Proteção de dados e recuperação de desastres

ONTAP 9

NetApp
January 17, 2025

Índice

Proteção de dados e recuperação de desastres

Peering de cluster e SVM

Visão geral do peering de cluster e SVM

Você pode criar relacionamentos entre clusters de origem e destino e entre máquinas virtuais de armazenamento de origem e destino (SVMs). Você precisa criar relacionamentos entre pares entre essas entidades antes de poder replicar cópias Snapshot usando o SnapMirror.

O ONTAP 9.3 oferece aprimoramentos que simplificam a maneira como você configura relacionamentos entre clusters e SVMs. Os procedimentos de peering de cluster e SVMs estão disponíveis para todas as versões do ONTAP 9. Você deve usar o procedimento apropriado para sua versão do ONTAP.

Você executa os procedimentos usando a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Preparar-se para peering de cluster e SVM

Noções básicas de peering

Você deve criar relacionamentos *peer* entre clusters de origem e destino e entre SVMs de origem e destino antes de poder replicar cópias Snapshot usando o SnapMirror. Um relacionamento de pares define conexões de rede que permitem que clusters e SVMs troquem dados com segurança.

Clusters e SVMs em relações entre pares se comunicam pela rede entre clusters usando *interfaces lógicas (LIFs).* um LIF entre clusters é um LIF que suporta o serviço de interface de rede "entre clusters-core" e é normalmente criado usando a política de serviço de interface de rede "default-clusters". É necessário criar LIFs entre clusters em cada nó nos clusters que estão sendo perados.

Os LIFs usam rotas que pertencem ao SVM do sistema ao qual são atribuídos. O ONTAP cria automaticamente um sistema SVM para comunicações em nível de cluster em um espaço de IPspace.

Topologias de fan-out e cascata são suportadas. Em uma topologia em cascata, você só precisa criar redes entre clusters primários e secundários e entre clusters secundários e secundários. Não é necessário criar uma rede entre clusters primário e terciário.

> É possível (mas não aconselhável) que um administrador remova o serviço entre clusters da política de serviços padrão entre clusters. Se isso ocorrer, LIFs criadas usando "default-clusters" não serão, na verdade, LIFs entre clusters. Para confirmar que a política de serviço padrão contém o serviço entre clusters-core, use o seguinte comando:
>
> ```
> network interface service-policy show -policy default-intercluster
> ```

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar se os requisitos de conetividade, porta, endereço IP, sub-rede, firewall e nomenclatura de cluster são

atendidos.

> A partir do ONTAP 9.6, o peering de cluster fornece suporte de criptografia TLS 1,2 AES-256 GCM para replicação de dados por padrão. As cifras de segurança padrão ("PSK-AES256-GCM-SHA384") são necessárias para que o peering de cluster funcione mesmo que a criptografia esteja desativada.
>
> Começando com ONTAP 9.11,1, as cifras de segurança DHE-PSK estão disponíveis por padrão.
>
> A partir do ONTAP 9.15,1, o peering de cluster fornece suporte de criptografia TLS 1,3 para replicação de dados por padrão.

Requisitos de conetividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve pertencer ao domínio de broadcast que contém as portas usadas para comunicação entre clusters.
- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

  Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.

> O ONTAP permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

  Você pode usar vários IPspaces para fazer pares com vários clusters. A conetividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

  As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de

interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall

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 .

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Tráfego ICMP bidirecional
- Tráfego TCP iniciado bidirecional para os endereços IP de todas as LIFs entre clusters nas portas 11104 e 11105
- HTTPS bidirecional entre os LIFs entre clusters

  Embora o HTTPS não seja necessário quando você configura o peering de cluster usando a CLI, o HTTPS é necessário mais tarde se você usar o System Manager para configurar a proteção de dados.

A política de firewall predefinida `intercluster` permite o acesso através do protocolo HTTPS e de todos os endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Requisito de cluster

Os clusters precisam atender aos seguintes requisitos:

- Um cluster não pode estar em um relacionamento de pares com mais de 255 clusters.

Use portas compartilhadas ou dedicadas

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. Ao decidir se deseja compartilhar portas, você precisa considerar a largura de banda da rede, o intervalo de replicação e a disponibilidade da porta.

Você pode compartilhar portas em um cluster com peered enquanto usa portas dedicadas no outro.

Largura de banda da rede

Se você tiver uma rede de alta velocidade, como 10 GbE, talvez tenha largura de banda local suficiente para executar a replicação usando as mesmas portas de 10 GbE usadas para acesso aos dados.

Mesmo assim, você deve comparar a largura de banda da WAN disponível com a largura de banda da LAN. Se a largura de banda da WAN disponível for significativamente menor que 10 GbE, talvez seja necessário usar portas dedicadas.

A única exceção a essa regra pode ser quando todos ou muitos nós no cluster replicarem dados, caso em que a utilização da largura de banda é normalmente espalhada pelos nós.

Se você não estiver usando portas dedicadas, o tamanho máximo da unidade de transmissão (MTU) da rede de replicação geralmente deve ser o mesmo que o tamanho da MTU da rede de dados.

Intervalo de replicação

Se a replicação ocorrer em horas fora do pico, você poderá usar portas de dados para replicação mesmo sem uma conexão LAN de 10 GbE.

Se a replicação ocorrer durante o horário comercial normal, você precisa considerar a quantidade de dados que serão replicados e se ela precisará de tanta largura de banda que poderia causar contenção com protocolos de dados. Se a utilização da rede por protocolos de dados (SMB, NFS, iSCSI) for superior a 50%, deverá utilizar portas dedicadas para comunicação entre clusters, para permitir uma performance não degradada se ocorrer failover de nó.

Disponibilidade da porta

Se você determinar que o tráfego de replicação está interferindo no tráfego de dados, poderá migrar LIFs para qualquer outra porta compartilhada com capacidade para clusters no mesmo nó.

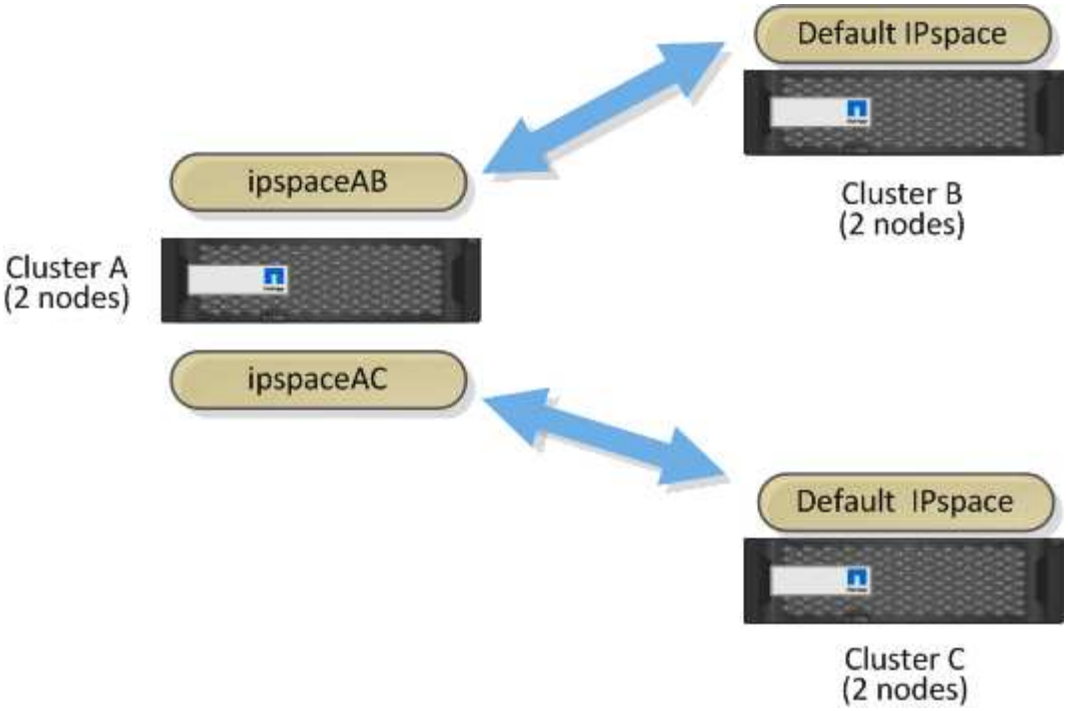
Você também pode dedicar portas VLAN para replicação. A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

Use IPspaces personalizados para isolar o tráfego de replicação

Você pode usar IPspaces personalizados para separar as interações que um cluster tem com seus pares. Chamada de *conetividade entre clusters designada*, essa configuração permite que os provedores de serviços isolem o tráfego de replicação em ambientes multitenant.

Suponha, por exemplo, que você deseja que o tráfego de replicação entre o Cluster A e o Cluster B seja separado do tráfego de replicação entre o Cluster A e o Cluster C. para conseguir isso, você pode criar dois espaços IPspaces no Cluster A.

Um IPspace contém as LIFs entre clusters que você usa para se comunicar com o Cluster B. o outro contém as LIFs entre clusters que você usa para se comunicar com o Cluster C, como mostrado na ilustração a seguir.



Para a configuração de IPspace personalizada, consulte o *Network Management Guide*.

Configurar LIFs entre clusters

Configurar LIFs entre clusters em portas de dados compartilhados

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.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   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. Crie LIFs entre clusters em um administrador SVM (IPspace padrão) ou em um sistema SVM (IPspace personalizado):

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
Em ONTAP 9.5 e anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Para obter a sintaxe completa do comando, consulte a página man.

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

```
cluster01::> network interface create -vserver cluster01 -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 cluster01 -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:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
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:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show –service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

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
```

Configurar LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que portas `e0e` e `e0f` não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

O exemplo a seguir atribui portas `e0e` e `e0f` ao grupo de failover `intercluster01` no SVM do sistema `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

`network interface failover-groups show`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`

Opção	Descrição
Em ONTAP 9.5 e anteriores:	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` no grupo failover `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` a porta SVM`e0e` farão failover para a `e0f` 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:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar LIFs entre clusters em IPspaces personalizados

Você pode configurar LIFs entre clusters em IPspaces personalizados. Isso permite isolar o tráfego de replicação em ambientes multitenant.

Quando você cria um IPspace personalizado, o sistema cria uma máquina virtual de storage do sistema (SVM) para servir como um contêiner para os objetos do sistema nesse IPspace. Você pode usar o novo SVM como contêiner para quaisquer LIFs entre clusters no novo IPspace. O novo SVM tem o mesmo nome que o IPspace personalizado.

Passos

1. Liste as portas no cluster:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Crie IPspaces personalizados no cluster:

   `network ipspace create -ipspace` *`ipspace`*

   O exemplo a seguir cria o IPspace personalizado `ipspace-IC1` :

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

3. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que portas `e0e` e `e0f` não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. Remova as portas disponíveis do domínio de broadcast padrão:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Uma porta não pode estar em mais de um domínio de broadcast de cada vez. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir remove portas `e0e` e `e0f` do domínio de broadcast padrão:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Verifique se as portas foram removidas do domínio de broadcast padrão:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que as portas `e0e` e `e0f` foram removidas do domínio de broadcast padrão:

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Crie um domínio de broadcast no IPspace personalizado:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   O exemplo a seguir cria o domínio de broadcast `ipspace-IC1-bd` no IPspace : `ipspace-IC1`

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Verifique se o domínio de broadcast foi criado:

   `network port broadcast-domain show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  ---------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a             complete
                            cluster01-01:e0b             complete
                            cluster01-02:e0a             complete
                            cluster01-02:e0b             complete
Default Default       1500
                            cluster01-01:e0c             complete
                            cluster01-01:e0d             complete
                            cluster01-01:e0f             complete
                            cluster01-01:e0g             complete
                            cluster01-02:e0c             complete
                            cluster01-02:e0d             complete
                            cluster01-02:e0f             complete
                            cluster01-02:e0g             complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e             complete
                            cluster01-01:e0f             complete
                            cluster01-02:e0e             complete
                            cluster01-02:e0f             complete
```

8. Crie LIFs entre clusters no sistema SVM e atribua-os ao domínio de broadcast:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
Em ONTAP 9.5 e anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

O LIF é criado no domínio de broadcast ao qual a porta inicial é atribuída. O domínio de broadcast tem um grupo de failover padrão com o mesmo nome do domínio de broadcast. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` no domínio de broadcast `ipspace-IC1-bd` :

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` a porta SVM `e0e` fazem failover para a porta 'e0f':

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar relações entre pares

Crie um relacionamento de pares de cluster

Antes de proteger seus dados replicando-os em um cluster remoto para fins de backup de dados e recuperação de desastres, você deve criar um relacionamento de peers de clusters entre o cluster local e o cluster remoto.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar a replicação de snapshot de configuração. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Várias políticas de proteção padrão estão disponíveis. Você deve ter criado suas políticas de proteção se quiser usar políticas personalizadas.

Antes de começar

- Se você estiver usando a CLI do ONTAP, crie LIFs entre clusters em todos os nós dos clusters que estão sendo direcionados usando um dos seguintes métodos:

    - "Configurar LIFs entre clusters em portas de dados compartilhados"
    - "Configurar LIFs entre clusters em portas de dados dedicadas"
    - "Configurar LIFs entre clusters em IPspaces personalizados"
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior. (Se os clusters estiverem executando o ONTAP 9.2 ou anterior, consulte os procedimentos em "este documento arquivado".)

Passos

Execute esta tarefa usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

1. No cluster local, clique em **Cluster > Settings**.
2. Na seção **Configurações de cluster**, clique em **Adicionar interfaces de rede** e insira o endereço IP e a máscara de sub-rede para adicionar interfaces de rede entre clusters para o cluster.

   Repita este passo no painel remoto.

3. No cluster remoto, clique em **Cluster > Settings**.
4. Clique ⋮ na secção **Cluster Peers** e selecione **Generate Passphrase** (gerar frase-passe).
5. Selecione a versão remota do cluster do ONTAP.
6. Copie a frase-passe gerada.
7. No cluster local, em **Cluster Peers**, clique ⋮ e selecione **Peer cluster**.
8. Na janela **cluster de pares**, cole a frase-passe e clique em **Iniciar peering de cluster**.

CLI

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   Se você especificar ambos `-generate-passphrase` e `-peer-addrs`, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addrs` poderá usar a senha gerada.

   Você pode ignorar a `-ipspace` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   Se você estiver criando o relacionamento de peering no ONTAP 9.6 ou posterior e não quiser que as comunicações de peering entre clusters sejam criptografadas, use a `-encryption-protocol -proposed none` opção para desativar a criptografia.

   O exemplo a seguir cria um relacionamento de peer de cluster com um cluster remoto não especificado e pré-autoriza relacionamentos entre pares com SVMs e `vs1` `vs2` no cluster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

O exemplo a seguir cria um relacionamento de peer de cluster com o cluster remoto nos endereços IP de LIF 192.140.112.103 e 192.140.112.104 e pré-autoriza um relacionamento de pares com qualquer SVM no cluster local:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

O exemplo a seguir cria um relacionamento de peer de cluster com um cluster remoto não especificado e pré-autoriza relacionamentos entre pares com SVMs e`vs1` `vs2` no cluster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. No cluster de origem, autentique o cluster de origem no cluster de destino:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir autentica o cluster local para o cluster remoto nos endereços IP 192.140.112.101 e 192.140.112.102 do LIF:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                               Remote Cluster Name: cluster2
                               Active IP Addresses: 192.140.112.101,
192.140.112.102
                             Cluster Serial Number: 1-80-123456
                    Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                      IPspace for the Relationship: Default
```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da preparação para recuperação de desastres em volume"

Criar um relacionamento entre pares SVM entre clusters

Você pode usar o `vserver peer create` comando para criar um relacionamento entre SVMs em clusters locais e remotos.

Antes de começar

- Os clusters de origem e destino devem ser percorridos.
- Os clusters devem estar executando o ONTAP 9.3. (Se os clusters estiverem executando o ONTAP 9.2 ou

anterior, consulte os procedimentos em "este documento arquivado".)

- Você deve ter relações de pares "pré-autorizadas" para os SVMs no cluster remoto.

  Para obter mais informações, "Criando um relacionamento de cluster peer"consulte .

Sobre esta tarefa

No ONTAP 9.2 e anteriores, você pode autorizar um relacionamento de pares para apenas um SVM de cada vez. Isso significa que você precisa executar o `vserver peer accept` comando cada vez que você autorizar um relacionamento de pares SVM pendente.

