas necessidades:
   a. Clique em **armazenamento > baldes** e, em seguida, selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal e efeito**: Selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações**: Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos**: Use os padrões (*bucketname, bucketname/**) ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Proteja um balde existente com proteção SnapMirror S3:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.
   b. Clique em **Protect** e insira os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster remoto.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster remoto.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *destination*.

6. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
7. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
8. Clique em **Salvar**. O bucket existente é espelhado em um novo bucket na VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se esta for a primeira relação do SnapMirror S3 para este SVM, verifique se existem chaves de usuário raiz para SVMs de origem e de destino e regenere-as se não o fizerem:
   `vserver object-store-server user show` Se não houver, digite:
   `vserver object-store-server user regenerate-keys -vserver` *`svm_name`* `-user` *`root`* Não regenere a chave se já existir.
2. Crie um bucket no SVM de destino para ser o destino espelhado:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Verifique se as regras de acesso das políticas de bucket padrão estão corretas nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

Exemplo

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. No SVM de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros:

   - `continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório).
   - `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Instalar certificados de CA nas SVMs administrativas dos clusters de origem e destino:
   a. No cluster de origem, instale o certificado da CA que assinou o certificado do servidor *Destination* S3:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`
   b. No cluster de destino, instale o certificado da CA que assinou o certificado do servidor *source* S3:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` Se você estiver usando um certificado assinado por um fornecedor de CA externo, instale o mesmo certificado no SVM do administrador de origem e destino.

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Na fonte SVM, crie uma relação do SnapMirror S3:

   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Você pode usar uma política criada ou aceitar o padrão.

Exemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Takeover e fornecimento de dados do bucket do destino (cluster remoto)

Se os dados em um bucket de origem ficarem indisponíveis, você poderá interromper a relação do SnapMirror para tornar o bucket de destino gravável e começar a fornecer dados.

Sobre esta tarefa

Quando uma operação de aquisição é executada, o bucket de origem é convertido em somente leitura e o bucket de destino original é convertido em leitura-gravação, revertendo assim a relação do SnapMirror S3.

Quando o bucket de origem desativado estiver disponível novamente, o SnapMirror S3 ressincroniza automaticamente o conteúdo dos dois buckets. Não é necessário ressincronizar explicitamente a relação, como é necessário para implantações de volume SnapMirror.

A operação de aquisição deve ser iniciada a partir do cluster remoto.

System Manager

Faça failover do bucket indisponível e comece a fornecer dados:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em , selecione **failover** e, em seguida, clique em **failover**.

CLI

1. Inicie uma operação de failover para o bucket de destino:
`snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verifique o status da operação de failover:
`snapmirror show -fields status`

Exemplo

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

Restaurar um bucket da VM de armazenamento de destino (cluster remoto)

Se os dados em um bucket de origem forem perdidos ou corrompidos, você poderá

preencher novamente os dados restaurando objetos de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O intervalo de destino para a operação de restauração deve ser maior do que o espaço lógico usado do intervalo de destino.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

A operação de restauração deve ser iniciada a partir do cluster remoto.

System Manager

Restaure os dados de cópia de segurança:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
     - Copie e cole o conteúdo do certificado da CA do servidor *destination* S3.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA do servidor *destination* S3.
4. Em **destino**, copie e cole o conteúdo do certificado da CA do servidor *source* S3.
5. Clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

Restaure os baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets bloqueados e restaurá-los conforme necessário.

Você pode restaurar um bucket bloqueado por objeto para um bucket novo ou existente. Você pode selecionar um bucket bloqueado por objeto como destino nos seguintes cenários:

- **Restaurar para um novo bucket**: Quando o bloqueio de objetos está ativado, um bucket pode ser restaurado criando um bucket que também tem o bloqueio de objetos ativado. Ao restaurar um bucket bloqueado, o modo de bloqueio de objetos e o período de retenção do bucket original são replicados. Também pode definir um período de retenção de bloqueio diferente para o novo balde. Este período de retenção é aplicado a objetos não bloqueados de outras fontes.
- **Restaurar para um bucket existente**: Um bucket bloqueado por objeto pode ser restaurado para um bucket existente, desde que o controle de versão e um modo de bloqueio de objeto semelhante estejam ativados no bucket existente. O período de retenção do balde original é mantido.
- **Restaurar bucket não bloqueado**: Mesmo que o bloqueio de objetos não esteja habilitado em um bucket, você pode restaurá-lo para um bucket que tenha o bloqueio de objetos ativado e esteja no cluster de origem. Quando você restaura o bucket, todos os objetos não bloqueados ficam bloqueados e o modo de retenção e a posse do bucket de destino se aplicam a eles.

CLI

1. Crie o novo intervalo de destino para restauração. Para obter mais informações, "Criar um relacionamento de backup para um novo bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*

Exemplo

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

Proteção de espelho e backup no cluster local

Criar uma relação de espelho para um novo bucket (cluster local)

Ao criar novos buckets do S3, você pode protegê-los imediatamente para um destino do SnapMirror S3 no mesmo cluster. É possível espelhar dados em um bucket em uma VM de storage diferente ou na mesma VM de storage que a origem.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Configurações**, clique no bloco S3.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma.
2. Edite a VM de armazenamento para adicionar usuários e adicionar usuários a grupos, tanto nas VMs de armazenamento de origem quanto de destino: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e depois em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Use os padrões `(bucketname, bucketname/*)` ou outros valores que você precisa

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
   d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**. Em seguida, introduza os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster local.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster local.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado de origem.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado de destino.

5. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
6. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
7. Clique em **Salvar**. Um novo bucket é criado na VM de storage de origem e é espelhado em um novo bucket que é criado a VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:
   `vserver object-store-server user show`

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Não regenere a chave se já existir uma.

2. Crie buckets nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Adicione regras de acesso às políticas de bucket padrão nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   ```

`-principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros:

   - `continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório).
   - `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Instalar certificados de servidor da CA no SVM do administrador:
   a. Instale o certificado da CA que assinou o certificado do servidor *source* S3 no SVM do administrador:
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`
   b. Instale o certificado da CA que assinou o certificado do servidor *destino* S3 no SVM admin:
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate` Se você estiver usando um certificado assinado por um fornecedor externo de CA, você só precisará instalar esse certificado no SVM do administrador.

      Consulte a `security certificate install` página de manual para obter detalhes.

6. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Você pode usar uma política criada ou aceitar o padrão.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

7. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Criar uma relação de espelhamento para um bucket existente (cluster local)

Você pode começar a proteger buckets S3 existentes no mesmo cluster a qualquer momento; por exemplo, se você atualizou uma configuração S3 de uma versão anterior ao ONTAP 9.10,1. É possível espelhar dados em um bucket em uma VM de storage diferente ou na mesma VM de storage que a origem.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma
2. Verifique se os usuários e grupos existentes estão presentes e têm o acesso correto nas VMs de armazenamento de origem e destino: Selecione **armazenamento > VMs de armazenamento** e, em seguida, selecione a VM de armazenamento e, em seguida, a guia **Configurações**. Por fim, localize o bloco **S3**, selecione e selecione a guia **usuários** e, em seguida, a guia **grupos** para exibir as configurações de acesso de usuário e grupo.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configuração de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Verifique se a política de acesso ao bucket do bucket existente continua atendendo às suas necessidades:
   a. Clique em **armazenamento > baldes** e, em seguida, selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Use os padrões *(bucketname, bucketname/*)* ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Proteja um balde existente com o SnapMirror S3:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.

b. Clique em **Protect** e insira os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster local.
  - **STORAGE VM**: Selecione a mesma ou outra VM de armazenamento.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *destination*.

6. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
7. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
8. Clique em **Salvar**. O bucket existente é espelhado em um novo bucket na VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:
   `vserver object-store-server user show`

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Não regenere a chave se já existir uma.

2. Crie um bucket no SVM de destino para ser o destino espelhado:

   `vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. Verifique se as regras de acesso às políticas de bucket padrão estão corretas nas SVMs de origem e de destino:

`vserver object-store-server bucket policy add-statement -vserver *svm_name* -bucket *bucket_name* -effect {allow|deny} -action *object_store_actions* -principal *user_and_group_names* -resource *object_store_resources* [-sid *text*] [-index *integer*]`

Exemplo

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:

   `snapmirror policy create -vserver *svm_name* -policy *policy_name* -type *continuous [-rpo _integer*] [-throttle *throttle_type*] [-comment text] [*additional_options*]`

   Parâmetros:

   - `continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório).
   - `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Instalar certificados de servidor da CA no SVM do administrador:
   a. Instale o certificado da CA que assinou o certificado do servidor *source* S3 no SVM do administrador:
      `security certificate install -type server-ca -vserver *admin_svm* -cert -name *src_server_certificate*`
   b. Instale o certificado da CA que assinou o certificado do servidor *destino* S3 no SVM admin:
      `security certificate install -type server-ca -vserver *admin_svm* -cert -name *dest_server_certificate*` Se você estiver usando um certificado assinado por um fornecedor externo de CA, você só precisará instalar esse certificado no SVM do administrador.

      Consulte a `security certificate install` página de manual para obter detalhes.

6. Criar uma relação do SnapMirror S3:
   `snapmirror create -source-path *src_svm_name*:/bucket/*bucket_name* -destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

Você pode usar uma política criada ou aceitar o padrão.

Exemplo

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Takeover e fornecimento de dados do bucket do destino (cluster local)

Se os dados em um bucket de origem ficarem indisponíveis, você poderá interromper a relação do SnapMirror para tornar o bucket de destino gravável e começar a fornecer dados.

Sobre esta tarefa

Quando uma operação de aquisição é executada, o bucket de origem é convertido em somente leitura e o bucket de destino original é convertido em leitura-gravação, revertendo assim a relação do SnapMirror S3.

Quando o bucket de origem desativado estiver disponível novamente, o SnapMirror S3 ressincroniza automaticamente o conteúdo dos dois buckets. Não é necessário ressincronizar explicitamente a relação, como é necessário para implantações padrão de volume SnapMirror.

Se o intervalo de destino estiver em um cluster remoto, a operação de aquisição deve ser iniciada a partir do cluster remoto.

System Manager

Faça failover do bucket indisponível e comece a fornecer dados:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em , selecione **failover** e, em seguida, clique em **failover**.

CLI

1. Inicie uma operação de failover para o bucket de destino:
`snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verifique o status da operação de failover:
`snapmirror show -fields status`

Exemplo

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Restaurar um bucket da VM de armazenamento de destino (cluster local)

Quando os dados em um bucket de origem são perdidos ou corrompidos, você pode

preencher novamente seus dados restaurando objetos de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O intervalo de destino para a operação de restauração deve ser maior que o intervalo de destino;s espaço lógico usado.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

A operação de restauração deve ser iniciada a partir do cluster local.

System Manager

Restaure os dados de backup:

1. Clique em **proteção > relacionamentos** e, em seguida, selecione o intervalo.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
4. Copie e cole o conteúdo do certificado de CA do servidor S3 de destino.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA de servidor S3 de destino.
5. Em **destino**, copie e cole o conteúdo do certificado de CA do servidor S3 de origem.
6. Clique em **proteção** > relacionamentos para monitorar o progresso da restauração.

Restaure os baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets bloqueados e restaurá-los conforme necessário.

Você pode restaurar um bucket bloqueado por objeto para um bucket novo ou existente. Você pode selecionar um bucket bloqueado por objeto como destino nos seguintes cenários:

- **Restaurar para um novo bucket**: Quando o bloqueio de objetos está ativado, um bucket pode ser restaurado criando um bucket que também tem o bloqueio de objetos ativado. Ao restaurar um bucket bloqueado, o modo de bloqueio de objetos e o período de retenção do bucket original são replicados. Também pode definir um período de retenção de bloqueio diferente para o novo balde. Este período de retenção é aplicado a objetos não bloqueados de outras fontes.
- **Restaurar para um bucket existente**: Um bucket bloqueado por objeto pode ser restaurado para um bucket existente, desde que o controle de versão e um modo de bloqueio de objeto semelhante estejam ativados no bucket existente. O período de retenção do balde original é mantido.
- **Restaurar bucket não bloqueado**: Mesmo que o bloqueio de objetos não esteja habilitado em um bucket, você pode restaurá-lo para um bucket que tenha o bloqueio de objetos ativado e esteja no cluster de origem. Quando você restaura o bucket, todos os objetos não bloqueados ficam bloqueados e o modo de retenção e a posse do bucket de destino se aplicam a eles.

CLI

1. Se você estiver restaurando objetos para um novo bucket, crie o novo bucket. Para obter mais informações, "Criar um relacionamento de backup para um novo bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

Exemplo

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

Proteção de backup com destinos em nuvem

Requisitos para relacionamentos de destino na nuvem

Certifique-se de que seus ambientes de origem e destino atendam aos requisitos de proteção de backup do SnapMirror S3 para destinos na nuvem.

Você deve ter credenciais de conta válidas com o provedor de armazenamento de objetos para acessar o intervalo de dados.

LIFs entre clusters e um espaço IPspace devem ser configurados no cluster antes que o cluster possa se conetar a um armazenamento de objetos em nuvem. Você deve criar LIFs entre clusters em cada nó para transferir dados de forma otimizada do storage local para o armazenamento de objetos em nuvem.