A partir do ONTAP 9.3, você pode "pré-autorizar" relacionamentos de pares para vários SVMs, listando os SVMs na `-initial-allowed-vserver` opção quando você cria um relacionamento de peer de cluster. Para obter mais informações, "Criando um relacionamento de cluster peer"consulte .

Passos

1. No cluster de destino de proteção de dados, exiba os SVMs que são pré-autorizados para peering:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. No cluster de origem de proteção de dados, crie um relacionamento de mesmo nível com um SVM pré-autorizado no cluster de destino de proteção de dados:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um relacionamento entre o SVM local `pvs1` e o SVM remoto pré-autorizado `vs1` :

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Verifique o relacionamento entre pares SVM:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Adicione um relacionamento entre pares SVM entre clusters

Se você criar um SVM depois de configurar um relacionamento de pares de cluster, precisará adicionar um relacionamento de mesmo nível para o SVM manualmente. Você pode usar o `vserver peer create` comando para criar um relacionamento entre pares entre SVMs. Após a criação do relacionamento de pares, você pode executar `vserver peer accept` no cluster remoto para autorizar o relacionamento de pares.

Antes de começar

Os clusters de origem e destino devem ser percorridos.

Sobre esta tarefa

Você pode criar relacionamentos entre pares entre SVMs no mesmo cluster para backup de dados locais. Para obter mais informações, consulte a `vserver peer create` página de manual.

Os administradores ocasionalmente usam o `vserver peer reject` comando para rejeitar uma proposta de relacionamento com colegas SVM. Se a relação entre SVMs estiver no `rejected` estado, você deverá excluir a relação antes de criar uma nova. Para obter mais informações, consulte a `vserver peer delete` página de manual.

Passos

1. No cluster de origem de proteção de dados, crie um relacionamento de mesmo nível com um SVM no cluster de destino de proteção de dados:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   O exemplo a seguir cria um relacionamento entre o SVM local`pvs1` e o SVM remoto`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Se os SVMs locais e remotos tiverem os mesmos nomes, você deverá usar um *local name* para criar o relacionamento de pares SVM:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. No cluster de origem de proteção de dados, verifique se o relacionamento de pares foi iniciado:

   `vserver peer show-all`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que a relação entre SVM`pvs1` e SVM`vs1` foi iniciada:

```
cluster01::> vserver peer show-all
            Peer        Peer                        Peering
Vserver     Vserver     State      Peer Cluster     Applications
--------    --------    ---------  -------------    ------------
pvs1        vs1         initiated   Cluster02         snapmirror
```

3. No cluster de destino da proteção de dados, exiba a relação de pares SVM pendente:

   `vserver peer show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir lista as relações de pares pendentes para `cluster02`:

```
cluster02::> vserver peer show

                  Peer              Peer
Vserver           Vserver           State
-----------       -----------       ------------
vs1               pvs1              pending
```

4. No cluster de destino de proteção de dados, autorize o relacionamento de pares pendente:

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autoriza o relacionamento entre pares entre o SVM local `vs1` e o SVM remoto `pvs1` :

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Verifique o relacionamento entre pares SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Habilitar a criptografia de peering de cluster em um relacionamento de pares existente

A partir do ONTAP 9.6, a criptografia de peering de cluster é ativada por padrão em todas as relações de peering de cluster recém-criadas. A criptografia de peering de cluster usa uma chave pré-compartilhada (PSK) e a camada de segurança de transporte (TLS) para proteger as comunicações de peering entre clusters. Isso adiciona uma camada adicional de segurança entre os clusters com peering.

Sobre esta tarefa

Se você estiver atualizando clusters peered para o ONTAP 9.6 ou posterior e a relação de peering tiver sido criada no ONTAP 9.5 ou anterior, a criptografia de peering de cluster deve ser ativada manualmente após a atualização. Ambos os clusters no relacionamento de peering devem estar executando o ONTAP 9.6 ou posterior para habilitar a criptografia de peering de cluster.

Passos

1. No cluster de destino, ative a encriptação para comunicações com o cluster de origem:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Quando solicitado, introduza uma frase-passe.
3. No cluster de origem da proteção de dados, ative a criptografia para comunicação com o cluster de destino da proteção de dados:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Quando solicitado, introduza a mesma frase-passe introduzida no cluster de destino.

Remova a criptografia de peering de cluster de um relacionamento de pares existente

Por padrão, a criptografia de peering de cluster é ativada em todos os relacionamentos de pares criados no ONTAP 9.6 ou posterior. Se você não quiser usar criptografia para

comunicações de peering entre clusters, você pode desativá-la.

Passos

1. No cluster de destino, modifique as comunicações com o cluster de origem para interromper o uso da criptografia de peering de cluster:
   - Para remover a criptografia, mas manter a autenticação, digite:

     ```
     cluster peer modify <source_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para remover criptografia e autenticação:
     i. Modifique a política de peering de cluster para permitir acesso não autenticado:

        ```
        cluster peer policy modify -is-unauthenticated-access-permitted
        true
        ```

     ii. Modificar criptografia e acesso de autenticação:

        ```
        cluster peer modify <source_cluster> -auth-status no-
        authentication
        ```

2. Quando solicitado, introduza a frase-passe.
3. Confirme a frase-passe reinserindo-a.
4. No cluster de origem, desative a encriptação para comunicação com o cluster de destino:
   - Para remover a criptografia, mas manter a autenticação, digite:

     ```
     cluster peer modify <destination_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para remover criptografia e autenticação:
     i. Modifique a política de peering de cluster para permitir acesso não autenticado:

        ```
        cluster peer policy modify -is-unauthenticated-access-permitted
        true
        ```

     ii. Modificar criptografia e acesso de autenticação:

        ```
        cluster peer modify <destination_cluster> -auth-status no-
        authentication
        ```

5. Quando solicitado, introduza e introduza novamente a mesma frase-passe utilizada no cluster de destino.

Gerenciar snapshots locais

Visão geral do gerenciamento de cópias Snapshot locais

Uma *cópia Snapshot* é uma imagem pontual e somente leitura de um volume. A imagem consome espaço de armazenamento mínimo e incorre em sobrecarga de desempenho insignificante, pois Registra apenas alterações nos arquivos desde a última cópia Snapshot.

Você pode usar uma cópia Snapshot para restaurar todo o conteúdo de um volume ou para recuperar arquivos individuais ou LUNs. As cópias snapshot são armazenadas no diretório `.snapshot` do volume.

No ONTAP 9.3 e versões anteriores, um volume pode conter até 255 cópias Snapshot. No ONTAP 9.4 e posterior, um FlexVol volume pode conter até 1023 cópias snapshot.

> A partir do ONTAP 9.8, os volumes FlexGroup podem conter 1023 cópias Snapshot. Para obter mais informações, "Proteja volumes FlexGroup com cópias Snapshot"consulte .

Configurar políticas de snapshot personalizadas

Configurar uma visão geral das políticas de Snapshot personalizadas

Uma política *Snapshot* define como o sistema cria cópias Snapshot. A política especifica quando criar cópias Snapshot, quantas cópias devem ser mantidas e como nomeá-las. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes e nomear as cópias "diárias.`*timestamp*`".

A política padrão de um volume cria automaticamente cópias Snapshot na programação a seguir, com as cópias Snapshot mais antigas excluídas para abrir espaço para cópias mais recentes:

- Um máximo de seis cópias Snapshot por hora levou cinco minutos depois da hora.
- Um máximo de duas cópias snapshot diárias realizadas de segunda a sábado, 10 minutos após a meia-noite.
- Um máximo de duas cópias Snapshot semanais realizadas todos os domingos, aos 15 minutos após a meia-noite.

A menos que você especifique uma política de Snapshot ao criar um volume, o volume herda a política de Snapshot associada a ela que contém a máquina virtual de storage (SVM).

Quando configurar uma política Snapshot personalizada

Se a política Snapshot padrão não for apropriada para um volume, você poderá configurar uma política personalizada que modifique a frequência, a retenção e o nome das cópias snapshot. A programação será ditada principalmente pela taxa de alteração do sistema de arquivos ativo.

Você pode fazer backup de um sistema de arquivos muito usado como um banco de dados a cada hora,

enquanto você faz backup de arquivos raramente usados uma vez por dia. Mesmo para um banco de dados, você normalmente executa um backup completo uma ou duas vezes por dia, enquanto faz backup de logs de transações a cada hora.

Outros fatores são a importância dos arquivos para a sua organização, seu Contrato de nível de Serviço (SLA), seu objetivo do ponto de recuperação (RPO) e seu objetivo de tempo de recuperação (rto). De um modo geral, você deve reter apenas quantas cópias snapshot forem necessárias.

Criar um agendamento de trabalho instantâneo

Uma política Snapshot requer pelo menos um agendamento de trabalho de cópia Snapshot. Você pode usar o System Manager ou o `job schedule cron create` comando para criar uma agenda de tarefas.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar uma agenda de trabalhos instantâneos. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Por padrão, o ONTAP forma os nomes das cópias Snapshot anexando um carimbo de data/hora ao nome da programação de trabalhos.

Se você especificar valores para o dia do mês e o dia da semana, os valores serão considerados independentemente. Por exemplo, um cronograma do cron com a especificação do dia `Friday` e a especificação do dia do mês `13` é executado todas as sextas-feiras e no dia 13th de cada mês, não apenas em todas as sextas-feiras, dia 13th.

Exemplo 1. Passos

System Manager

1. Navegue até **proteção > Visão geral** e expanda **configurações de política local**.
2. No painel **horários**, clique em .
3. Na janela **horários**, clique em .
4. Na janela **Adicionar agendamento**, insira o nome da programação e escolha o contexto e o tipo de agendamento.
5. Clique em **Salvar**.

CLI

1. Criar uma agenda de trabalhos:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

A partir do ONTAP 9.10,1, você pode incluir o SVM para sua agenda de trabalho:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

O exemplo a seguir cria um horário de trabalho chamado `myweekly` que é executado aos sábados às 3:00 da manhã:

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

O exemplo a seguir cria uma programação chamada `myweeklymulti` que especifica vários dias, horas e minutos:

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

Criar uma política Snapshot

Uma política Snapshot especifica quando criar cópias Snapshot, quantas cópias devem ser mantidas e como nomeá-las. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes e

nomeá-las "diárias.`*timestamp*`". Uma política Snapshot pode conter até cinco agendamentos de tarefas.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar uma política de snapshot. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Por padrão, o ONTAP forma os nomes das cópias Snapshot anexando um carimbo de data/hora ao nome da programação de trabalhos:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Se preferir, pode substituir um prefixo para o nome da agenda de trabalhos.

A `snapmirror-label` opção é para replicação SnapMirror. Para obter mais informações, "Definir uma regra para uma política"consulte .

Passos

Você pode criar uma política de cópia Snapshot usando o Gerenciador do sistema ou a CLI do ONTAP. O procedimento cria uma política de cópia Snapshot apenas no cluster local.

System Manager

1. Navegue até **proteção > Visão geral** e expanda **configurações de política local**.
2. No painel **políticas de instantâneos**, clique em .
3. Na guia **políticas de instantâneos**, clique Add em .
4. Na janela **Add Snapshot policy** (Adicionar instantâneo), insira o nome da política e escolha o escopo.
5. Clique Add em .
6. Para selecionar uma programação, clique no nome da programação atualmente exibida, clique em e escolha uma programação diferente.
7. Insira o máximo de cópias Snapshot a reter e, se necessário, insira o rótulo SnapMirror e o período de retenção do SnapLock.
8. Clique em **Salvar**.

CLI

1. Criar uma política Snapshot:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

O exemplo a seguir cria uma política de Snapshot chamada `snap_policy_daily` que é executada em um `daily` agendamento. A política tem no máximo cinco cópias Snapshot, cada uma com o nome `daily.`*`timestamp`* e o rótulo SnapMirror `daily` :

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

Gerencie cópias Snapshot manualmente

Criar e excluir cópias Snapshot manualmente

Você pode criar cópias Snapshot manualmente quando não puder esperar que uma cópia Snapshot agendada seja criada. Além disso, você pode excluir cópias snapshot quando elas não forem mais necessárias.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar um snapshot sob demanda. Os sistemas ASA R2

fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Crie uma cópia Snapshot manualmente

Você pode criar manualmente uma cópia Snapshot usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

Passos

1. Navegue até **armazenamento > volumes** e selecione a guia **cópias Snapshot**.
2. Clique + Add em .
3. Na janela **Adicionar uma cópia Snapshot**, aceite o nome da cópia Snapshot padrão ou edite-o, se desejado.
4. **Opcional**: Adicione uma etiqueta SnapMirror.
5. Clique em **Add**.

CLI

1. Criar uma cópia Snapshot:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Exclua uma cópia Snapshot manualmente

Você pode excluir manualmente uma cópia Snapshot usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

Passos

1. Navegue até **armazenamento > volumes** e selecione a guia **cópias Snapshot**.
2. Localize a cópia Snapshot que deseja excluir, clique ⋮ em e selecione **Excluir**.
3. Na janela **Excluir cópia Snapshot**, selecione **Excluir cópia Snapshot**.
4. Clique em **Excluir**.

CLI

1. Excluir uma cópia Snapshot:

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Calcule o espaço que pode ser recuperado antes de excluir cópias Snapshot

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para selecionar

cópias Snapshot que deseja excluir e calcular o espaço que pode ser recuperado antes de excluí-las.

Passos

1. Clique em **armazenamento > volumes**.
2. Selecione o volume a partir do qual deseja excluir cópias Snapshot.
3. Clique em **cópias Snapshot**.
4. Selecione uma ou mais cópias Snapshot.
5. Clique em **Calculate Recenclaable Space** (calcular espaço de recuperação).

Gerenciar a reserva de cópias Snapshot

Gerencie a visão geral da reserva de cópias instantâneas

O *reserva de cópia Snapshot* reserva uma porcentagem de espaço em disco para cópias Snapshot, cinco por padrão. Como as cópias Snapshot usam espaço no sistema de arquivos ativo quando a reserva de cópias Snapshot está esgotada, talvez você queira aumentar a reserva de cópias snapshot conforme necessário. Como alternativa, você pode fazer cópias Snapshot autodelete quando a reserva estiver cheia.

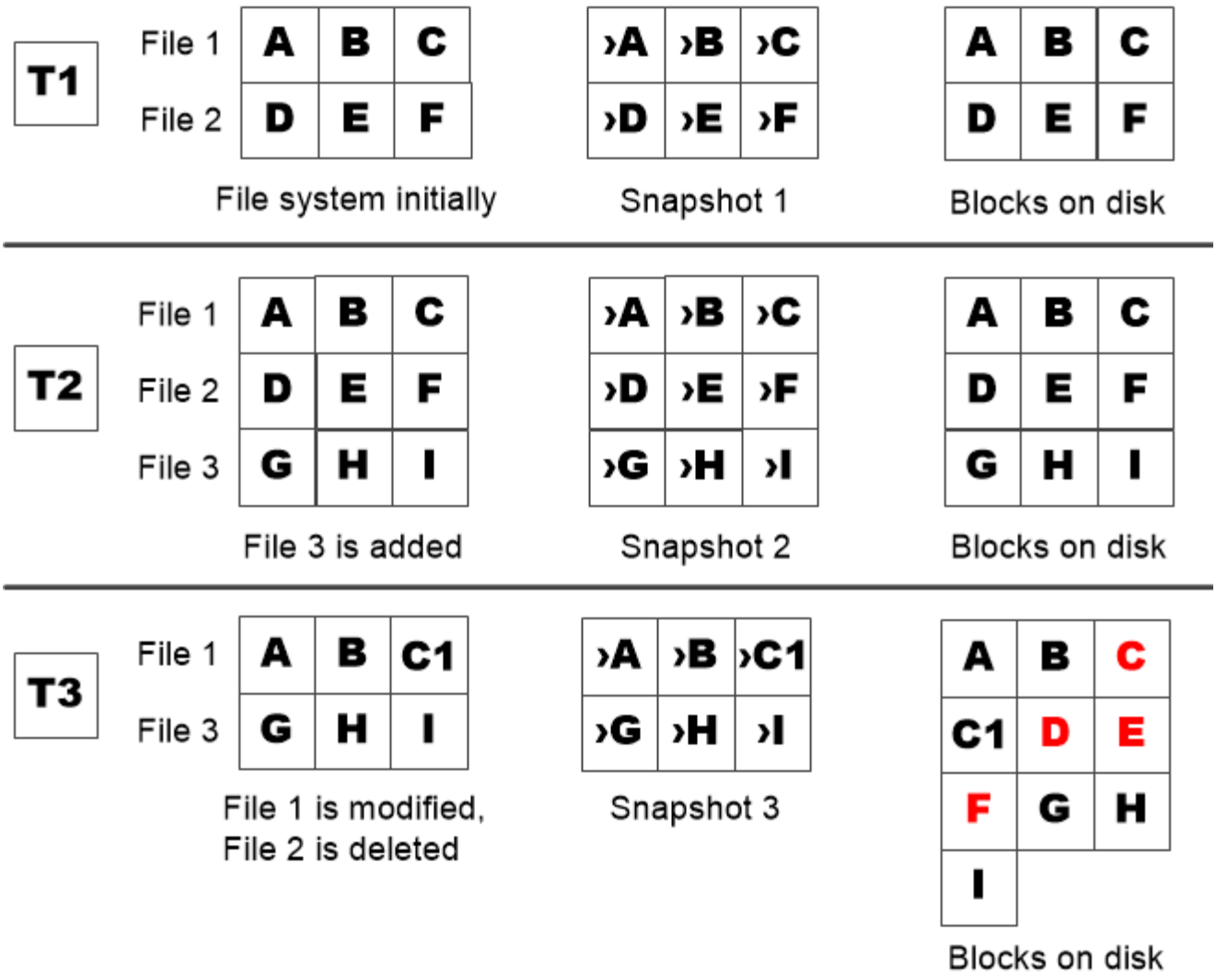
Quando aumentar a reserva de cópia Snapshot

Ao decidir se deseja aumentar a reserva Snapshot, é importante lembrar que uma cópia Snapshot Registra apenas alterações nos arquivos desde que a última cópia Snapshot foi feita. Ele consome espaço em disco somente quando blocos no sistema de arquivos ativo são modificados ou excluídos.

Isso significa que a taxa de alteração do sistema de arquivos é o fator chave para determinar a quantidade de espaço em disco usada pelas cópias Snapshot. Não importa quantas cópias Snapshot você criar, elas não consumirão espaço em disco se o sistema de arquivos ativo não for alterado.

Um FlexVol volume contendo logs de transação de banco de dados, por exemplo, pode ter uma reserva de cópia Snapshot tão grande quanto 20% para contabilizar sua maior taxa de alteração. Não só você deseja criar mais cópias Snapshot para capturar as atualizações mais frequentes do banco de dados, como também ter uma reserva de cópias Snapshot maior para lidar com o espaço de disco adicional que as cópias snapshot consomem.

Uma cópia Snapshot consiste em ponteiros para blocos em vez de cópias de blocos. Você pode pensar em um ponteiro como uma "reivindicação" em um bloco: O ONTAP mantém o bloco até que a cópia Snapshot seja excluída.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

Como excluir arquivos protegidos pode levar a menos espaço do arquivo do que o esperado

Uma cópia Snapshot aponta para um bloco mesmo depois que você exclui o arquivo que usou o bloco. Isso explica por que uma reserva de cópia Snapshot esgotada pode levar ao resultado contra-intuitivo no qual a exclusão de um sistema de arquivos inteiro resulta em menos espaço disponível do que o sistema de arquivos ocupado.

Considere o exemplo a seguir. Antes de excluir quaisquer arquivos, a `df` saída do comando é a seguinte:

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Depois de excluir todo o sistema de arquivos e fazer uma cópia Snapshot do volume, o `df` comando gera a seguinte saída:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Como mostra a saída, os 3 GB usados anteriormente pelo sistema de arquivos ativo agora estão sendo usados por cópias Snapshot, além dos 0,5 GB usados antes da exclusão.

Como o espaço em disco usado pelas cópias Snapshot agora excede a reserva de cópias Snapshot, o excesso de 2,5 GB "pílulas" para o espaço reservado para arquivos ativos, deixando você com 0,5 GB de espaço livre para arquivos onde você poderia razoavelmente ter esperado 3 GB.

Monitorar o consumo do disco de cópia Snapshot

Você pode monitorar o consumo de disco de cópia Snapshot usando o `df` comando. O comando exibe a quantidade de espaço livre no sistema de arquivos ativo e na reserva de cópia Snapshot.

Passo

1. Exibir consumo do disco de cópia Snapshot: `df`

   O exemplo a seguir mostra o consumo do disco de cópia Snapshot:

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Verifique a reserva de cópias Snapshot disponível em um volume

Você pode querer verificar quanto reserva de cópia Snapshot está disponível em um volume usando o `snapshot-reserve-available` parâmetro com o `volume show` comando.

Passo

1. Verifique a reserva de cópias instantâneas disponível em um volume:

   `vol show -vserver` *`SVM`* `-volume` *`volume`* `-fields snapshot-reserve-available`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir exibe a reserva de cópia Snapshot disponível para `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

Modifique a reserva de cópia Snapshot

Talvez você queira configurar uma reserva de cópias Snapshot maior para impedir que cópias snapshot usem espaço reservado para o sistema de arquivos ativo. Você pode diminuir a reserva de cópias Snapshot quando não precisar mais de espaço para cópias Snapshot.

Passo

1. Modificar a reserva de cópia Instantânea:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-percent-snapshot-space` *`snap_reserve`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir define a reserva de cópia Snapshot para `vol1` 10%:

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

Cópias Snapshot Autodelete

Você pode usar o `volume snapshot autodelete modify` comando para acionar a exclusão automática de cópias Snapshot quando a reserva Snapshot for excedida. Por padrão, as cópias Snapshot mais antigas são excluídas primeiro.

Sobre esta tarefa

Os clones de arquivos e LUN são excluídos quando não houver mais cópias Snapshot a serem excluídas.

Passo

1. Cópias Snapshot Autodelete

   `volume snapshot autodelete modify -vserver` *`SVM`* `-volume` *`volume`* `-enabled true|false -trigger volume|snap_reserve`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir exclui automaticamente as cópias Snapshot para `vol1` quando a reserva de cópias snapshot estiver esgotada:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Restaure arquivos de cópias Snapshot

Restaurar um arquivo a partir de uma cópia Snapshot em um cliente NFS ou SMB

Um usuário em um cliente NFS ou SMB pode restaurar um arquivo diretamente de uma cópia Snapshot sem a intervenção de um administrador do sistema de storage.

Cada diretório no sistema de arquivos contém um subdiretório chamado `.snapshot` acessível para usuários NFS e SMB. O `.snapshot` subdiretório contém subdiretórios correspondentes às cópias Snapshot do volume:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Cada subdiretório contém os arquivos referenciados pela cópia Snapshot. Se os usuários excluírem ou sobrescreverem acidentalmente um arquivo, eles poderão restaurar o arquivo para o diretório de leitura e gravação pai copiando o arquivo do subdiretório Snapshot para o diretório de leitura e gravação:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Ative e desative o acesso de clientes NFS e SMB ao diretório de cópia Snapshot

Você pode ativar e desativar o acesso ao diretório cópia Snapshot usando a opção `volume modify` CLI do comando ONTAP `-snapdir-access` e, começando com ONTAP 9.10,1, você pode usar o Gerenciador do sistema para habilitar ou desabilitar sistemas cliente para acessar um diretório cópia Snapshot em um volume. A ativação do acesso torna o diretório de cópia Snapshot visível para os clientes e permite que os clientes Windows mapeem uma unidade para o diretório de cópia Snapshot para

visualizar e acessar seu conteúdo. Os clientes NFS e SMB podem restaurar um arquivo ou LUN a partir de um snapshot.

Você pode ativar ou desativar o acesso ao diretório de cópia Snapshot de um volume editando as configurações de volume ou editando as configurações de compartilhamento do volume.

Ative ou desative o acesso do cliente ao diretório de cópia Snapshot editando um volume

Passos

Você pode ativar e desativar o acesso ao diretório de cópia Snapshot do cliente usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. Por padrão, o diretório cópia Snapshot em um volume está acessível aos clientes.

System Manager

1. Clique em **armazenamento > volumes**.
2. Selecione o volume que contém o diretório cópias Snapshot que deseja exibir ou ocultar.
3. Clique ⋮ e selecione **Editar**.
4. Na seção **Configurações de cópias instantâneas (locais)**, marque ou desmarque **Mostrar o diretório cópias instantâneas para clientes**.
5. Clique em **Salvar**.

CLI

1. Verifique o status de acesso ao diretório Snapshot:

   ```
   volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
   access
   ```

   Exemplo:

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
   access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

2. Ative ou desative o acesso ao diretório cópia Instantânea:

   ```
   volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
   <true|false>
   ```

   O exemplo a seguir habilita o acesso ao diretório de cópia Snapshot no vol1:

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
   true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

Ative ou desative o acesso do cliente ao diretório de cópia Snapshot editando um compartilhamento

Por padrão, o diretório cópia Snapshot em um volume está acessível aos clientes.

Passos

1. Clique em **armazenamento > compartilhamentos**.
2. Selecione o volume que contém o diretório cópias Snapshot que deseja exibir ou ocultar.

3. Clique ⋮ e selecione **Editar**.
4. Na seção **Propriedades de compartilhamento**, marque ou desmarque **permitir que os clientes acessem o diretório cópias Snapshot**.
5. Clique em **Salvar**.

Restaurar um único arquivo a partir de uma cópia Snapshot

Você pode usar o `volume snapshot restore-file` comando para restaurar um único arquivo ou LUN a partir de uma cópia Snapshot. Você pode restaurar o arquivo para um local diferente no volume de leitura e gravação pai se não quiser substituir um arquivo existente.

Sobre esta tarefa

Se você estiver restaurando um LUN existente, um clone de LUN será criado e feito backup na forma de uma cópia Snapshot. Durante a operação de restauração, você pode ler e gravar no LUN.

Os arquivos com fluxos são restaurados por padrão.

Passos

1. Listar as cópias Snapshot em um volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as cópias Snapshot `vol1` no :

   ```
   clus1::> volume snapshot show -vserver vs1 -volume vol1

   Vserver Volume Snapshot                State    Size  Total% Used%
   ------- ------ ---------- ----------- ------   -----  ------ -----
   vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
                  daily.2013-01-25_0010   valid   92KB      0%    0%
                  hourly.2013-01-25_0105  valid   228KB     0%    0%
                  hourly.2013-01-25_0205  valid   236KB     0%    0%
                  hourly.2013-01-25_0305  valid   244KB     0%    0%
                  hourly.2013-01-25_0405  valid   244KB     0%    0%
                  hourly.2013-01-25_0505  valid   244KB     0%    0%

   7 entries were displayed.
   ```

2. Restaurar um arquivo a partir de uma cópia Snapshot:

   `volume snapshot restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-restore-path` *`destination_path`*

   Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir restaura o arquivo `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Restaure parte de um arquivo a partir de uma cópia Snapshot

Você pode usar o `volume snapshot partial-restore-file` comando para restaurar um intervalo de dados de uma cópia Snapshot para um LUN ou para um arquivo de contentor NFS ou SMB, supondo que você saiba o deslocamento de byte inicial dos dados e a contagem de bytes. Você pode usar esse comando para restaurar um dos bancos de dados em um host que armazena vários bancos de dados no mesmo LUN.

A partir do ONTAP 9.12,1, a restauração parcial está disponível para volumes usando Sincronização ativa do SnapMirroro .

Passos

1. Listar as cópias Snapshot em um volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as cópias Snapshot `vol1` no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure parte de um arquivo a partir de uma cópia Snapshot:

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   O desvio de byte inicial e a contagem de bytes devem ser múltiplos de 4.096.

O exemplo a seguir restaura os primeiros 4.096 bytes do arquivo `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Restaure o conteúdo de um volume a partir de uma cópia Snapshot

Você pode recuperar um volume para um ponto anterior no tempo restaurando a partir de uma cópia Snapshot. Você pode usar o System Manager ou o `volume snapshot restore` comando para restaurar o conteúdo de um volume a partir de uma cópia Snapshot.

Sobre esta tarefa

Se o volume tiver relações SnapMirror, replique manualmente todas as cópias espelhadas do volume imediatamente após a restauração a partir de uma cópia Snapshot. Não fazer isso pode resultar em cópias espelhadas inutilizáveis que devem ser excluídas e recriadas.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para restaurar a partir de uma cópia Snapshot anterior.

System Manager

1. Clique em **armazenamento** e selecione um volume.
2. Em **cópias Snapshot**, clique ⋮ ao lado da cópia Snapshot que deseja restaurar e selecione **Restaurar**.

CLI

1. Listar as cópias Snapshot em um volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra as cópias Snapshot `vol1` no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure o conteúdo de um volume a partir de uma cópia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

O exemplo a seguir restaura o conteúdo `vol1` de :

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Replicação de volume SnapMirror

Noções básicas de recuperação de desastres assíncrona do SnapMirror

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

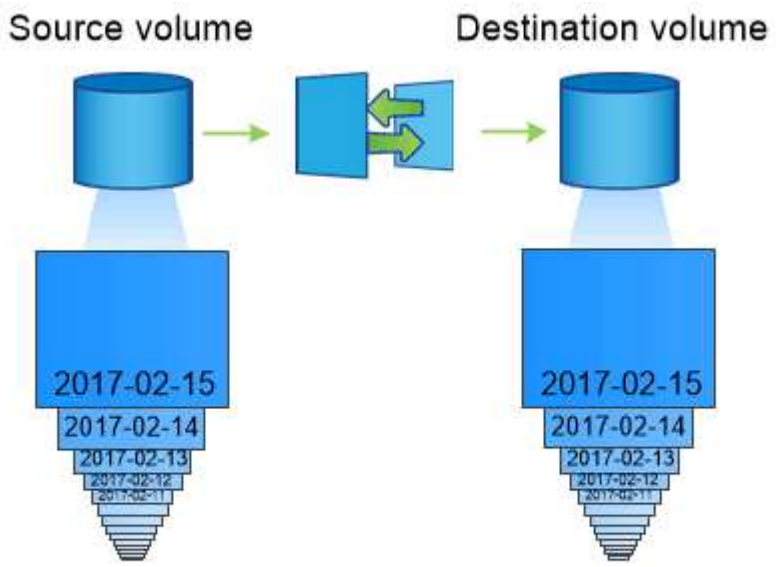
Se o site principal ainda estiver disponível para fornecer dados, você pode simplesmente transferir quaisquer dados necessários de volta para ele e não atender clientes do espelho. Como o caso de uso de failover indica, as controladoras no sistema secundário devem ser equivalentes ou quase equivalentes às controladoras no sistema primário para atender dados com eficiência do storage espelhado.

Relações de proteção de dados

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

"Peering de cluster e SVM"

A figura abaixo ilustra as relações de proteção de dados da SnapMirror.



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

Escopo das relações de proteção de dados

Você pode criar uma relação de proteção de dados diretamente entre volumes ou entre as SVMs que possuem os volumes. Em uma relação de proteção de dados *SVM,* toda ou parte da configuração SVM, de exportações de NFS e compartilhamentos de SMB para RBAC, são replicados, bem como os dados nos volumes proprietários do SVM.

Você também pode usar o SnapMirror para aplicativos especiais de proteção de dados:

- Uma cópia do volume raiz do SVM garante que os dados permaneçam acessíveis em caso de interrupção ou failover de nó.
- Uma relação de proteção de dados entre o *SnapLock volumes* permite replicar arquivos WORM para um storage secundário.

  "Arquivamento e conformidade com a tecnologia SnapLock"

- A partir do ONTAP 9.13,1, você pode usar o SnapMirror assíncrono para proteger grupos de consistência. A partir do ONTAP 9.14,1, você pode usar o SnapMirror assíncrono para replicar snapshots granular de volume para o cluster de destino usando a relação de grupo de consistência. Para obter mais informações, Configurar a proteção assíncrona do SnapMirrorconsulte .

Como as relações de proteção de dados do SnapMirror são inicializadas

Na primeira vez que você invocar o SnapMirror, ele executa uma *transferência de linha de base* do volume de origem para o volume de destino. A política *SnapMirror* da relação define o conteúdo da linha de base e quaisquer atualizações.

Uma transferência de linha de base sob a política SnapMirror padrão `MirrorAllSnapshots` envolve as seguintes etapas:

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

Como os relacionamentos de proteção de dados da SnapMirror são atualizados

As atualizações são assíncronas, seguindo a programação configurada. A retenção espelha a política do Snapshot na origem.