Para alvos StorageGRID, você precisa saber as seguintes informações:

- Nome do servidor, expresso como um nome de domínio totalmente qualificado (FQDN) ou endereço IP
- nome do bucket; o bucket já deve existir
- chave de acesso
- chave secreta

Além disso, o certificado da CA usado para assinar o certificado do servidor StorageGRID precisa ser instalado na VM de armazenamento de administrador do cluster do ONTAP S3 usando o `security certificate install command`. Para obter mais informações, consulte "Instalando um certificado CA" se você usa o StorageGRID.

Para os destinos do AWS S3, você precisa saber as seguintes informações:

- Nome do servidor, expresso como um nome de domínio totalmente qualificado (FQDN) ou endereço IP
- nome do bucket; o bucket já deve existir
- chave de acesso
- chave secreta

O servidor DNS para a VM de armazenamento de administrador do cluster ONTAP deve ser capaz de resolver FQDNs (se usado) para endereços IP.

Criar um relacionamento de backup para um novo bucket (destino na nuvem)

Ao criar novos buckets do S3, você pode fazer backup deles imediatamente em um bucket de destino do SnapMirror S3 em um provedor de armazenamento de objetos, que pode ser um sistema StorageGRID ou uma implantação do Amazon S3.

Antes de começar

- Você tem credenciais de conta válidas e informações de configuração para o provedor de armazenamento de objetos.
- Interfaces de rede entre clusters e um IPspace foram configurados no sistema de origem.
- • A configuração DNS para a VM de armazenamento de origem deve ser capaz de resolver o FQDN do destino.

System Manager

1. Edite a VM de armazenamento para adicionar usuários e para adicionar usuários a grupos:
   a. Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em **S3**.

      Consulte "Adicione S3 usuários e grupos" para obter mais informações.

2. Adicione um Cloud Object Store no sistema de origem:
   a. Clique em **proteção > Visão geral** e selecione **Cloud Object Stores**.
   b. Clique em **Adicionar** e selecione **Amazon S3** ou **StorageGRID**.
   c. Introduza os seguintes valores:
      - Nome do armazenamento de objetos na nuvem
      - Estilo de URL (caminho ou virtual-hospedado)
      - VM de armazenamento (ativada para S3)
      - Nome do servidor de armazenamento de objetos (FQDN)
      - Certificado de armazenamento de objetos
      - Chave de acesso
      - Chave secreta
      - Nome do recipiente (balde)
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique → ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
        bjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
        ```

      - **Recursos** - Use os padrões `_(bucketname, bucketname/*)` ou outros valores que você

precisa.

Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.

d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**, selecione **armazenamento em nuvem** e, em seguida, selecione **armazenamento de objetos em nuvem**.

Quando você clica em **Salvar**, um novo bucket é criado na VM de armazenamento de origem e é feito o backup no armazenamento de objetos na nuvem.

CLI

1. Se esta for a primeira relação do SnapMirror S3 para este SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e regenere-as se não o fizerem:
`vserver object-store-server user show` Confirme que há uma chave de acesso para o usuário raiz. Se não houver, digite:
`vserver object-store-server user regenerate-keys -vserver svm_name -user root` Não regenere a chave se já existir.
2. Crie um bucket no SVM de origem:
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. Adicione regras de acesso à política de bucket padrão:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros: * `type continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório). * `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional). * `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

Exemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. Se o destino for um sistema StorageGRID, instale o certificado do servidor da CA StorageGRID no SVM admin do cluster de origem:
`security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Defina o armazenamento de objetos de destino do SnapMirror S3:
`snapmirror object-store config create -vserver` *`svm_name`* `-object-store-name` *`target_store_name`* `-usage data -provider-type {AWS_S3|SGWS} -server` *`target_FQDN`* `-container-name` *`remote_bucket_name`* `-is-ssl-enabled true -port` *`port_number`* `-access-key target_access_key -secret-password` *`target_secret_key`*

   Parâmetros: * `-object-store-name` – O nome do alvo do armazenamento de objetos no sistema ONTAP local. * `-usage` – use `data` para este fluxo de trabalho. * `-provider-type` – `AWS_S3` E `SGWS` (StorageGRID) alvos são suportados. `-server`* – O FQDN ou endereço IP do servidor de destino. * `-is-ssl-enabled` –Ativar SSL é opcional, mas recomendado. Veja a `snapmirror object-store config create` página de manual para mais detalhes.

   Exemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

   Parâmetros: * `-destination-path` - O nome do armazenamento de objetos que você criou na etapa anterior e o valor fixo `objstore` . Você pode usar uma política que você criou ou aceitar o padrão.

   Exemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Criar um relacionamento de backup para um bucket existente (destino na nuvem)

Você pode começar a fazer backup de buckets S3 existentes a qualquer momento; por exemplo, se você atualizou uma configuração S3 de uma versão anterior ao ONTAP 9.10,1.

Antes de começar

- Você tem credenciais de conta válidas e informações de configuração para o provedor de armazenamento de objetos.
- Interfaces de rede entre clusters e um IPspace foram configurados no sistema de origem.
- A configuração DNS para a VM de armazenamento de origem deve ser capaz de resolver o FQDN do destino.

System Manager

1. Verifique se os usuários e grupos estão definidos corretamente: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em abaixo de S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.

2. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
   c. Introduza o nome e a descrição da política.
   d. Selecione o escopo da política, o cluster ou o SVM
   e. Selecione **contínuo** para relações SnapMirror S3.
   f. Insira os valores de objetivo **Throttle** e **ponto de recuperação**.
3. Adicione um Cloud Object Store no sistema de origem:
   a. Clique em **proteção > Visão geral** e selecione **Cloud Object Store**.
   b. Clique em **Adicionar** e selecione **Amazon S3** ou **outros** para o StorageGRID Webscale.
   c. Introduza os seguintes valores:
      - Nome do armazenamento de objetos na nuvem
      - Estilo de URL (caminho ou virtual-hospedado)
      - VM de armazenamento (ativada para S3)
      - Nome do servidor de armazenamento de objetos (FQDN)
      - Certificado de armazenamento de objetos
      - Chave de acesso
      - Chave secreta
      - Nome do recipiente (balde)
4. Verifique se a política de acesso ao bucket do bucket existente ainda atende às suas necessidades:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Recursos** - Use os padrões *`(bucketname, bucketname/*)`* ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Faça backup do balde usando o SnapMirror S3:

a. Clique em **Storage** > **Buckets** e selecione o bucket que deseja fazer backup.

b. Clique em **Protect**, selecione **Cloud Storage** em **Target** e, em seguida, selecione **Cloud Object Store**.

Quando você clica em **Salvar**, o bucket existente é feito o backup no armazenamento de objetos na nuvem.