Em cada atualização sob `MirrorAllSnapshots` a política, o SnapMirror cria uma cópia Snapshot do volume de origem e transfere essa cópia Snapshot e todas as cópias Snapshot feitas desde a última atualização. Na saída a seguir do `snapmirror policy show` comando para a `MirrorAllSnapshots` política, observe o seguinte:

- `Create Snapshot` É "verdadeiro", indicando que `MirrorAllSnapshots` cria uma cópia Snapshot quando o SnapMirror atualiza o relacionamento.
- `MirrorAllSnapshots` Tem regras "sm_created" e "all_source_snapshots", indicando que tanto a cópia Snapshot criada pelo SnapMirror quanto todas as cópias snapshot que foram feitas desde a última atualização são transferidas quando o SnapMirror atualiza a relação.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

Política MirrorLatest

A política pré-configurada `MirrorLatest` funciona exatamente da mesma forma que `MirrorAllSnapshots`, exceto que apenas a cópia Snapshot criada pelo SnapMirror é transferida na inicialização e atualização.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

Noções básicas de recuperação de desastres síncrona SnapMirror

A partir do ONTAP 9.5, a tecnologia SnapMirror Synchronous (SM-S) é suportada em todas as plataformas FAS e AFF que tenham pelo menos 16 GB de memória e em todas as plataformas ONTAP Select. A tecnologia síncrona SnapMirror é um recurso licenciado

por nó que fornece replicação de dados síncrona no nível do volume.

Esse recurso atende aos mandatos regulatórios e nacionais para replicação síncrona nos setores financeiro, de saúde e outros que tenham regulamentação com perda de dados zero.

Operações síncronas do SnapMirror permitidas

O limite do número de operações de replicação síncrona SnapMirror por par de HA depende do modelo de controladora.

A tabela a seguir lista o número de operações síncronas do SnapMirror permitidas por par de HA de acordo com o tipo de plataforma e o lançamento do ONTAP.

Plataforma	Versões anteriores ao ONTAP 9.9,1	ONTAP 9.9,1	ONTAP 9.10,1	ONTAP 9.11,1 através de ONTAP 9.14,1
AFF	80	160	200	400
ASA	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

Recursos suportados

A tabela a seguir indica os recursos compatíveis com o SnapMirror Synchronous e as versões do ONTAP nas quais o suporte está disponível.

Recurso	Lançamento primeiro suportado	Informações adicionais
Antivírus sobre o volume principal da relação síncrona SnapMirror	ONTAP 9,6	
Replicação de cópia Snapshot criada pela aplicação	ONTAP 9,7	Se uma cópia Snapshot estiver marcada com o rótulo apropriado no momento `snapshot create` da operação, usando a CLI ou a API ONTAP, o SnapMirror Synchronous replica as cópias Snapshot, criadas pelo usuário ou criadas com scripts externos, após a desativação das aplicações. As cópias Snapshot programadas criadas usando uma política Snapshot não são replicadas. Para obter mais informações sobre como replicar cópias Snapshot criadas por aplicativos, consulte o artigo da base de dados de Conhecimento: "Como replicar snapshots criados pela aplicação com o SnapMirror síncrono".
Clonar a eliminação automática	ONTAP 9,6	

Agregados FabricPool com política de disposição em camadas nenhuma, Snapshot ou Automático são compatíveis com origem e destino síncronos SnapMirror.	ONTAP 9,5	O volume de destino em um agregado do FabricPool não pode ser definido para todas as políticas de disposição em camadas.
FC	ONTAP 9,5	Em todas as redes para as quais a latência não exceda 10ms ms
FC-NVMe	ONTAP 9,7	
Clones de arquivos	ONTAP 9,7	
FPolicy no volume principal da relação síncrona SnapMirror	ONTAP 9,6	
Cotas rígidas e flexíveis sobre o volume primário do relacionamento síncrono SnapMirror	ONTAP 9,6	As regras de cota não são replicadas para o destino; portanto, o banco de dados de cota não é replicado para o destino.
Relações síncronas intra-cluster	ONTAP 9.14,1	Alta disponibilidade é fornecida quando os volumes de origem e destino são colocados em diferentes pares de HA. Se todo o cluster ficar inativo, o acesso aos volumes não será possível até que o cluster seja recuperado. As relações síncronas de SnapMirror intramcluster contribuirão para o limite geral de simultâneos Relacionamentos por par de HA.
ISCSI	ONTAP 9,5	
Clones de LUN e clones de namespace NVMe	ONTAP 9,7	
Clones de LUN com respaldo de cópias Snapshot criadas pela aplicação	ONTAP 9,7	
Acesso a protocolo misto (NFS v3 e SMB)	ONTAP 9,6	
Restauração NDMP/NDMP	ONTAP 9.13,1	Tanto o cluster de origem quanto o de destino devem estar executando o ONTAP 9.13,1 ou posterior para usar o NDMP com o SnapMirror Synchronous. Para obter mais informações, Transfira dados usando cópia ndmpconsulte .
Operações síncronas de SnapMirror (NDO) sem interrupções em plataformas AFF/ASA, somente.	ONTAP 9.12,1	O suporte a operações sem interrupções permite que você execute muitas tarefas de manutenção comuns sem agendar o tempo de inatividade. As operações suportadas incluem takeover e giveback e movimentação de volume, desde que um único nó sobreviva a cada um dos dois clusters.
NFS v4.2	ONTAP 9.10,1	
NFS v4.3	ONTAP 9,5	
NFS v4.0	ONTAP 9,6	
NFS v4.1	ONTAP 9,6	

NVMe/TCP	9.10.1	
Remoção de limitação de frequência de operação de metadados elevados	ONTAP 9,6	
Segurança para dados confidenciais em trânsito usando criptografia TLS 1,2	ONTAP 9,6	
Restauração de arquivo único e parcial	ONTAP 9.13,1	
SMB 2,0 ou posterior	ONTAP 9,6	
Cascata de espelho-espelho síncrono SnapMirror	ONTAP 9,6	A relação do volume de destino da relação síncrona do SnapMirror deve ser uma relação assíncrona do SnapMirror.
Recuperação de desastres da SVM	ONTAP 9,6	* Uma fonte síncrona SnapMirror também pode ser uma fonte de recuperação de desastres do SVM, por exemplo, uma configuração de fan-out com SnapMirror síncrono como uma etapa e a recuperação de desastres do SVM, como a outra. * Uma fonte síncrona SnapMirror não pode ser um destino de recuperação de desastres da SVM, pois o SnapMirror síncrono não oferece suporte a uma fonte de proteção de dados em cascata. É necessário liberar a relação síncrona antes de executar uma flip-ressincronização da recuperação de desastres da SVM no cluster de destino. * Um destino síncrono do SnapMirror não pode ser uma fonte de recuperação de desastres do SVM, pois a recuperação de desastres do SVM não dá suporte à replicação de volumes de DP. Uma nova sincronização da fonte síncrona resultaria na recuperação de desastres da SVM, excluindo o volume de DP no cluster de destino.
Restauração baseada em fita para o volume de origem	ONTAP 9.13,1	
Paridade de carimbo de data/hora entre volumes de origem e destino para nas	ONTAP 9,6	Se você atualizou do ONTAP 9.5 para o ONTAP 9.6, o carimbo de data/hora será replicado apenas para quaisquer arquivos novos e modificados no volume de origem. O carimbo de data/hora dos arquivos existentes no volume de origem não é sincronizado.

Funcionalidades não suportadas

Os recursos a seguir não são compatíveis com relacionamentos síncronos do SnapMirror:

- Grupos de consistência
- Sistemas DP_Optimized (DPO)
- Volumes FlexGroup
- Volumes FlexCache
- Limitação global

- Em uma configuração de fan-out, apenas uma relação pode ser uma relação síncrona do SnapMirror; todas as outras relações do volume de origem devem ser relações assíncronas do SnapMirror.
- Movimento LUN
- Configurações do MetroCluster
- LUNs de acesso mistos SAN e NVMe e namespaces NVMe não são compatíveis com o mesmo volume ou SVM.
- SnapCenter
- Volumes SnapLock
- Cópias Snapshot à prova de violações
- Backup ou restauração em fita usando dump e SMTape no volume de destino
- Piso de taxa de transferência (QoS min) para volumes de origem
- Volume SnapRestore
- VVol

Modos de funcionamento

O SnapMirror Synchronous tem dois modos de operação com base no tipo da política SnapMirror usada:

- **Modo de sincronização** no modo de sincronização, as operações de e/S do aplicativo são enviadas em paralelo aos sistemas de armazenamento primário e secundário. Se a gravação no storage secundário não for concluída por qualquer motivo, o aplicativo poderá continuar gravando no storage primário. Quando a condição de erro é corrigida, a tecnologia síncrona SnapMirror ressincroniza automaticamente com o storage secundário e retoma a replicação do storage primário para o storage secundário no modo síncrono. No modo de sincronização, o RPO 0 e o rto são muito baixos até que ocorra uma falha de replicação secundária no momento em que o RPO e o rto se tornam indeterminados, mas equivalem ao tempo de reparar o problema que fez com que a replicação secundária falhasse e para que o ressync fosse concluído.
- **Modo StrictSync** SnapMirror síncrono pode operar opcionalmente no modo StrictSync. Se a gravação no storage secundário não for concluída por qualquer motivo, a e/S do aplicativo falhará, garantindo assim que o storage primário e secundário sejam idênticos. A e/S da aplicação para o primário é retomada somente após a relação SnapMirror retornar ao `InSync` status. Se o storage primário falhar, a e/S da aplicação poderá ser retomada no storage secundário, após o failover, sem perda de dados. No modo StrictSync, o RPO é sempre zero, e o rto é muito baixo.

Status do relacionamento

O status de uma relação síncrona SnapMirror está sempre no `InSync` status durante a operação normal. Se a transferência SnapMirror falhar por qualquer motivo, o destino não está sincronizado com a origem e pode ir para o `OutofSync` status.

Para relações síncronas do SnapMirror, o sistema verifica automaticamente o status da relação `InSync`ou `OutofSync`) em um intervalo fixo. Se o status do relacionamento for `OutofSync`, o ONTAP acionará automaticamente o processo de ressincronização automática para trazer de volta a relação ao `InSync` status. A ressincronização automática é acionada apenas se a transferência falhar devido a qualquer operação, como failover não planejado de armazenamento na origem ou destino ou uma interrupção de rede. Operações iniciadas pelo usuário, `snapmirror quiesce` como e `snapmirror break` não acionam a ressincronização automática.

Se o status do relacionamento se tornar `OutofSync` para um relacionamento síncrono SnapMirror no modo

StrictSync, todas as operações de e/S para o volume primário serão interrompidas. `OutofSync`O estado da relação síncrona SnapMirror no modo de sincronização não causa interrupções para as operações primárias e/S são permitidas no volume primário.

Informações relacionadas

"Relatório técnico da NetApp 4733: Configuração síncrona da SnapMirror e práticas recomendadas"

Políticas de proteção padrão

O ONTAP inclui várias políticas de proteção padrão que você pode usar para seus relacionamentos de proteção de dados. A política que você usa depende do tipo de relação de proteção.

Se as políticas padrão não atenderem às suas necessidades de relacionamentos de proteção de dados, você poderá "crie uma política personalizada".

Lista de políticas e descrições de proteção padrão

As políticas de proteção padrão e seus tipos de política associados são descritos abaixo.

Nome	Descrição	Tipo de política
Assíncrono	Uma política unificada de cofre e assíncrono SnapMirror para espelhamento do sistema de arquivos ativo mais recente e snapshots diários e semanais com um agendamento de transferência por hora.	Assíncrono
AutomatedFailOver	Política para SnapMirror síncrona com garantia de rto zero, em que a e/S do cliente não será interrompida em caso de falha de replicação.	Síncrono
AutomatedFailOverDuplex	Política para SnapMirror síncrono com garantia de rto zero e replicação de sincronização bidirecional.	Síncrono
CloudBackupDefault	Política de cofre com regra diária.	Assíncrono
Contínuo	Política para espelhamento de bucket S3.	Contínuo
DailyBackup	Política de cofre com uma regra diária e um cronograma de transferência diário.	Assíncrono
DPDefault	Política assíncrona do SnapMirror para espelhamento de todas as cópias Snapshot e do sistema de arquivos ativo mais recente.	Assíncrono
MirrorAllinstantâneos	Política assíncrona do SnapMirror para espelhamento de todos os snapshots e o sistema de arquivos ativo mais recente.	Assíncrono
MirrorAllSnapshotsDiscardNetwork	Política assíncrona do SnapMirror para espelhamento de todos os snapshots e o sistema de arquivos ativo mais recente, excluindo as configurações de rede.	Assíncrono

Nome	Descrição	Tipo de política
MirrorAndVault	Uma política unificada de cofre e assíncrono do SnapMirror para espelhamento do sistema de arquivos ativo mais recente e snapshots diários e semanais.	Assíncrono
MirrorAndVaultDiscardNetwork	Uma política unificada de cofre e assíncrono SnapMirror para espelhamento do sistema de arquivos ativo mais recente e instantâneos diários e semanais, excluindo as configurações de rede.	Assíncrono
MirrorLatest	Política assíncrona do SnapMirror para espelhamento do sistema de arquivos ativo mais recente.	Assíncrono
SnapCenterSync	Política para SnapMirror síncrono para SnapCenter com a configuração Snapshot criada pela aplicação.	Síncrono
StrictSync	Política para SnapMirror síncrono em que o acesso do cliente será interrompido em caso de falha de replicação.	Síncrono
Síncrono	Política para SnapMirror síncrono em que o acesso do cliente não será interrompido em caso de falha de replicação.	Síncrono
Unified7year	Política de SnapMirror unificado com retenção de 7 anos.	Assíncrono
XDPDefat	Política de cofre com regras diárias e semanais.	Assíncrono

Sobre workloads compatíveis com políticas de StrictSync e sincronização

As políticas StrictSync e Sync são compatíveis com todas as aplicações baseadas em LUN com protocolos FC, iSCSI e FC-NVMe, bem como com os protocolos NFSv3 e NFSv4 para aplicações empresariais, como bancos de dados, VMware, cota, SMB etc. A partir do ONTAP 9.6, o SnapMirror síncrono pode ser usado para serviços de arquivos empresariais, como automação de design eletrônico (EDA), diretórios base e workloads de compilação de software.

No ONTAP 9.5, para uma política de sincronização, você precisa considerar alguns aspectos importantes ao selecionar as cargas de trabalho NFSv3 ou NFSv4. A quantidade de operações de leitura ou gravação de dados por workloads não é uma consideração, já que a política de sincronização pode lidar com workloads de e/S de alta leitura ou gravação. No ONTAP 9.5, as cargas de trabalho que têm criação excessiva de arquivos, criação de diretórios, alterações de permissão de arquivo ou alterações de permissão de diretório podem não ser adequadas (essas são chamadas de cargas de trabalho de alto metadados). Um exemplo típico de um workload de metadados altos é um workload de DevOps no qual você cria vários arquivos de teste, executa a automação e exclui os arquivos. Outro exemplo é a carga de trabalho de compilação paralela que gera vários arquivos temporários durante a compilação. O impactos de uma alta taxa de atividade de metadados de gravação é que ela pode fazer com que a sincronização entre espelhos quebre temporariamente, o que bloqueia o iOS de leitura e gravação do cliente.

A partir do ONTAP 9.6, essas limitações são removidas e o SnapMirror síncrono pode ser usado para workloads de serviços de arquivos empresariais que incluem ambientes de vários usuários, como diretórios base e workloads de compilação de software.

Informações relacionadas

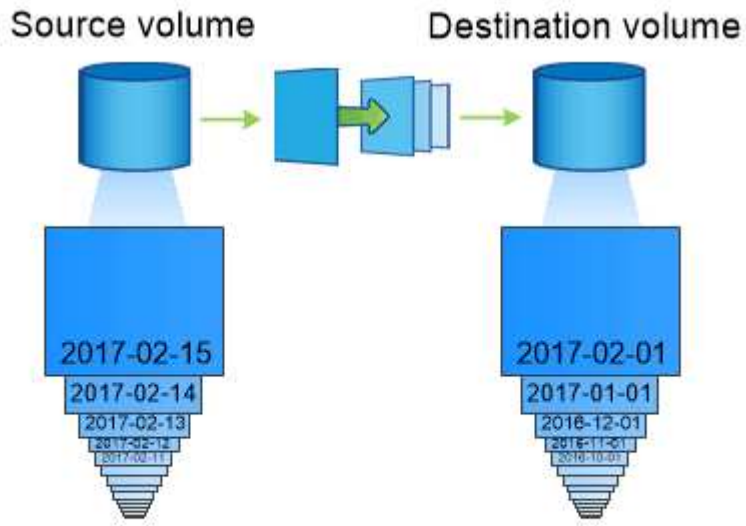
"Configuração síncrona SnapMirror e práticas recomendadas"

Arquivamento de cofre usando a tecnologia SnapMirror

As políticas do SnapMirror Vault substituem a tecnologia SnapVault no ONTAP 9.3 e posterior. Você usa uma política de cofre do SnapMirror para replicação de cópia Snapshot de disco para disco para conformidade com padrões e outros fins relacionados à governança. Em contraste com uma relação do SnapMirror, em que o destino geralmente contém apenas as cópias Snapshot atualmente no volume de origem, um destino do Vault normalmente retém cópias Snapshot pontuais criadas por um período muito mais longo.