CLI

1. Verifique se as regras de acesso na política de bucket padrão estão corretas:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros: * `type continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório). * `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional). * `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. Se o destino for um sistema StorageGRID, instale o certificado da CA StorageGRID no SVM de administrador do cluster de origem:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Consulte a `security certificate install` página de manual para obter detalhes.

4. Defina o armazenamento de objetos de destino do SnapMirror S3:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password`

target_secret_key

Parâmetros: * `-object-store-name` – O nome do alvo do armazenamento de objetos no sistema ONTAP local. * `-usage` – use `data` para este fluxo de trabalho. * `-provider-type` – `AWS_S3` E `SGWS` (StorageGRID) alvos são suportados. `-server`* – O FQDN ou endereço IP do servidor de destino. * `-is-ssl-enabled` –Ativar SSL é opcional, mas recomendado. Veja a `snapmirror object-store config create` página de manual para mais detalhes.

Exemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

   Parâmetros: * `-destination-path` - O nome do armazenamento de objetos que você criou na etapa anterior e o valor fixo `objstore` . Você pode usar uma política que você criou ou aceitar o padrão.

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
   -destination-path sgws-store:/objstore -policy test-policy
   ```

6. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Restaurar um bucket do destino na nuvem

Quando os dados em um bucket de origem são perdidos ou corrompidos, você pode preencher novamente seus dados restaurando de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O bucket de destino para a operação de restauração deve ser maior que o espaço lógico usado do bucket de destino.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

System Manager

Restaure os dados de backup:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
     - Copie e cole o conteúdo do certificado da CA do servidor *destination* S3.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA de servidor S3 de destino.
4. Em **destino**, copie e cole o conteúdo do certificado da CA do servidor *source* S3.
5. Clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

Procedimento CLI

1. Crie o novo intervalo de destino para restauração. Para obter mais informações, "Criar um relacionamento de backup para um bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   Exemplo

   O exemplo a seguir restaura um bucket de destino para um bucket existente.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

Modificar uma política de espelho

Você pode querer modificar uma política de espelhamento do S3; por exemplo, se quiser ajustar os valores de RPO e acelerador.

System Manager

Se você quiser ajustar esses valores, você pode editar uma política de proteção existente.

1. Clique em **proteção > relacionamentos** e, em seguida, selecione a política de proteção para o relacionamento que deseja modificar.
2. Clique ⋮ ao lado do nome da política e, em seguida, clique em **Editar**.

CLI

Modificar uma política do SnapMirror S3:
`snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer] [-throttle throttle_type] [-comment text]`

Parâmetros:

- `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos.
- `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Proteger dados do S3 com snapshots

Visão geral do instantâneo do S3

A partir do ONTAP 9.16,1, você pode usar a tecnologia de snapshot do ONTAP para gerar imagens pontuais e somente leitura dos buckets do ONTAP S3.

Usando o recurso snapshots S3, você pode criar snapshots manualmente ou gerá-los automaticamente por meio de políticas de snapshot. Os snapshots S3 são apresentados como buckets S3 para S3 clientes. Você pode navegar e restaurar o conteúdo dos instantâneos através de clientes S3.

No ONTAP 9.16,1, os snapshots S3 capturam apenas as versões atuais dos objetos em buckets do S3. As versões não atuais dos buckets versionados não são capturadas nos snapshots S3. Além disso, as tags de objeto point-in-time não são capturadas nos snapshots se as tags de objeto forem modificadas após as capturas instantâneas serem tiradas.

S3 snapshots dependem do tempo do cluster. Você deve configurar o servidor NTP no cluster para sincronizar a hora. Para obter mais informações, "Gerenciar o tempo do cluster"consulte .

Uso de cota e espaço

As cotas rastreiam o número de objetos e o tamanho lógico usados em um bucket do S3. Quando são criados instantâneos S3D, os objetos capturados nos instantâneos S3D são contados em direção à contagem e ao tamanho de objetos de bucket usados, até que os instantâneos sejam excluídos do sistema de arquivos.

Objetos multiparte

Para objetos multiparte, apenas os objetos finais são capturados em instantâneos. Uploads parciais de

objetos multipart não são capturados em snapshots.

Snapshots em buckets versionados e não versionados

Você pode criar snapshots em buckets versionados e não versionados. O instantâneo contém apenas as versões atuais do objeto em um momento em que o instantâneo é capturado.

Buckets e snapshots versionados

Em buckets com o controle de versão de objeto habilitado, um snapshot retém o conteúdo da versão de objeto mais recente após a qual o snapshot foi capturado. Exclui versões não atuais no balde.

Considere este exemplo: Em um bucket onde o controle de versão do objeto está habilitado, o objeto `obj1` tem as versões v1, v2, v3, v4, v5. Você criou um instantâneo `snap1` a partir `obj1` de v3 (a versão mais recente no ponto de captura). Ao navegar `snap1`, `obj1` aparecerá como um objeto com conteúdo criado em v3. O conteúdo das versões anteriores não será devolvido.

> As versões não atuais são mantidas no sistema de arquivos, até que os snapshots sejam excluídos.

Buckets e snapshots não versionados

Em buckets não versionados, os snapshots S3 preservam o conteúdo dos commits mais recentes antes da criação do snapshot.

Considere este exemplo: Em um bucket onde o controle de versão de objetos não está disponível, o objeto `obj1` foi substituído várias vezes em (T1, T2, T3, T4 e T5). Você criou um snapshot S3 `snap1` em algum momento entre T3 e T4. Ao navegar `snap1`, `obj1` aparecerá com o conteúdo criado em T3.

Expiração de objetos e snapshots

A expiração de objetos do ONTAP S3 e os snapshots S3 funcionam independentemente um do outro. O recurso de expiração de objeto do ONTAP expira as versões de objeto de acordo com as regras de gerenciamento de ciclo de vida definidas para o bucket do S3. Os snapshots S3 são cópias estáticas dos objetos bucket em um momento em que o snapshot é criado.

Se o controle de versão do objeto estiver habilitado em um bucket, quando uma versão específica de um objeto for excluída devido a uma regra de expiração definida para esse bucket, o conteúdo da versão expirada do objeto continuará a permanecer no sistema de arquivos se a versão tiver sido capturada como uma versão atual em um ou mais snapshots S3. Essa versão do objeto deixará de existir no sistema de arquivos somente quando esse snapshot for excluído.