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

A figura abaixo ilustra as relações de proteção de dados do SnapMirror Vault.



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

Como as relações de proteção de dados do Vault são inicializadas

A política SnapMirror para o relacionamento define o conteúdo da linha de base e quaisquer atualizações.

Uma transferência de linha de base sob a política de Vault padrão `XDPDefault` faz uma cópia Snapshot do volume de origem e, em seguida, transfere essa cópia e os dados bloqueiam as referências ao volume de destino. Diferentemente dos relacionamentos do SnapMirror, um backup de Vault não inclui cópias Snapshot mais antigas na linha de base.

Como os relacionamentos de proteção de dados do Vault são atualizados

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

Em cada atualização sob `XDPDefault` a política, o SnapMirror transfere cópias Snapshot feitas desde a última atualização, desde que tenham rótulos que correspondam aos rótulos definidos nas regras da política. Na saída a seguir do `snapmirror policy show` comando para a `XDPDefault` política, observe o seguinte:

- `Create Snapshot` É falso, indicando que `XDPDefault` não cria uma cópia Snapshot quando o SnapMirror atualiza a relação.
- `XDPDefault` Tem regras "diárias" e "semanais", indicando que todas as cópias Snapshot com rótulos correspondentes na origem são transferidas quando o SnapMirror atualiza o relacionamento.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                    Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
            Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Noções básicas de replicação unificada da SnapMirror

O SnapMirror *Unified replication* permite configurar a recuperação de desastres e o arquivamento no mesmo volume de destino. Quando a replicação unificada é apropriada,

ela oferece benefícios na redução da quantidade de storage secundário de que você precisa, limitando o número de transferências de linha de base e diminuindo o tráfego de rede.

Como os relacionamentos de proteção de dados unificada são inicializados

Assim como no SnapMirror, a proteção de dados unificada realiza uma transferência de linha de base na primeira vez que você a invoca. A política SnapMirror para o relacionamento define o conteúdo da linha de base e quaisquer atualizações.

Uma transferência de linha de base sob a política de proteção de dados unificada padrão `MirrorAndVault` faz uma cópia Snapshot do volume de origem e, em seguida, transfere essa cópia e os blocos de dados que ela faz referência ao volume de destino. Assim como o arquivamento de cofres, a proteção de dados unificada não inclui cópias Snapshot mais antigas na linha de base.

Como os relacionamentos unificados de proteção de dados são atualizados

Em cada atualização sob `MirrorAndVault` a política, o SnapMirror cria uma cópia Snapshot do volume de origem e transfere essa cópia Snapshot e todas as cópias Snapshot feitas desde a última atualização, desde que tenham rótulos que correspondam aos rótulos definidos nas regras de política de snapshot. Na saída a seguir do `snapmirror policy show` comando para a `MirrorAndVault` política, observe o seguinte:

- `Create Snapshot` É "verdadeiro", indicando que `MirrorAndVault` cria uma cópia Snapshot quando o SnapMirror atualiza o relacionamento.
- `MirrorAndVault` Tem regras "sm_created", "daily" e "semanal", indicando que tanto a cópia Snapshot criada pelo SnapMirror quanto as cópias Snapshot com rótulos correspondentes na fonte são transferidas quando o SnapMirror atualiza a relação.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Política do Unified7year

A política pré-configurada `Unified7year` funciona exatamente da mesma maneira que `MirrorAndVault`o , exceto que uma quarta regra transfere cópias Snapshot mensais e as retém por sete anos.

```
                          Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                                 ----------------     ----  -------- ----
-------- ------
                                 sm_created              1  false       0 -
-
                                 daily                   7  false       0 -
-
                                 weekly                 52  false       0 -
-
                                 monthly                84  false       0 -
-
```

Proteja-se contra possíveis corrupção de dados

A replicação unificada limita o conteúdo da transferência da linha de base para a cópia Snapshot criada pelo SnapMirror na inicialização. Em cada atualização, o SnapMirror cria outra cópia Snapshot da origem e transfere essa cópia Snapshot e quaisquer novas cópias Snapshot que tenham rótulos correspondentes aos rótulos definidos nas regras de política do Snapshot.

Você pode se proteger contra a possibilidade de que uma cópia Snapshot atualizada seja corrompida criando uma cópia da última cópia Snapshot transferida no destino. Essa cópia local é mantida independentemente das regras de retenção na origem, de modo que, mesmo que o Snapshot originalmente transferido pelo SnapMirror não esteja mais disponível na origem, uma cópia dele estará disponível no destino.

Quando usar a replicação de dados unificada

Você precisa pesar o benefício de manter um espelhamento completo em relação às vantagens que a replicação unificada oferece na redução da quantidade de storage secundário, na limitação do número de transferências de linha de base e na diminuição do tráfego de rede.

O fator chave para determinar a adequação da replicação unificada é a taxa de alteração do sistema de arquivos ativo. Um espelho tradicional pode ser mais adequado para um volume que armazena cópias Snapshot por hora de logs de transações de banco de dados, por exemplo.

O XDP substitui o DP como o padrão SnapMirror

A partir do ONTAP 9.3, o modo SnapMirror Extended Data Protection (XDP) substitui o modo SnapMirror Data Protection (DP) como padrão do SnapMirror.

Antes de atualizar para o ONTAP 9.12,1, você deve converter relações de tipo DP existentes para XDP antes de poder atualizar para o ONTAP 9.12,1 e versões posteriores. Para obter mais informações, "Converta uma relação de tipo DP existente para XDP"consulte .

Até o ONTAP 9.3, o SnapMirror invocado no modo DP e o SnapMirror invocado no modo XDP usavam diferentes mecanismos de replicação, com diferentes abordagens para dependência de versão:

- O SnapMirror invocado no modo DP usou um mecanismo de replicação *dependente da versão* no qual a versão do ONTAP era necessária para ser a mesma no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- O SnapMirror invocado no modo XDP usou um mecanismo de replicação *version-flexivel* que suportava diferentes versões do ONTAP no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Com melhorias no desempenho, os benefícios significativos do SnapMirror flexível de versão superam a ligeira vantagem na taxa de transferência de replicação obtida com o modo dependente da versão. Por esse motivo, começando com ONTAP 9.3, o modo XDP foi feito o novo padrão, e todas as invocações do modo DP na linha de comando ou em scripts novos ou existentes são automaticamente convertidas para o modo XDP.

As relações existentes não são afetadas. Se uma relação já for do tipo DP, ela continuará sendo do tipo DP. A partir do ONTAP 9.5, o MirrorAndVault é a nova política padrão quando nenhum modo de proteção de dados é especificado ou quando o modo XDP é especificado como o tipo de relacionamento. A tabela abaixo mostra o comportamento que você pode esperar.

Se especificar…	O tipo é…	A política padrão (se você não especificar uma política) é…
DP	XDP	Espelhamento AllSnapshots (SnapMirror DR)
Nada	XDP	MirrorAndVault (replicação unificada)
XDP	XDP	MirrorAndVault (replicação unificada)

Como mostra a tabela, as políticas padrão atribuídas ao XDP em diferentes circunstâncias garantem que a conversão mantenha a equivalência funcional dos tipos antigos. É claro que você pode usar políticas diferentes conforme necessário, incluindo políticas para replicação unificada:

Se especificar…	E a política é…	O resultado é…
DP	MirrorAllinstantâneos	SnapMirror DR
XDPDefat	SnapVault	MirrorAndVault
Replicação unificada	XDP	MirrorAllinstantâneos
SnapMirror DR	XDPDefat	SnapVault

As únicas exceções à conversão são as seguintes:

- As relações de proteção de dados do SVM continuam como padrão no modo DP no ONTAP 9.3 e versões anteriores.

  A partir do ONTAP 9.4, as relações de proteção de dados do SVM passam por padrão no modo XDP.

- As relações de proteção de dados de compartilhamento de carga de volume raiz continuam a ser padrão para o modo DP.
- As relações de proteção de dados do SnapLock continuam a ser padrão para o modo DP no ONTAP 9.4 e anterior.

  A partir do ONTAP 9.5, as relações de proteção de dados do SnapLock são padrão para o modo XDP.

- As invocações explícitas do DP continuam a ser padrão para o modo DP se você definir a seguinte opção em todo o cluster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Essa opção será ignorada se você não invocar explicitamente o DP.

Quando um volume de destino cresce automaticamente

Durante uma transferência espelhada de proteção de dados, o volume de destino aumenta automaticamente em tamanho se o volume de origem tiver crescido, desde que haja espaço disponível no agregado que contenha o volume.

Este comportamento ocorre independentemente de qualquer definição de crescimento automático no destino. Você não pode limitar o crescimento do volume ou impedir que o ONTAP o aumente.

Por padrão, os volumes de proteção de dados são definidos para o `grow_shrink` modo automático, o que permite que o volume cresça ou diminua em resposta à quantidade de espaço usado. O dimensionamento automático máximo para volumes de proteção de dados é igual ao tamanho máximo de FlexVol e depende da plataforma. Por exemplo:

- FAS8200, volume DP padrão máximo-dimensionamento automático: 100TB

Para obter mais informações, "NetApp Hardware Universe"consulte .

Implantações de proteção de dados em cascata e fan-out

Você pode usar uma implantação *fan-out* para estender a proteção de dados a vários sistemas secundários. Você pode usar uma implantação *Cascade* para estender a proteção de dados para sistemas terciários.

As implantações em fan-out e em cascata são compatíveis com qualquer combinação de recuperação de desastres, SnapVault ou replicação unificada da SnapMirror. A partir do ONTAP 9.5, as relações síncronas do SnapMirror são compatíveis com implantações fan-out com uma ou mais relações assíncronas do SnapMirror. Apenas uma relação na configuração de fan-out pode ser uma relação síncrona SnapMirror, todas as outras relações do volume de origem devem ser relações assíncronas do SnapMirror. As relações síncronas do SnapMirror também são compatíveis com implantações em cascata (a partir de ONTAP 9.6). No entanto, a relação do volume de destino da relação síncrona do SnapMirror deve ser uma relação assíncrona do

SnapMirror. Sincronização ativa do SnapMirror (Suportado a partir do ONTAP 9.3,1) também suporta configurações de fan-out.

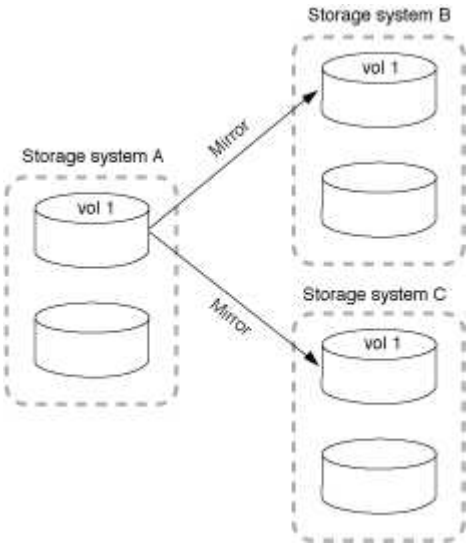
Você pode usar uma implantação *fan-in* para criar relações de proteção de dados entre vários sistemas primários e um único sistema secundário. Cada relação deve usar um volume diferente no sistema secundário.

Você deve estar ciente de que os volumes que fazem parte de uma configuração de fan-out ou cascata podem levar mais tempo para ressincronizar. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

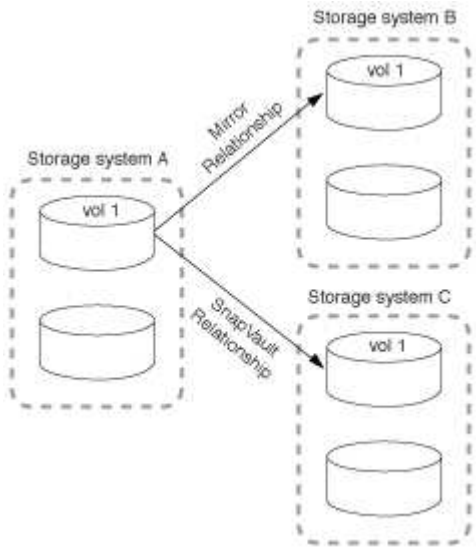
Como as implantações de fan-out funcionam

O SnapMirror suporta implantações de fan-out *multiple-mirrors* e *mirror-Vault*.

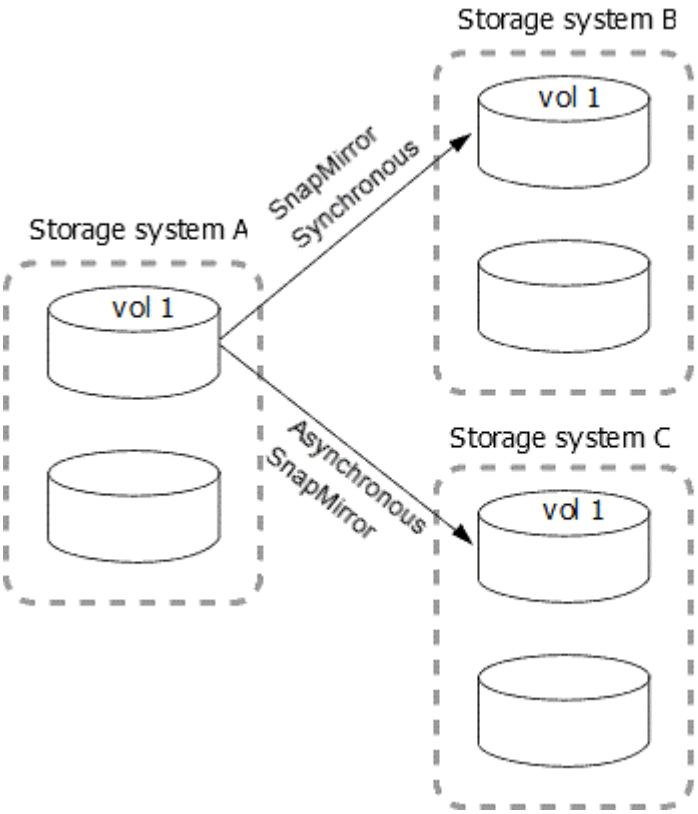
Uma implantação de fan-out de vários espelhos consiste em um volume de origem que tem uma relação espelhada com vários volumes secundários.



Uma implantação de fan-out do mirror-Vault consiste em um volume de origem que tem uma relação de espelhamento com um volume secundário e uma relação de SnapVault com um volume secundário diferente.



A partir do ONTAP 9.5, você pode ter implantações de fan-out com relacionamentos síncronos do SnapMirror; no entanto, apenas uma relação na configuração de fan-out pode ser uma relação síncrona do SnapMirror, todas as outras relações do volume de origem devem ser relações assíncronas do SnapMirror.

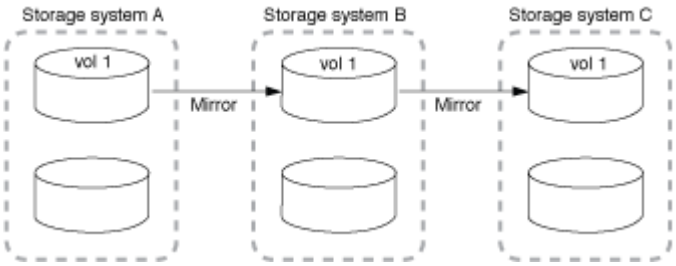


Como as implantações em cascata funcionam

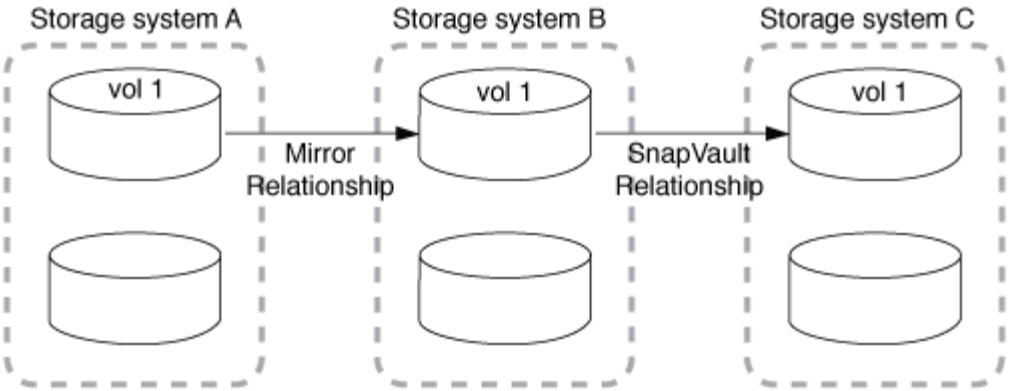
O SnapMirror suporta implantações em cascata *mirror-mirror*, *mirror-Vault*, *Vault-mirror* e *Vault-Vault*.