Da mesma forma, em um intervalo no qual o controle de versão é desativado, se um objeto é excluído com base em uma regra de expiração, mas o objeto ainda é capturado em alguns snapshots S3 existentes, o objeto será retido no sistema de arquivos. O objeto será removido permanentemente do sistema de arquivos quando os snapshots que capturam forem excluídos.

Para obter informações sobre a expiração do objeto S3 e o gerenciamento do ciclo de vida, "Crie uma regra de gerenciamento do ciclo de vida do bucket"consulte .

Limitações com S3 instantâneos

Observe as seguintes exclusões e cenários de recursos no ONTAP 9.16,1:

- Você pode gerar até 1023 snapshots para um bucket do S3.

- É necessário excluir todos os snapshots e metadados do S3 de todos os buckets em um cluster antes de reverter o cluster para uma versão do ONTAP anterior ao ONTAP 9.16,1.
- Se você precisar excluir um bucket do S3 contendo objetos com snapshots, verifique se você excluiu todos os snapshots correspondentes de todos os objetos nesse bucket.
- S3 snapshots não são suportados nessas configurações:
  - Em buckets em um relacionamento com o SnapMirror
  - Em buckets onde o bloqueio de objetos está ativado
  - No NetApp BlueXP
  - No System Manager
  - Nas configurações do ONTAP MetroCluster

Crie instantâneos S3D.

Você pode gerar snapshots S3 manualmente ou configurar políticas de snapshot para criar snapshots S3 automaticamente para você. Os snapshots servem como cópias estáticas de objetos que você usa para backup e recuperação de dados. Para determinar a duração da retenção de snapshot, você pode criar políticas de snapshot que facilitem a criação automática de snapshot em intervalos especificados.

Os snapshots S3 ajudam a proteger os dados de objetos em buckets do S3 com ou sem o controle de versão de objetos ativado.

Os snapshots podem ser especialmente úteis no estabelecimento da proteção de dados quando o controle de versão de objetos não está habilitado em um bucket do S3, porque atuam como Registros pontuais que podem ser usados para operações de restauração quando uma versão de objeto anterior não está disponível.

Sobre esta tarefa

- As seguintes regras de nomenclatura aplicam-se ao instantâneo (para instantâneos manuais e automáticos):
  - Os nomes de instantâneos S3 podem ter até 30 carateres
  - S3 os nomes de instantâneos podem consistir apenas em letras minúsculas, números, pontos (.) e hífens (-)
  - Os nomes de instantâneos S3 devem terminar com uma letra ou um número
  - Os nomes de instantâneos S3 não podem conter subcadeia de carateres `s3snap`
- No contexto do protocolo S3, as restrições de nomes de buckets limitam um nome de bucket a 63 carateres. Como os snapshots do ONTAP S3 são apresentados como buckets por meio do protocolo S3, restrições semelhantes se aplicam aos nomes dos buckets do snapshot. Por padrão, o nome do bucket original é usado como o nome do bucket base.
- Para facilitar a identificação de qual snapshot pertence a qual bucket, o nome do bucket do snapshot consiste no nome do bucket base, juntamente com uma string especial, `-s3snap-` que é prefixada ao nome do snapshot. Os nomes do bucket do instantâneo são formatados como `<base_bucket_name>-s3snap-<snapshot_name>`.

  Por exemplo, executar o comando a seguir para criar `snap1` no `bucket-a` cria um bucket de snapshot com nome `bucket-a-s3snap-snap1`, que pode ser acessado por meio de clientes S3 se você tiver

permissões para acessar o bucket base.

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- Não é possível criar um instantâneo que resulte em um nome de intervalo de instantâneo com mais de 63 carateres.
- O nome do instantâneo automático contém o nome do agendamento da política e o carimbo de data/hora, que é semelhante à convenção de nomenclatura para os instantâneos de volume tradicionais. Por exemplo, os nomes de instantâneos programados podem ser `daily-2024-01-01-0015` e `hourly-2024-05-22-1105`.

Crie manualmente S3 instantâneos

Você pode criar manualmente um snapshot S3 usando a CLI do ONTAP. O procedimento cria um instantâneo apenas no cluster local.

Passos

1. Criar um instantâneo S3D:

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

O exemplo a seguir cria um snapshot nomeado `pre-update` na `vs0` VM e bucket do storage `website-data`:

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

Atribua uma política de snapshot S3 a um bucket

Quando você configura políticas de snapshot no nível do bucket do S3, o ONTAP cria snapshots S3 programados para você automaticamente. Como as políticas de snapshot tradicionais, até cinco programações podem ser configuradas para snapshots S3.

Uma política de snapshot normalmente especifica as agendas para criar snapshots, o número de cópias a reter para cada agendamento e o prefixo de agendamento. Por exemplo, uma política pode criar um snapshot S3 todos os dias às 12:10 AM, reter as duas cópias mais recentes e nomeá-las `daily-<timestamp>`.

A política de snapshot padrão preserva:

- Seis snapshots por hora
- Dois instantâneos diários
- Dois instantâneos semanais

Antes de começar

- Uma política de snapshot deve ter sido criada antes de atribuí-la ao bucket S3.

> As políticas para snapshots S3 seguem as mesmas regras que outras políticas de snapshot do ONTAP. No entanto, uma política de snapshot com um período de retenção configurado em qualquer uma das programações de snapshot não pode ser atribuída a um bucket do S3.

Para obter mais informações sobre a criação de políticas de snapshot para geração automática de snapshots, "Configure a visão geral das políticas de snapshot personalizadas"consulte .

Passos

1. Atribua a política de snapshot no bucket:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

ou

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

> Se for necessário reverter um cluster para uma versão do ONTAP anterior ao ONTAP 9.16,1, verifique se o valor para `snapshot-policy` todos os buckets está definido como `none` (ou `-`).

Informações relacionadas

"Visão geral do instantâneo do S3"

Visualizar e restaurar snapshots S3

O recurso de snapshot do ONTAP S3 permite exibir e navegar o conteúdo de snapshot do S3 para seus buckets de clientes do S3. Além disso, você pode restaurar um único objeto, um conjunto de objetos ou um bucket inteiro em um cliente S3 a partir de um snapshot S3.

Antes de começar

Para visualizar, navegar e restaurar instantâneos do ONTAP S3 nos seus buckets, os instantâneos devem ter sido criados e o bucket base do S3 deve estar acessível a você por meio do cliente de protocolo S3.

Liste e e visualize instantâneos S3D.

Você pode visualizar os detalhes do snapshot do S3, compará-los e identificar erros. Usando a CLI do ONTAP, você pode listar todos os snapshots criados nos buckets do S3.

Passos

1. Listar S3 instantâneos:

```
vserver object-store-server bucket snapshot show
```

É possível visualizar os nomes dos snapshots, as VMs de storage, os buckets, o tempo de criação e `instance-uuid` os snapshots do S3 criados para todos os buckets no cluster.

2. Você também pode especificar um nome de bucket para exibir os nomes, o tempo de criação e `instance-uuid` todos os snapshots S3 criados para esse bucket específico.

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

PESQUISE conteúdo de instantâneos S3

Se você notar falhas ou problemas no seu ambiente, poderá navegar pelo conteúdo dos snapshots do bucket do S3 para identificar os erros. Você também pode navegar nos snapshots S3 para determinar o conteúdo livre de erros a ser restaurado.

Os snapshots S3 são apresentados como buckets de snapshot para os clientes S3. O nome do bucket do instantâneo é formatado como `<base_bucket_name>-s3snap-<snapshot_name>`. Você pode ver todos os buckets de snapshot em uma VM de storage usando a `ListBuckets` operação da API S3.

O bucket do snapshot S3 herda as políticas de acesso do bucket base e dá suporte apenas a operações somente leitura. Se você tiver permissões para acessar o bucket base, também poderá executar operações de API S3D somente leitura no bucket do snapshot S3, como `HeadObject` `GetObject` , , `GetObjectTagging` `ListObjects` , , , `ListObjectVersions`, `GetObjectAcl`, e `CopyObject`.

> ⓘ A `CopyObject` operação é suportada em um bucket de instantâneos do S3 somente se for uma cópia instantânea do bucket de origem, e não se for o destino de armazenamento do snapshot.

Para obter mais informações sobre essas operações, "Ações compatíveis com o ONTAP S3"consulte .

Restaure o conteúdo de snapshots S3

Você pode executar uma operação de restauração em um cliente S3 para recuperar um único objeto, um conjunto de objetos ou um bucket inteiro copiando o conteúdo de um bucket de snapshot para o bucket original ou diferente. Você pode procurar instantâneos para determinar qual conteúdo de snapshot você deve copiar.

Você restaura todo o bucket, objetos com um prefixo ou um único objeto usando o `aws s3 cp` comando.

Passos

1. Tire um instantâneo do balde base S3.

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. Restaure o bucket da base usando o snapshot:
   - Restaure um balde inteiro. Use o nome do bucket do instantâneo no formato `<base_bucket_name>-s3snap-<snapshot_name>`.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

   - Restaure objetos em um diretório com o prefixo `dir1`:

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

   - Restaurar um único objeto chamado `web.py`:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

Eliminar S3 instantâneos

Você pode excluir snapshots S3 que não precisam mais e liberar espaço de armazenamento em seus buckets. Você pode remover manualmente snapshots S3 ou modificar as políticas de snapshot anexadas aos buckets do S3 para alterar o número de snapshots a serem retidos para um agendamento.

As políticas de snapshot para buckets do S3 seguem as mesmas regras de exclusão das políticas tradicionais de snapshot do ONTAP. Para obter mais informações sobre como criar políticas de snapshot, "Criar uma política de snapshot"consulte .

Sobre esta tarefa

- Se uma versão de objeto (em um bucket versionado) ou um objeto (em um bucket não versionado) for capturada em vários snapshots, o objeto será removido do sistema de arquivos somente após o último snapshot protegendo-o ser excluído.
- Se você precisar excluir um bucket do S3 contendo objetos com snapshots, verifique se você excluiu todos os snapshots de todos os objetos nesse bucket.
- Se você precisar reverter um cluster para uma versão do ONTAP anterior ao ONTAP 9.16,1, certifique-se de excluir todos os snapshots do S3 para todos os buckets. Você também pode precisar executar o `vserver object-store-server bucket clear-snapshot-metadata` comando para remover os metadados de snapshot de um bucket do S3. Para obter informações, "Limpar metadados de instantâneos do S3"consulte .
- Ao excluir snapshots em lotes, você pode remover um grande número de objetos capturados em vários snapshots, liberando efetivamente mais espaço do que a exclusão individual de snapshot causaria. Como resultado, você pode recuperar mais espaço para seus objetos de storage.

Passos

1. Para excluir um snapshot S3 específico, execute este comando:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. Para remover todos os snapshots S3 em um bucket, execute este comando:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

Limpar metadados de instantâneos do S3

Com snapshots S3, os metadados de snapshot também são gerados em um bucket. Os metadados do snapshot continuam a estar no bucket, mesmo que todos os snapshots sejam removidos dele. A presença de metadados do Snapshot bloqueia as seguintes operações:

- O cluster reverte para uma versão do ONTAP anterior ao ONTAP 9.16,1
- Configuração do SnapMirror S3 no balde

Antes de executar essas operações, você deve limpar todos os metadados do snapshot do bucket.

Antes de começar

Certifique-se de que removeu todos os instantâneos do S3 de um intervalo antes de começar a limpar os metadados.

Passos

1. Para limpar os metadados de snapshot de um bucket, execute este comando:

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

Auditoria S3 eventos

Auditoria S3 eventos

A partir do ONTAP 9.10,1, você pode auditar dados e eventos de gerenciamento em ambientes ONTAP S3. A funcionalidade de auditoria do S3 é semelhante aos recursos de auditoria nas existentes, e a auditoria do S3 e nas pode coexistir em um cluster.

Quando você cria e ativa uma configuração de auditoria do S3 em um SVM, os eventos do S3 são registrados em um arquivo de log. Você pode especificar os seguintes eventos a serem registrados:

Eventos de acesso a objetos (dados) por lançamento

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects of 9.10.1 foi renomeado para este)
- ListAllMyBuckets (ListBuckets de 9.10.1 foi renomeado para este)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPCompletar
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- Marcação de objetos
- ListUploads
- ListParts

Eventos de gerenciamento por liberação

9.15.1:

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- Retenção PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- Política de GetBucketPolicy
- CopyObject
- UploadPartCopy
- Política de PutBucketPolicy
- DeleteBucketPolicy

9.11.1:

- GetBucketControle de versão
- PutBucketControle de versão

9.10.1:

- Balde para a cabeça
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketlocalização

O formato de log é JavaScript Object Notation (JSON).

O limite combinado para configurações de auditoria S3 e NFS é de 400 SVMs por cluster.

É necessária a seguinte licença:

- ONTAP One, anteriormente parte do pacote principal, para protocolo e storage ONTAP S3

Para obter mais informações, "Como funciona o processo de auditoria do ONTAP"consulte .

Auditoria garantida

Por padrão, a auditoria S3 e nas é garantida. O ONTAP garante que todos os eventos de acesso de bucket auditáveis sejam registrados, mesmo que um nó não esteja disponível. Uma operação de bucket solicitada não pode ser concluída até que o Registro de auditoria dessa operação seja salvo no volume de estadiamento no armazenamento persistente. Se os Registros de auditoria não puderem ser confirmados nos arquivos de teste, seja por espaço insuficiente ou por causa de outros problemas, as operações do cliente serão negadas.

Requisitos de espaço para auditoria

No sistema de auditoria do ONTAP, os Registros de auditoria são armazenados inicialmente em arquivos de teste binário em nós individuais. Periodicamente, eles são consolidados e convertidos em logs de eventos legíveis pelo usuário, que são armazenados no diretório de log de eventos de auditoria do SVM.

Os arquivos de estadiamento são armazenados em um volume de estadiamento dedicado, que é criado pelo ONTAP quando a configuração de auditoria é criada. Há um volume de estadiamento por agregado.

Você precisa Planejar espaço disponível suficiente na configuração de auditoria:

- Para os volumes de estadiamento em agregados que contêm buckets auditados.
- Para o volume que contém o diretório onde os logs de eventos convertidos são armazenados.

Você pode controlar o número de logs de eventos e, portanto, o espaço disponível no volume, usando um de dois métodos ao criar a configuração de auditoria S3:

- Um limite numérico; o `-rotate-limit` parâmetro controla o número mínimo de arquivos de auditoria que devem ser preservados.
- Um limite de tempo; o `-retention-duration` parâmetro controla o período máximo que os arquivos podem ser preservados.

Em ambos os parâmetros, uma vez que o configurado é excedido, os arquivos de auditoria mais antigos podem ser excluídos para abrir espaço para os mais novos. Para ambos os parâmetros, o valor é 0, indicando que todos os arquivos devem ser mantidos. Para garantir espaço suficiente, é, portanto, uma prática recomendada definir um dos parâmetros para um valor não zero.

Devido à auditoria garantida, se o espaço disponível para os dados de auditoria acabar antes do limite de rotação, os dados de auditoria mais recentes não podem ser criados, resultando em falha no acesso dos clientes aos dados. Portanto, a escolha desse valor e do espaço alocado à auditoria deve ser escolhida cuidadosamente, e você deve responder a avisos sobre o espaço disponível do sistema de auditoria.

Para obter mais informações, "Conceitos básicos de auditoria"consulte .

Planejar uma configuração de auditoria S3

Você deve especificar vários parâmetros para a configuração de auditoria S3 ou aceitar os padrões. Em particular, você deve considerar quais parâmetros de rotação de log ajudarão a garantir espaço livre adequado.

Consulte a *`vserver object-store-server audit create`página man * para obter detalhes de sintaxe.

Parâmetros gerais

Há dois parâmetros necessários que você deve especificar ao criar a configuração de auditoria. Há também três parâmetros opcionais que você pode especificar.

Tipo de informação	Opção	Obrigatório
Nome da SVM Nome do SVM no qual você pode criar a configuração de auditoria. O SVM já deve existir e estar habilitado para S3.	`-vserver` *`svm_name`*	Sim

Log Destination path Especifica onde os logs de auditoria convertidos são armazenados. O caminho já deve existir no SVM. O caminho pode ter até 864 carateres de comprimento e deve ter permissões de leitura e gravação. Se o caminho não for válido, o comando de configuração de auditoria falhará.	`-destination` *text*	Sim
Categorias de eventos a auditar As seguintes categorias de eventos podem ser auditadas: • Eventos GetObject, PutObject e DeleteObject de dados • Eventos PutBucket de Gestão e DeleteBucket O padrão é auditar somente eventos de dados.	`-events {data|management}, …`	Não

Pode introduzir um dos seguintes parâmetros para controlar o número de ficheiros de registo de auditoria. Se nenhum valor for inserido, todos os arquivos de log serão retidos.

Tipo de informação	Opção	Obrigatório
Limite de rotação de arquivos de log Determina quantos arquivos de log de auditoria devem ser mantidos antes de girar o arquivo de log mais antigo. Por exemplo, se você inserir um valor de 5, os últimos cinco arquivos de log serão retidos. Um valor de 0 indica que todos os arquivos de log são mantidos. O valor padrão é 0.	`-rotate-limit` *integer*	Não
Limite de duração dos ficheiros de registo Determina por quanto tempo um arquivo de log pode ser retido antes de ser excluído. Por exemplo, se você inserir um valor de 5d0h0m, os logs com mais de 5 dias serão excluídos. Um valor de 0 indica que todos os arquivos de log são mantidos. O valor padrão é 0.	`-retention duration` *integer_time*	Não

Parâmetros para rotação do log de auditoria

Você pode girar os logs de auditoria com base no tamanho ou na programação. O padrão é girar os logs de auditoria com base no tamanho.

Rode registos com base no tamanho do registo

Se você quiser usar o método de rotação de log padrão e o tamanho padrão do log, não será necessário configurar nenhum parâmetro específico para a rotação de log. O tamanho padrão do log é de 100 MB.

Se você não quiser usar o tamanho padrão do log, você pode configurar o `-rotate-size` parâmetro para especificar um tamanho de log personalizado.

Se você quiser redefinir a rotação com base em um tamanho de log sozinho, use o seguinte comando para desdefinir o `-rotate-schedule-minute` parâmetro:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Gire os logs com base em um agendamento

Se você optar por girar os logs de auditoria com base em um agendamento, poderá agendar a rotação de logs usando os parâmetros de rotação baseados em tempo em qualquer combinação.

- Se utilizar rotação baseada no tempo, o `-rotate-schedule-minute` parâmetro é obrigatório.
- Todos os outros parâmetros de rotação baseados no tempo são opcionais.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- O programa de rotação é calculado utilizando todos os valores relacionados com o tempo. Por exemplo, se você especificar apenas o `-rotate-schedule-minute` parâmetro, os arquivos de log de auditoria serão girados com base nos minutos especificados em todos os dias da semana, durante todas as horas em todos os meses do ano.
- Se você especificar apenas um ou dois parâmetros de rotação baseados no tempo (por exemplo, `-rotate-schedule-month` e `-rotate-schedule-minutes`), os arquivos de log serão girados com base nos valores de minuto especificados em todos os dias da semana, durante todas as horas, mas somente durante os meses especificados.

  Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro, março e agosto em todas as segundas, quartas e sábados às 10:30 da manhã

- Se você especificar valores para ambos `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, eles serão considerados independentemente.

  Por exemplo, se você especificar `-rotate-schedule-dayofweek` como sexta-feira e `-rotate -schedule-day` como 13, os logs de auditoria serão girados em todas as sextas-feiras e no dia 13th do mês especificado, não apenas em todas as sextas-feiras, dia 13th.

- Se quiser redefinir a rotação com base em um agendamento sozinho, use o seguinte comando para desmarcar o `-rotate-size parameter`:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Rode registos com base no tamanho e na programação do registo

Você pode optar por girar os arquivos de log com base no tamanho do log e em uma programação, definindo o parâmetro -Rotate-size e os parâmetros de rotação baseados no tempo em qualquer combinação. Por exemplo: Se `-rotate-size` estiver definido para 10 MB e `-rotate-schedule-minute` estiver definido para 15, os arquivos de log rodam quando o tamanho do arquivo de log atinge 10 MB ou nos 15th minutos de cada hora (o que ocorrer primeiro).

Crie e habilite uma configuração de auditoria S3

Para implementar a auditoria do S3, primeiro você cria uma configuração de auditoria de armazenamento de objetos persistente em um SVM habilitado para S3 e, em seguida, ativa a configuração.

O que você vai precisar

- SVM habilitado para S3.
- Espaço suficiente para estadiamento de volumes no agregado.

Sobre esta tarefa