Uma implantação em cascata espelhada consiste em uma cadeia de relacionamentos em que um volume de origem é espelhado em um volume secundário e o volume secundário é espelhado em um volume terciário. Se o volume secundário ficar indisponível, é possível sincronizar a relação entre os volumes primário e terciário sem efetuar uma nova transferência de linha de base.

A partir do ONTAP 9.6, as relações síncronas do SnapMirror são suportadas em uma implantação em cascata espelhada. Somente os volumes primário e secundário podem estar em uma relação síncrona do SnapMirror. A relação entre os volumes secundários e os volumes terciários deve ser assíncrona.



Uma implantação em cascata de cofre-espelho consiste em uma cadeia de relacionamentos em que um volume de origem é espelhado em um volume secundário, e o volume secundário é abobadado a um volume terciário.



Vault-mirror e, a partir do ONTAP 9.2, as implantações em cascata Vault-Vault também são suportadas:

- Uma implantação em cascata de espelho de cofre consiste em uma cadeia de relacionamentos em que um volume de origem é abobadado para um volume secundário, e o volume secundário é espelhado para um volume terciário.
- (Começando com ONTAP 9.2) Uma implantação em cascata de Vault-Vault consiste em uma cadeia de relacionamentos em que um volume de origem é abobadado para um volume secundário e o volume secundário é abobadado para um volume terciário.

Leitura adicional

- Retome a proteção em uma configuração de fan-out com a sincronização ativa do SnapMirror

Licenciamento do SnapMirror

Visão geral do licenciamento do SnapMirror

A partir do ONTAP 9.3, o licenciamento foi simplificado para replicação entre instâncias do ONTAP. Nas versões do ONTAP 9, a licença do SnapMirror suporta relações de cofre e espelho. Você pode usar uma licença do SnapMirror para dar suporte à replicação do ONTAP para casos de uso de backup e recuperação de desastres.

Antes da versão do ONTAP 9.3, uma licença SnapVault separada era necessária para configurar relações *Vault* entre instâncias do ONTAP, onde a instância DP poderia reter um número maior de cópias Snapshot para suportar casos de uso de backup com tempos de retenção mais longos, e uma licença SnapMirror era necessária para configurar relações *mirror* entre instâncias do ONTAP, onde cada instância do ONTAP manteria o mesmo número de cópias Snapshot (ou seja, uma imagem *mirror*) para permitir o uso de falhas de recuperação de cluster. Ambas as licenças SnapMirror e SnapVault continuam a ser usadas e suportadas para versões do ONTAP 8.x e 9.x.

Embora as licenças do SnapVault continuem a funcionar e sejam suportadas para ambas as versões do ONTAP 8.x e 9.x, a licença do SnapMirror pode ser usada em vez de uma licença SnapVault e pode ser usada para configurações de espelhamento e cofre.

Para replicação assíncrona do ONTAP, a partir do ONTAP 9.3, um único mecanismo de replicação unificada é usado para configurar políticas de modo de proteção de dados estendida (XDP), em que a licença do SnapMirror pode ser configurada para uma política de espelhamento, uma política de cofre ou uma política de cofre-espelho. É necessária uma licença SnapMirror nos clusters de origem e destino. Uma licença SnapVault não é necessária se uma licença SnapMirror já estiver instalada. A licença perpétua assíncrona do SnapMirror está incluída no pacote de software ONTAP One que é instalado nos novos sistemas AFF e FAS.

Os limites de configuração de proteção de dados são determinados usando vários fatores, incluindo a versão do ONTAP, a plataforma de hardware e as licenças instaladas. Para obter mais informações, "Hardware Universe"consulte .

Licença síncrona SnapMirror

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas. Você precisa das seguintes licenças para criar um relacionamento síncrono do SnapMirror:

- A licença síncrona do SnapMirror é necessária no cluster de origem e no cluster de destino.

  A licença síncrona do SnapMirror faz parte do "Pacote de licenças ONTAP One".

  Se o seu sistema tiver sido adquirido antes de junho de 2019 com um pacote Premium ou Flash, você poderá baixar uma chave mestra NetApp para obter a licença síncrona SnapMirror necessária no site de suporte da NetApp: "Chaves da licença principal".

- A licença SnapMirror é necessária no cluster de origem e no cluster de destino.

Licença de nuvem da SnapMirror

A partir do ONTAP 9.8, a licença de nuvem do SnapMirror fornece replicação assíncrona de cópias Snapshot de instâncias do ONTAP para pontos de extremidade de storage de objetos. Os destinos de replicação podem ser configurados usando armazenamentos de objetos no local e serviços de storage de objetos em nuvem pública compatíveis com S3 e S3. Os relacionamentos de nuvem da SnapMirror são compatíveis com sistemas ONTAP para destinos de storage de objetos pré-qualificados.

A nuvem do SnapMirror não está disponível como uma licença autônoma. Apenas uma licença é necessária por cluster do ONTAP. Além de uma licença de nuvem do SnapMirror, a licença assíncrona do SnapMirror também é necessária.

Você precisa das seguintes licenças para criar um relacionamento de nuvem do SnapMirror:

- Uma licença SnapMirror e uma licença de nuvem SnapMirror para replicação diretamente no endpoint do armazenamento de objetos.
- Ao configurar um fluxo de trabalho de replicação de várias políticas (por exemplo, disco para disco para nuvem), é necessária uma licença SnapMirror em todas as instâncias do ONTAP, enquanto a licença de nuvem do SnapMirror é necessária apenas para o cluster de origem que está replicando diretamente para o endpoint de armazenamento de objetos.

Começando com ONTAP 9.9,1, você pode "Use o System Manager para replicação na nuvem do SnapMirror".

Uma lista de aplicativos de terceiros autorizados na nuvem da SnapMirror é publicada no site da NetApp.

Licença otimizada de proteção de dados

As licenças de proteção de dados otimizada (DPO) não estão mais sendo vendidas e o DPO não é suportado nas plataformas atuais; no entanto, se você tiver uma licença de DPO instalada em uma plataforma compatível, o NetApp continuará fornecendo suporte até o final da disponibilidade dessa plataforma.

O DPO não está incluído com o pacote de licenças ONTAP One e não pode atualizar para o pacote de licenças ONTAP One se a licença DPO estiver instalada num sistema.

Para obter informações sobre plataformas compatíveis, "Hardware Universe" consulte .

Instalar licenças de nuvem do SnapMirror

Os relacionamentos de nuvem do SnapMirror podem ser orquestrados usando aplicativos de backup de terceiros pré-qualificados. A partir do ONTAP 9.9,1, você também pode usar o System Manager para orquestrar a replicação na nuvem do SnapMirror. As licenças de capacidade de nuvem do SnapMirror e do SnapMirror são necessárias ao usar o System Manager para orquestrar ONTAP on-premises para backups de storage de objetos. Você também precisará solicitar e instalar a licença da API de nuvem do SnapMirror.

Sobre esta tarefa

A nuvem SnapMirror e as licenças do SnapMirror S3 são licenças de cluster, não de nós, portanto, elas *não* são entregues com o pacote de licenças do ONTAP One. Essas licenças estão incluídas no pacote de compatibilidade ONTAP One separado. Se você quiser habilitar a nuvem do SnapMirror, precisará solicitar este pacote.

Além disso, a orquestração do System Manager dos backups da nuvem do SnapMirror para o storage de objetos requer uma chave de API de nuvem da SnapMirror. Essa licença de API é uma licença de cluster de instância única, o que significa que não precisa ser instalada em todos os nós do cluster.

Passos

Você precisa solicitar e baixar o pacote de compatibilidade do ONTAP One e a licença da API de nuvem do SnapMirror e instalá-los usando o Gerenciador de sistema.

1. Localize e grave o UUID de cluster para o cluster que deseja licenciar.

   O UUID do cluster é necessário quando você envia sua solicitação para solicitar o pacote de compatibilidade do ONTAP One para o cluster.

2. Entre em Contato com sua equipe de vendas da NetApp e solicite o pacote de compatibilidade do ONTAP One.
3. Solicite a licença da API de nuvem da SnapMirror seguindo as instruções fornecidas no site de suporte da NetApp.

   "Solicite a chave de licença da API de nuvem da SnapMirror"

4. Quando você receber e baixar os arquivos de licença, use o Gerenciador do sistema para fazer o upload do NLF de compatibilidade da nuvem do ONTAP e do NLF da API da nuvem do SnapMirror para o cluster:
   a. Clique em **Cluster > Settings**.
   b. Na janela **Settings**, clique em **Licenses**.
   c. Na janela **Licenses**, clique + Add em .
   d. Na caixa de diálogo **Add License** (Adicionar licença), clique em **Browse** (Procurar) para selecionar o NLF transferido e, em seguida, clique em **Add** (Adicionar) para carregar o ficheiro para o cluster.

Informações relacionadas

"Faça backup dos dados na nuvem usando o SnapMirror"

"Pesquisa de licença de software NetApp"

Os sistemas DPO apresentam melhorias

A partir do ONTAP 9.6, o número máximo de volumes FlexVol suportados aumenta quando a licença DP_Optimized (DPO) é instalada. A partir do ONTAP 9.4, os sistemas com licença de DPO dão suporte a SnapMirror backoff, deduplicação em segundo plano entre volumes, uso de blocos Snapshot como doadores e compactação.

A partir do ONTAP 9.6, o número máximo de volumes FlexVol com suporte em sistemas secundários ou de proteção de dados aumentou, permitindo que você escale até 2.500 volumes FlexVol por nó ou até 5.000 TB no modo failover. O aumento dos volumes FlexVol é ativado com o "Licença DP_Optimized (DPO)". Ainda é necessário um "Licença SnapMirror"nos nós de origem e de destino.

A partir do ONTAP 9.4, os seguintes aprimoramentos de recursos são feitos nos sistemas DPO:

- SnapMirror backoff: Nos sistemas DPO, o tráfego de replicação tem a mesma prioridade que as cargas de trabalho do cliente são dadas.

  O backoff do SnapMirror é desativado por padrão nos sistemas DPO.

- Deduplicação em segundo plano do volume e deduplicação em segundo plano entre volumes: A deduplicação em segundo plano do volume e a deduplicação em segundo plano entre volumes são ativadas em sistemas DPO.

  Você pode executar `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` o comando para deduplicar os dados existentes. A prática recomendada é executar o comando durante horas fora do pico para reduzir o impactos no desempenho.

- Maior economia ao usar blocos Snapshot como doadores: Os blocos de dados que não estão disponíveis no sistema de arquivos ativo, mas estão presos em cópias Snapshot são usados como doadores para deduplicação de volume.

  Os novos dados podem ser deduplicados com os dados retidos nas cópias Snapshot. Eles também compartilham os blocos Snapshot com eficiência. O maior espaço de doadores oferece mais economia, especialmente quando o volume tem um grande número de cópias Snapshot.

- Compactação: A compactação de dados está ativada por padrão nos volumes DPO.

Gerenciar a replicação de volume do SnapMirror

Fluxo de trabalho de replicação do SnapMirror

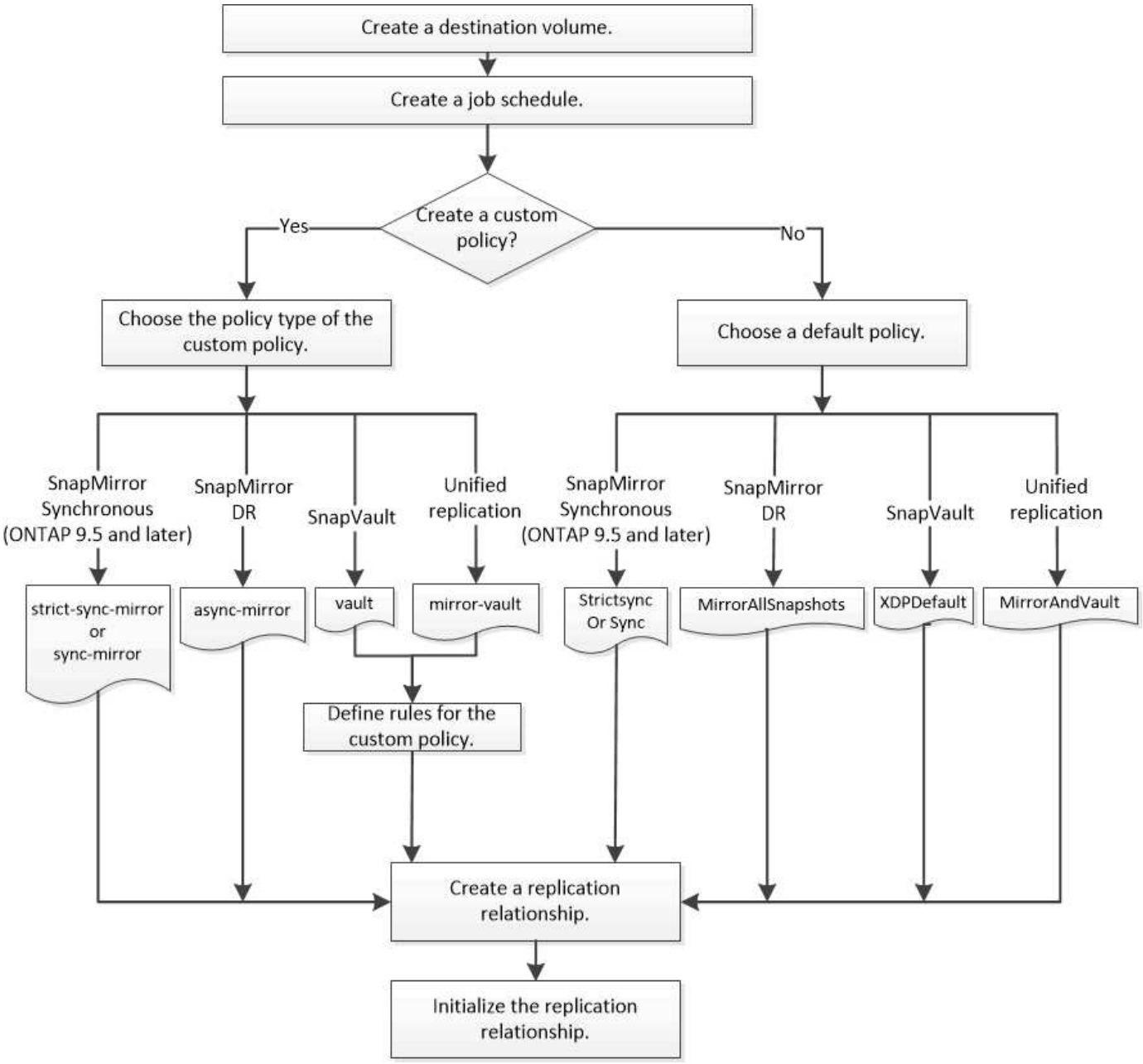
O SnapMirror oferece três tipos de relação de proteção de dados: Recuperação de desastres do SnapMirror, arquivamento (anteriormente conhecido como SnapVault) e replicação unificada. Você pode seguir o mesmo fluxo de trabalho básico para configurar cada tipo de relacionamento.

A partir da disponibilidade geral no ONTAP 9.9,1"Sincronização ativa do SnapMirror", fornece objetivo de tempo de recuperação zero (rto zero) ou failover transparente de aplicações (TAF) para permitir o failover automático de aplicações essenciais aos negócios em ambientes SAN.

Para cada tipo de relação de proteção de dados do SnapMirror, o fluxo de trabalho é o mesmo: Criar um

volume de destino, criar uma agenda de trabalho, especificar uma política, criar e inicializar a relação.

A partir do ONTAP 9.3, você pode usar o `snapmirror protect` comando para configurar uma relação de proteção de dados em uma única etapa. Mesmo que você use `snapmirror protect`o , você precisa entender cada etapa do fluxo de trabalho.



Configure uma relação de replicação em uma etapa

A partir do ONTAP 9.3, você pode usar o `snapmirror protect` comando para configurar uma relação de proteção de dados em uma única etapa. Você especifica uma lista de volumes a serem replicados, uma SVM no cluster de destino, uma programação de tarefa e uma política do SnapMirror. `snapmirror protect` faz o resto.

O que você vai precisar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

  "Peering de cluster e SVM"

- O idioma no volume de destino deve ser o mesmo que o idioma no volume de origem.

Sobre esta tarefa

`snapmirror protect`O comando escolhe um agregado associado ao SVM especificado. Se nenhum agregado estiver associado ao SVM, ele escolherá entre todos os agregados no cluster. A escolha do agregado é baseada na quantidade de espaço livre e no número de volumes no agregado.

O `snapmirror protect` comando então executa as seguintes etapas:

- Cria um volume de destino com um tipo apropriado e uma quantidade de espaço reservado para cada volume na lista de volumes a serem replicados.
- Configura uma relação de replicação apropriada para a política especificada.
- Inicializa o relacionamento.

O nome do volume de destino é do formulário *`source_volume_name_dst`*. Em caso de conflito com um nome existente, o comando adiciona um número ao nome do volume. Você pode especificar um prefixo e/ou sufixo nas opções de comando. O sufixo substitui o sufixo fornecido pelo sistema `dst`.

No ONTAP 9.3 e versões anteriores, um volume de destino pode conter até 251 cópias Snapshot. No ONTAP 9.4 e posterior, um volume de destino pode conter até 1019 cópias snapshot.

A inicialização pode ser demorada. `snapmirror protect` não espera que a inicialização seja concluída antes de o trabalho terminar. Por esse motivo, você deve usar o `snapmirror show` comando em vez do `job show` comando para determinar quando a inicialização está concluída.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror podem ser criadas usando o `snapmirror protect` comando.

Passo

1. Crie e inicialize uma relação de replicação em uma etapa:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. A `-auto-initialize` opção padrão é "'true'".

O exemplo a seguir cria e inicializa um relacionamento de DR do SnapMirror usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

Você pode usar uma política personalizada se preferir. Para obter mais informações, "Criando uma política de replicação personalizada"consulte .

O exemplo a seguir cria e inicializa um relacionamento SnapVault usando a política padrão `XDPDefault`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

O exemplo a seguir cria e inicializa uma relação de replicação unificada usando a política padrão `MirrorAndVault`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

O exemplo a seguir cria e inicializa um relacionamento síncrono do SnapMirror usando a política padrão `Sync`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

Para políticas de replicação unificada e SnapVault, talvez seja útil definir uma programação para criar uma cópia da última cópia Snapshot transferida no destino. Para obter mais informações, "Definir uma agenda para criar uma cópia local no destino"consulte .

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Configure uma relação de replicação uma etapa de cada vez

Crie um volume de destino

Você pode usar o `volume create` comando no destino para criar um volume de destino. O volume de destino deve ser igual ou maior em tamanho do que o volume de origem.

Passo

1. Criar um volume de destino:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um volume de destino de 2 GB chamado `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Criar um agendamento de trabalho de replicação

O agendamento de trabalhos determina quando o SnapMirror atualiza automaticamente a relação de proteção de dados à qual o agendamento é atribuído. Você pode usar o System Manager ou o `job schedule cron create` comando para criar uma agenda de trabalho de replicação.

Sobre esta tarefa

Você atribui um agendamento de trabalho ao criar um relacionamento de proteção de dados. Se não atribuir uma agenda de trabalhos, tem de atualizar a relação manualmente.

Passos

Você pode criar uma programação de trabalho de replicação usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

1. Navegue até **proteção > Visão geral** e expanda **configurações de política local**.
2. No painel **horários**, clique em .
3. Na janela **horários**, clique em .
4. Na janela **Adicionar agendamento**, insira o nome da programação e escolha o contexto e o tipo de agendamento.
5. Clique em **Salvar**.

CLI

1. Criar uma agenda de trabalhos:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

A partir do ONTAP 9.10,1, você pode incluir o SVM para sua agenda de trabalho:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

O cronograma mínimo com suporte (RPO) para volumes FlexVol em uma relação de volume SnapMirror é de 5 minutos. O cronograma mínimo com suporte (RPO) para volumes FlexGroup em uma relação de volume SnapMirror é de 30 minutos.

O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Personalizar uma política de replicação

Crie uma política de replicação personalizada

Você pode criar uma política de replicação personalizada se a política padrão para um relacionamento não for adequada. Você pode querer compactar dados em uma transferência de rede, por exemplo, ou modificar o número de tentativas que o SnapMirror faz para transferir cópias Snapshot.

Você pode usar uma política padrão ou personalizada ao criar uma relação de replicação. Para um arquivo personalizado (anteriormente SnapVault) ou uma política de replicação unificada, você deve definir uma ou mais *regras* para determinar quais cópias snapshot serão transferidas durante a inicialização e a atualização. Também é possível definir uma programação para criar cópias Snapshot locais no destino.

O *policy type* da diretiva de replicação determina o tipo de relação que ela suporta. A tabela abaixo mostra os tipos de política disponíveis.

Tipo de política	Tipo de relação
espelho assíncrono	SnapMirror DR
cofre	SnapVault
espelho-cofre	Replicação unificada
strict-sync-mirror	SnapMirror síncrono no modo StrictSync (suportado a partir de ONTAP 9.5)
espelho de sincronização	SnapMirror síncrono no modo de sincronização (suportado a partir de ONTAP 9.5)

Quando você cria uma política de replicação personalizada, é uma boa ideia modelar a política após uma política padrão.

Passos

Você pode criar políticas de proteção de dados personalizadas com o System Manager ou a CLI do ONTAP. A partir do ONTAP 9.11,1, você pode usar o Gerenciador do sistema para criar políticas de espelhamento e cofre personalizadas e exibir e selecionar políticas herdadas. Essa capacidade também está disponível no ONTAP 9.8P12 e patches posteriores do ONTAP 9.8.

Crie políticas de proteção personalizadas no cluster de origem e destino.

System Manager

1. Clique em **proteção > Visão geral > Configurações de política local**.
2. Em **políticas de proteção**, clique em .
3. No painel **políticas de proteção**, clique em Add .
4. Introduza o novo nome da política e selecione o âmbito da política.
5. Escolha um tipo de política. Para adicionar uma política somente para Vault ou somente para espelhamento, escolha **assíncrono** e clique em **usar um tipo de política legado**.
6. Preencha os campos obrigatórios.
7. Clique em **Salvar**.
8. Repita estas etapas no outro cluster.

CLI

1. Criar uma política de replicação personalizada:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

Para obter a sintaxe completa do comando, consulte a página man.

A partir do ONTAP 9.5, você pode especificar a programação para criar uma agenda comum de cópias Snapshot para relacionamentos síncronos do SnapMirror usando o `-common-snapshot-schedule` parâmetro. Por padrão, o agendamento comum de cópia Snapshot para relacionamentos síncronos do SnapMirror é de uma hora. Você pode especificar um valor de 30 minutos a duas horas para a programação da cópia Snapshot para relacionamentos síncronos do SnapMirror.

O exemplo a seguir cria uma política de replicação personalizada para o SnapMirror DR que permite a compactação de rede para transferências de dados:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

O exemplo a seguir cria uma política de replicação personalizada para o SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

O exemplo a seguir cria uma política de replicação personalizada para replicação unificada:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

O exemplo a seguir cria uma política de replicação personalizada para o relacionamento síncrono do SnapMirror no modo StrictSync:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Depois de terminar

Para os tipos de política "'Vault'" e "mirror-Vault", você deve definir regras que determinam quais cópias snapshot serão transferidas durante a inicialização e atualização.

Use o `snapmirror policy show` comando para verificar se a política SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Defina uma regra para uma política

Para políticas personalizadas com o tipo de política "'Vault'" ou "mirror-Vault", você deve definir pelo menos uma regra que determina quais cópias snapshot serão transferidas durante a inicialização e atualização. Você também pode definir regras para políticas padrão com o tipo de política "'Vault'" ou "mirror-Vault".

Sobre esta tarefa

Todas as políticas com o tipo de política "'Vault'" ou "mirror-Vault" devem ter uma regra que especifique quais cópias snapshot devem ser replicadas. A regra "bimestral", por exemplo, indica que apenas cópias Snapshot atribuídas ao rótulo "bimestral" do SnapMirror devem ser replicadas. Você especifica o rótulo SnapMirror ao configurar a política de captura instantânea na origem.

Cada tipo de política está associado a uma ou mais regras definidas pelo sistema. Essas regras são atribuídas automaticamente a uma política quando você especifica seu tipo de política. A tabela abaixo mostra as regras definidas pelo sistema.

Regra definida pelo sistema	Usado em tipos de política	Resultado
sm_created	Espelho assíncrono, espelho-Vault, sincronização, StrictSync	Uma cópia Snapshot criada pelo SnapMirror é transferida na inicialização e atualização.
all_source_snapshots	espelho assíncrono	Novas cópias Snapshot na origem são transferidas na inicialização e atualização.

diariamente	cofre, espelho-cofre	Novas cópias Snapshot na fonte com o rótulo "diário" do SnapMirror são transferidas na inicialização e atualização.
semanalmente	cofre, espelho-cofre	Novas cópias Snapshot na origem com o rótulo "semanal" do SnapMirror são transferidas na inicialização e atualização.
mensalmente	espelho-cofre	Novas cópias Snapshot na fonte com o rótulo SnapMirror "em quarto lugar" são transferidas na inicialização e atualização.
app_consistente	Sincronizar, StrictSync	As cópias snapshot com o rótulo SnapMirror "app_consistent" na origem são replicadas de forma síncrona para o destino. Suportado a partir de ONTAP 9.7.

Exceto para o tipo de política "async-mirror", você pode especificar regras adicionais conforme necessário, para políticas padrão ou personalizadas. Por exemplo:

- Para a política padrão `MirrorAndVault`, você pode criar uma regra chamada "bimestral" para combinar cópias Snapshot na origem com o rótulo SnapMirror ""bimestral"".
- Para uma política personalizada com o tipo de política "mirror-Vault", você pode criar uma regra chamada "bi-semporal" para combinar cópias Snapshot na origem com o rótulo SnapMirror "bi-semporal".

Passo

1. Defina uma regra para uma política:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir adiciona uma regra com o rótulo SnapMirror `bi-monthly` à política padrão `MirrorAndVault`:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   O exemplo a seguir adiciona uma regra com o rótulo SnapMirror `bi-weekly` à política personalizada `my_snapvault`:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

O exemplo a seguir adiciona uma regra com o rótulo SnapMirror `app_consistent` à política personalizada `Sync`:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Em seguida, é possível replicar cópias Snapshot do cluster de origem que corresponda a este rótulo SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Defina uma agenda para criar uma cópia local no destino

Para relacionamentos de replicação unificada e SnapVault, você pode se proteger contra a possibilidade de que uma cópia Snapshot atualizada seja corrompida criando uma cópia da última cópia Snapshot transferida no destino. Essa cópia local é mantida independentemente das regras de retenção na origem, de modo que, mesmo que o Snapshot originalmente transferido pelo SnapMirror não esteja mais disponível na origem, uma cópia dele estará disponível no destino.

Sobre esta tarefa

Você especifica a programação para criar uma cópia local na `-schedule` opção `snapmirror policy add-rule` do comando.

Passo

1. Defina uma agenda para criar uma cópia local no destino:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   Para obter a sintaxe completa do comando, consulte a página man. Para obter um exemplo de como criar uma agenda de trabalhos, "Criando um agendamento de trabalho de replicação"consulte .

   O exemplo a seguir adiciona uma programação para criar uma cópia local à política padrão `MirrorAndVault`:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   O exemplo a seguir adiciona uma programação para criar uma cópia local à política personalizada

`my_unified`:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Crie uma relação de replicação

A relação entre o volume de origem no storage primário e o volume de destino no storage secundário é chamada de *relação de proteção de dados.* você pode usar o `snapmirror create` comando para criar relacionamentos de proteção de dados de replicação unificada, SnapVault ou DR do SnapMirror.

> Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar uma relação de replicação. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A partir do ONTAP 9.11,1, você pode usar o Gerenciador do sistema para selecionar políticas de espelhamento e cofre pré-criadas e personalizadas, exibir e selecionar políticas herdadas e substituir as programações de transferência definidas em uma política de proteção ao proteger volumes e VMs de storage. Essa capacidade também está disponível no ONTAP 9.8P12 e patches posteriores do ONTAP 9.8.

> Se você estiver usando a versão de patch do ONTAP 9.8P12 ou posterior do ONTAP 9.8 e tiver configurado o SnapMirror usando o Gerenciador de sistema, use o ONTAP 9.9.1P13 ou versões de patch do ONTAP 9.10.1P10 ou versões posteriores se você planeja atualizar para versões do ONTAP 9.9,1 ou do ONTAP 9.10,1.

Antes de começar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

  "Peering de cluster e SVM"

- O idioma no volume de destino deve ser o mesmo que o idioma no volume de origem.

Sobre esta tarefa

Até o ONTAP 9.3, o SnapMirror invocado no modo DP e o SnapMirror invocado no modo XDP usavam diferentes mecanismos de replicação, com diferentes abordagens para dependência de versão:

- O SnapMirror invocado no modo DP usou um mecanismo de replicação *dependente da versão* no qual a versão do ONTAP era necessária para ser a mesma no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- O SnapMirror invocado no modo XDP usou um mecanismo de replicação *version-flexível* que suportava diferentes versões do ONTAP no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Com melhorias no desempenho, os benefícios significativos do SnapMirror flexível de versão superam a ligeira vantagem na taxa de transferência de replicação obtida com o modo dependente da versão. Por esse motivo, começando com ONTAP 9.3, o modo XDP foi feito o novo padrão, e todas as invocações do modo DP na linha de comando ou em scripts novos ou existentes são automaticamente convertidas para o modo XDP.

As relações existentes não são afetadas. Se uma relação já for do tipo DP, ela continuará sendo do tipo DP. A tabela abaixo mostra o comportamento que você pode esperar.

Se especificar…	O tipo é…	A política padrão (se você não especificar uma política) é…
DP	XDP	Espelhamento AllSnapshots (SnapMirror DR)
Nada	XDP	Espelhamento AllSnapshots (SnapMirror DR)
XDP	XDP	XDPDefault (SnapVault)

Veja também os exemplos no procedimento abaixo.

As únicas exceções à conversão são as seguintes:

- As relações de proteção de dados do SVM continuam como padrão no modo DP.

  Especifique XDP explicitamente para obter o modo XDP com a política padrão `MirrorAllSnapshots`.

- As relações de proteção de dados de compartilhamento de carga continuam para o modo DP padrão.
- As relações de proteção de dados do SnapLock continuam a ser padrão para o modo DP.
- As invocações explícitas do DP continuam a ser padrão para o modo DP se você definir a seguinte opção em todo o cluster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Essa opção será ignorada se você não invocar explicitamente o DP.

No ONTAP 9.3 e versões anteriores, um volume de destino pode conter até 251 cópias Snapshot. No ONTAP 9.4 e posterior, um volume de destino pode conter até 1019 cópias snapshot.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas.

A partir de ONTAP 9.14,1, a `-backoff-level` opção é adicionada aos `snapmirror create` comandos , `snapmirror modify` e `snapmirror restore` para permitir que você especifique o nível de backoff por relacionamento. A opção é suportada apenas com relacionamentos FlexVol SnapMirror. O comando opcional especifica o nível de backoff do SnapMirror devido às operações do cliente. Os valores de backoff podem ser altos, médios ou nenhum. O valor padrão é alto.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para criar uma relação de replicação.

System Manager

1. Selecione o volume ou LUN a proteger: Clique em **armazenamento > volumes** ou **armazenamento > LUNs** e, em seguida, clique no volume ou nome LUN desejado.
2. Clique em Protect.
3. Selecione o cluster de destino e a VM de armazenamento.
4. A política assíncrona é selecionada por padrão. Para selecionar uma política síncrona, clique em **mais opções**.
5. Clique em **Protect**.
6. Clique na guia **SnapMirror (local ou remoto)** para o volume ou LUN selecionado para verificar se a proteção está configurada corretamente.

CLI

1. No cluster de destino, crie uma relação de replicação:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O `schedule` parâmetro não é aplicável ao criar relações síncronas do SnapMirror.