É necessária uma configuração de auditoria para cada SVM que contenha buckets do S3 que você deseja auditar. Você pode habilitar a auditoria S3 em servidores S3 novos ou existentes. As configurações de auditoria persistem em um ambiente S3 até serem removidas pelo comando **vserver object-store-server audit delete**.

A configuração de auditoria do S3 se aplica a todos os buckets do SVM que você selecionar para auditoria. Um SVM habilitado para auditoria pode conter buckets auditados e não auditados.

É recomendável configurar a auditoria S3 para rotação automática de logs, determinada pelo tamanho do log ou por um agendamento. Se você não configurar a rotação automática de log, todos os arquivos de log serão retidos por padrão. Você também pode girar arquivos de log S3 manualmente usando o comando **vserver object-store-server audit rotate-log**.

Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino não poderá estar no volume raiz.

Procedimento

1. Crie a configuração de auditoria para girar logs de auditoria com base no tamanho do log ou em uma programação.

Se você quiser girar logs de auditoria…	Digite…
Tamanho do registo	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integer_d][_integer_h][_integer_m][_integers`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`

Se você quiser girar logs de auditoria…	Digite…
Uma programação	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integerd`*`][`*`integerh`*`] [`*`integerm`*`][`*`integers`*`]] } [-rotate-schedule-month` *`chron_month`*`] [-rotate-schedule-dayofweek` *`chron_dayofweek`*`] [-rotate-schedule-day` *`chron_dayofmonth`*`] [-rotate-schedule-hour` *`chron_hour`*`] -rotate-schedule-minute` *`chron_minute`* O `-rotate-schedule-minute` parâmetro é necessário se você estiver configurando a rotação de log de auditoria baseada em tempo.

2. Ativar auditoria S3:

   `vserver object-store-server audit enable -vserver` *`svm_name`*

Exemplos

O exemplo a seguir cria uma configuração de auditoria que audita todos os eventos S3 (o padrão) usando rotação baseada em tamanho. Os logs são armazenados no diretório /audit_log. O limite de tamanho do arquivo de log é de 200 MB. Os logs são girados quando atingem 200 MB de tamanho.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

O exemplo a seguir cria uma configuração de auditoria que audita todos os eventos S3 (o padrão) usando rotação baseada em tamanho. O limite de tamanho do arquivo de log é de 100 MB (o padrão) e os logs são mantidos por 5 dias antes de serem excluídos.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

O exemplo a seguir cria uma configuração de auditoria que audita eventos de gerenciamento S3 e eventos de preparação de políticas de acesso central usando rotação baseada em tempo. Os logs de auditoria são girados mensalmente, às 12:30 horas em todos os dias da semana. O limite de rotação do registo é 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Selecione buckets para auditoria S3

Você precisa especificar quais buckets auditar em um SVM habilitado para auditoria.

O que você vai precisar

- Um SVM foi habilitado para auditoria S3.

Sobre esta tarefa

As configurações de auditoria do S3 são habilitadas por SVM, mas você precisa selecionar os buckets no SVMS que estão habilitados para auditoria. Se você adicionar buckets ao SVM e quiser que os novos buckets sejam auditados, selecione-os com este procedimento. Também é possível ter buckets não auditados em uma SVM habilitada para auditoria S3.

As configurações de auditoria persistem para buckets até serem removidas pelo `vserver object-store-server audit event-selector delete` comando.

Procedimento

Selecione um bucket para a auditoria S3:

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

- `-access` - especifica o tipo de acesso a eventos a ser auditado: `read-only`, `write-only` ou `all` (o padrão é `all`).
- `-permission` - especifica o tipo de permissão de evento a ser auditado: `allow-only`, `deny-only` ou `all` (o padrão é `all`).

Exemplo

O exemplo a seguir cria uma configuração de auditoria de bucket que somente Registra eventos permitidos com acesso somente leitura:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Modificar uma configuração de auditoria S3

É possível modificar os parâmetros de auditoria de buckets individuais ou a configuração de auditoria de todos os buckets selecionados para auditoria no SVM.

Se você quiser modificar a configuração de auditoria para…	Digite…
Baldes individuais	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
Todos os buckets no SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Exemplos

O exemplo a seguir modifica uma configuração de auditoria de bucket individual para auditar somente eventos de acesso somente gravação:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

O exemplo a seguir modifica a configuração de auditoria de todos os buckets no SVM para alterar o limite de tamanho do log para 10MB e reter arquivos de log 3 antes de girar.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Mostrar configurações de auditoria do S3

Depois de concluir a configuração de auditoria, você pode verificar se a auditoria está configurada corretamente e está habilitada. Você também pode exibir informações sobre todas as configurações de auditoria de armazenamento de objetos no cluster.

Sobre esta tarefa

É possível exibir informações sobre configurações de auditoria de bucket e SVM.

- Buckets – use o `vserver object-store-server audit event-selector show` comando

  Sem parâmetros, o comando exibe as seguintes informações sobre buckets em todos os SVMs no cluster com configurações de auditoria de armazenamento de objetos:

  - Nome do SVM
  - Nome do intervalo
  - Valores de acesso e permissão
- SVMs – use o `vserver object-store-server audit show` comando

  Sem parâmetros, o comando exibe as seguintes informações sobre todos os SVMs no cluster com configurações de auditoria de armazenamento de objetos:

  - Nome do SVM
  - Estado de auditoria
  - Diretório de destino

Você pode especificar o `-fields` parâmetro para especificar quais informações de configuração de auditoria serão exibidas.

Procedimento

Mostrar informações sobre configurações de auditoria do S3:

Se pretender modificar a configuração para…	Digite…
Baldes	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Se pretender modificar a configuração para…	Digite…
SVMs	`vserver object-store-server audit show [-vserver` *svm_name*`] [`*parameters*`]`

Exemplos

O exemplo a seguir exibe informações para um único bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

O exemplo a seguir exibe informações de todos os buckets em um SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

O exemplo a seguir exibe o nome, o estado de auditoria, os tipos de eventos, o formato de log e o diretório de destino para todos os SVMs.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

O exemplo a seguir exibe os nomes e detalhes da SVM sobre o log de auditoria de todos os SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details

                Rotation                            Rotation
      Vserver   File Size Rotation Schedule         Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                        0
```

O exemplo a seguir exibe em forma de lista todas as informações de configuração de auditoria sobre todos os SVMs.

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                           Log Format: json
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
                   Log Retention Time: 0s
```

Informações sobre direitos autorais

Informações sobre marcas comerciais