   O exemplo a seguir cria uma relação de DR do SnapMirror usando a política padrão `MirrorLatest`:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   O exemplo a seguir cria um relacionamento SnapVault usando a política padrão `XDPDefault`:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   O exemplo a seguir cria uma relação de replicação unificada usando a política padrão `MirrorAndVault`:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorAndVault
```

O exemplo a seguir cria uma relação de replicação unificada usando a política personalizada `my_unified`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

O exemplo a seguir cria um relacionamento síncrono do SnapMirror usando a política padrão `Sync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

O exemplo a seguir cria um relacionamento síncrono do SnapMirror usando a política padrão `StrictSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

O exemplo a seguir cria uma relação de DR do SnapMirror. Com o tipo DP convertido automaticamente para XDP e sem nenhuma política especificada, a política é padrão para a `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

O exemplo a seguir cria uma relação de DR do SnapMirror. Sem nenhum tipo ou política especificada, a política é padrão para a `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

O exemplo a seguir cria uma relação de DR do SnapMirror. Sem nenhuma política especificada, a política é padrão para a `XDPDefault` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

O exemplo a seguir cria um relacionamento síncrono do SnapMirror com a política `SnapCenterSync`predefinida :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

A política predefinida `SnapCenterSync` é do tipo `Sync`. Essa política replica qualquer cópia Snapshot criada com o `snapmirror-label` de "app_consistent".

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Informações relacionadas

- "Criar e excluir volumes de teste de failover do SnapMirror".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral do backup de volume usando o SnapVault"

Inicializar uma relação de replicação

Para todos os tipos de relacionamento, a inicialização executa uma *Baseline transfer*: Ele faz uma cópia Snapshot do volume de origem, depois transfere essa cópia e todos os blocos de dados que ela faz referência ao volume de destino. Caso contrário, o conteúdo da transferência depende da política.

O que você vai precisar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

"Peering de cluster e SVM"

Sobre esta tarefa

A inicialização pode ser demorada. Você pode querer executar a transferência de linha de base em horas fora do pico.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas.

Passo

1. Inicializar uma relação de replicação:

   ```
   snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir inicializa a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Exemplo: Configurar uma cascata Vault-Vault

Um exemplo mostrará em termos concretos como você pode configurar relacionamentos de replicação uma etapa de cada vez. Você pode usar a implantação em cascata do Vault-Vault configurada no exemplo para reter mais de 251 cópias Snapshot rotuladas "semanal".

O que você vai precisar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.
- Você deve estar executando o ONTAP 9.2 ou posterior. As cascatas do Vault-Vault não são suportadas em versões anteriores do ONTAP.

Sobre esta tarefa

O exemplo assume o seguinte:

- Você configurou cópias Snapshot no cluster de origem com os rótulos SnapMirror """diariamente", "semanal" e "mensal".
- Você configurou volumes de destino chamados "volA" nos clusters de destino secundário e terciário.
- Você configurou as programações de tarefas de replicação chamadas "mmy_SnapVault" nos clusters de destino secundário e terciário.

O exemplo mostra como criar relacionamentos de replicação com base em duas políticas personalizadas:

- A política "SnapVault_secondary" retém 7 cópias Snapshot diárias, 52 semanais e 180 mensais no cluster de destino secundário.
- A política SnapVault_terciária mantém 250 cópias Snapshot semanais no cluster de destino terciário.

Passos

1. No cluster de destino secundário, crie a política "SnapVault_secondary":

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment “Policy on secondary for vault to vault cascade” -vserver
   svm_secondary
   ```

2. No cluster de destino secundário, defina a regra "diariamente" para a política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. No cluster de destino secundário, defina a regra "semanal" para a política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. No cluster de destino secundário, defina a regra "mensal" para a política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. No cluster de destino secundário, verifique a política:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily               7  false       0 -
-
                              my-weekly             52  false       0 -
-
                              my-monthly           180  false       0 -
-
```

6. No cluster de destino secundário, crie a relação com o cluster de origem:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. No cluster de destino secundário, inicialize a relação com o cluster de origem:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. No cluster de destino terciário, crie a política "'SnapVault_terciária":

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment “Policy on tertiary for vault to vault cascade” -vserver
svm_tertiary
```

9. No cluster de destino terciário, defina a regra "semanal" para a política:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. No cluster de destino terciário, verifique a política:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. No cluster de destino terciário, crie a relação com o cluster secundário:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. No cluster de destino terciário, inicialize a relação com o cluster secundário:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Converta uma relação existente do tipo ONTAP DP para XDP

Se você estiver atualizando para o ONTAP 9.12,1 ou posterior, você deverá converter relações do tipo DP para XDP antes de atualizar. O ONTAP 9.12,1 e posterior não suporta relações do tipo DP. Você pode facilmente converter uma relação de tipo DP existente para XDP para aproveitar o SnapMirror flexível de versão.

Sobre esta tarefa

- O SnapMirror não converte automaticamente relacionamentos do tipo DP existentes para XDP. Para converter o relacionamento, você precisa quebrar e excluir o relacionamento existente, criar um novo relacionamento XDP e ressincronizar o relacionamento. Para obter informações de fundo, "O XDP substitui o DP como o padrão SnapMirror"consulte .
- Ao Planejar sua conversão, você deve estar ciente de que a preparação em segundo plano e a fase de armazenamento de dados de um relacionamento XDP SnapMirror podem levar muito tempo. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

> Depois de converter um tipo de relacionamento SnapMirror de DP para XDP, as configurações relacionadas ao espaço, como dimensionamento automático e garantia de espaço, não são mais replicadas para o destino.

Passos

1. No cluster de destino, verifique se a relação SnapMirror é do tipo DP, se o estado do espelho é SnapMirrored, o status do relacionamento está ocioso e se o relacionamento está saudável:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   O exemplo a seguir mostra a saída do `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

Você pode achar útil manter uma cópia da `snapmirror show` saída do comando para manter o controle existente das configurações de relacionamento. Saiba mais sobre `snapmirror show` o "Referência do comando ONTAP"na .

2. A partir dos volumes de origem e destino, verifique se ambos os volumes têm uma cópia Snapshot comum:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra a `volume snapshot show` saída para os volumes de origem e destino:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantir que as atualizações agendadas não sejam executadas durante a conversão, execute o relacionamento existente do tipo DP:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Saiba mais sobre `snapmirror quiesce` o "Referência do comando ONTAP"na .

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir anula a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` em `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Quebre a relação existente do tipo DP:

```
snapmirror break -destination-path <SVM:volume>
```

Saiba mais sobre `snapmirror-break` o "Referência do comando ONTAP"na .

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir rompe a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Se a exclusão automática de cópias Snapshot estiver ativada no volume de destino, desative-a:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

O exemplo a seguir desativa a cópia snapshot autodelete no volume de `volA_dst` destino :

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Eliminar a relação do tipo DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

Saiba mais sobre `snapmirror-delete` o "Referência do comando ONTAP"na .

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir exclui a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Solte a relação de recuperação de desastres do SVM de origem na fonte:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

O exemplo a seguir libera a relação de recuperação de desastres da SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. Você pode usar a saída que reteve do `snapmirror show` comando para criar a nova relação do tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

O novo relacionamento deve usar o mesmo volume de origem e destino. Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir cria uma relação de recuperação de desastres do SnapMirror entre o volume de origem `volA` ligado `svm1` e o volume de `volA_dst` destino ligado `svm_backup` usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Ressincronizar os volumes de origem e destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para melhorar o tempo de ressincronização, você pode usar a `-quick-resync` opção, mas deve estar ciente de que a economia com eficiência de storage pode ser perdida. Saiba mais sobre `snapmirror resync` o "Referência do comando ONTAP"na .

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Se a exclusão automática de cópias Snapshot for desativada, reative-a:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Depois de terminar

1. Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada.
2. Quando o volume de destino XDP do SnapMirror começar a atualizar cópias Snapshot conforme definido pela política SnapMirror, use a saída `snapmirror list-destinations` do comando do cluster de origem para exibir a nova relação XDP do SnapMirror.

Converta o tipo de uma relação SnapMirror

A partir do ONTAP 9.5, o SnapMirror síncrono é suportado. Você pode converter uma relação assíncrona do SnapMirror para uma relação síncrona do SnapMirror ou vice-versa sem realizar uma transferência de linha de base.

Sobre esta tarefa

Não é possível converter uma relação assíncrona do SnapMirror para uma relação síncrona do SnapMirror ou vice-versa alterando a política do SnapMirror

Passos

- * Conversão de uma relação assíncrona do SnapMirror para uma relação síncrona do SnapMirror*

  a. No cluster de destino, exclua a relação assíncrona do SnapMirror:

  `snapmirror delete -destination-path <SVM:volume>`

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. No cluster de origem, libere a relação do SnapMirror sem excluir as cópias Snapshot comuns:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. No cluster de destino, crie uma relação síncrona SnapMirror:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM>:<destination_volume> -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. Ressincronizar a relação síncrona do SnapMirror:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- * Conversão de uma relação síncrona SnapMirror para uma relação assíncrona SnapMirror*

a. A partir do cluster de destino, quiesce a relação síncrona SnapMirror existente:

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. No cluster de destino, exclua a relação assíncrona do SnapMirror:

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. No cluster de origem, libere a relação do SnapMirror sem excluir as cópias Snapshot comuns:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. No cluster de destino, crie uma relação assíncrona do SnapMirror:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Ressincronizar a relação síncrona do SnapMirror:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Converta o modo de uma relação síncrona SnapMirror

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas. Você pode converter o modo de uma relação síncrona SnapMirror de StrictSync para sincronização ou vice-versa.

Sobre esta tarefa

Você não pode modificar a política de uma relação síncrona SnapMirror para converter seu modo.

Passos

1. A partir do cluster de destino, quiesce a relação síncrona SnapMirror existente:

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. No cluster de destino, exclua a relação síncrona SnapMirror existente:

```
snapmirror delete -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. No cluster de origem, libere a relação do SnapMirror sem excluir as cópias Snapshot comuns:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. No cluster de destino, crie uma relação síncrona SnapMirror especificando o modo para o qual você deseja converter a relação síncrona SnapMirror:

   ```
   snapmirror create -source-path vs1:vol1 -destination-path
   <destination_SVM>:<destination_volume> -policy Sync|StrictSync
   ```

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. A partir do cluster de destino, ressincronize a relação SnapMirror:

   ```
   snapmirror resync -destination-path <destination_SVM>:<destination_volume>
   ```

   ```
   cluster2::> snapmirror resync -destination-path vs1_dr:vol1
   ```

Criar e excluir volumes de teste de failover do SnapMirror

A partir do ONTAP 9.14,1, você pode usar o System Manager para criar um clone de volume para testar o failover do SnapMirror e a recuperação de desastres sem interromper o relacionamento do SnapMirror ativo. Quando terminar o teste, você pode limpar os dados associados e excluir o volume do teste.

Criar um volume de teste de failover do SnapMirror

Sobre esta tarefa

- É possível executar testes de failover em relacionamentos assíncronos e assíncronos do SnapMirror.
- Um clone de volume é criado para executar o teste de recuperação de desastre.
- O volume do clone é criado na mesma VM de storage que o destino do SnapMirror.
- Você pode usar relacionamentos FlexVol e FlexGroup SnapMirror.
- Se já existir um clone de teste para a relação selecionada, não é possível criar outro clone para essa relação.
- As relações do SnapLock Vault não são suportadas.

Antes de começar

- Você deve ser um administrador de cluster.
- A licença SnapMirror deve ser instalada no cluster de origem e destino.

Passos

1. No cluster de destino, selecione **proteção > relacionamentos**.
2. Selecione ⋮ ao lado da fonte do relacionamento e escolha **Teste failover**.
3. Na janela **Teste failover**, selecione **Teste failover**.
4. Selecione **Storage > volumes** e verifique se o volume de failover de teste está listado.
5. Selecione **armazenamento > partilhar**.

6. Clique 

e escolha **compartilhar**.
7. Na janela **Adicionar compartilhamento**, digite um nome para o compartilhamento no campo **Nome do compartilhamento**.
8. No campo **pasta**, selecione **Procurar**, selecione o volume do clone de teste e **Salvar**.
9. Na parte inferior da janela **Adicionar compartilhamento**, escolha **Salvar**.
10. Abra o compartilhamento no cliente e verifique se o volume de teste tem recursos de leitura e gravação.

Limpe os dados de failover e exclua o volume de teste

Depois de concluir o teste de failover, você pode limpar todos os dados associados ao volume de teste e excluí-lo.

Passos

1. No cluster de destino, selecione **proteção > relacionamentos**.
2. Selecione ⋮ ao lado da fonte do relacionamento e escolha **Limpar failover de teste**.
3. Na janela **Limpar failover de teste**, selecione **Limpar**.
4. Selecione **armazenamento > volumes** e verifique se o volume de teste foi excluído.

Fornecer dados de um volume de destino do SnapMirror DR

Torne o volume de destino gravável

Você precisa fazer com que o volume de destino seja gravável antes de poder fornecer dados do volume para os clientes. Para servir dados de um destino espelhado quando uma origem ficar indisponível, pare as transferências agendadas para o destino e, em seguida, quebre a relação SnapMirror para tornar o destino gravável.

Sobre esta tarefa

É necessário executar essa tarefa a partir do SVM de destino ou do cluster de destino.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para tornar um volume de destino gravável.

System Manager

1. Selecione a relação de proteção: Clique em **proteção > relacionamentos** e, em seguida, clique no nome do volume desejado.
2. Clique em .
3. Parar transferências agendadas : clique em **Pausar**.
4. Deixe o destino gravável: Clique em **Break**.
5. Vá para a página principal **relacionamentos** para verificar se o estado da relação é exibido como "quebrado".

Próximas etapas

Você precisa "ressincronizar a relação de replicação reversa" depois de fazer um volume de destino gravável.

Quando o volume de origem desativado estiver novamente disponível, você deverá voltar a sincronizar a relação novamente para copiar os dados atuais para o volume de origem original.

CLI

1. Parar transferências programadas para o destino:

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir interrompe as transferências agendadas entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

2. Parar transferências contínuas para o destino:

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

   Para obter a sintaxe completa do comando, consulte a página man.

   Esta etapa não é necessária para relacionamentos síncronos do SnapMirror (suportado a partir do ONTAP 9.5).

   O exemplo a seguir interrompe as transferências contínuas entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

3. Quebre a relação de DR do SnapMirror:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir rompe a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Próximas etapas

Você precisa "ressincronize a relação de replicação" depois de fazer um volume de destino gravável.

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da recuperação de desastres de volume"

Configure o volume de destino para acesso aos dados

Depois de fazer o volume de destino gravável, você deve configurar o volume para acesso aos dados. Clientes nas, subsistema NVMe e hosts SAN podem acessar os dados do volume de destino até que o volume de origem seja reativado.

Ambiente nas:

1. Monte o volume nas no namespace usando o mesmo caminho de junção no qual o volume de origem foi montado no SVM de origem.
2. Aplique as ACLs apropriadas aos compartilhamentos SMB no volume de destino.
3. Atribua as políticas de exportação NFS ao volume de destino.
4. Aplique as regras de quota ao volume de destino.
5. Redirecione os clientes para o volume de destino.
6. Remontagem dos compartilhamentos de NFS e SMB nos clientes.

AMBIENTE SAN:

1. Mapeie os LUNs no volume para o grupo de iniciadores apropriado.
2. Para iSCSI, crie sessões iSCSI dos iniciadores do host SAN para os LIFs SAN.
3. No cliente SAN, efetue uma nova verificação de armazenamento para detetar os LUNs ligados.

Para obter informações sobre o ambiente NVMe, "Administração da SAN"consulte .

Reative o volume da fonte original

É possível restabelecer a relação de proteção de dados original entre os volumes de origem e destino quando não precisar mais fornecer dados do destino.

Sobre esta tarefa

- O procedimento abaixo pressupõe que a linha de base no volume de origem original está intacta. Se a linha de base não estiver intacta, você deverá criar e inicializar a relação entre o volume do qual você está fornecendo dados e o volume de origem original antes de executar o procedimento.
- A preparação em segundo plano e a fase de armazenamento de dados de um relacionamento XDP SnapMirror podem levar muito tempo. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

Passos

1. Inverta a relação original de proteção de dados:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original. Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico. O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. `snapmirror initialize`Use para reinicializar o relacionamento.

   O exemplo a seguir inverte a relação entre o volume de origem original, `volA` On (ligado `svm1`) e o volume do qual você está fornecendo dados, `volA_dst` On (ligado `svm_backup`):

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. Quando estiver pronto para restabelecer o acesso aos dados à origem original, pare o acesso ao volume de destino original. Uma maneira de fazer isso é parar o SVM de destino original:

   `vserver stop -vserver` *`SVM`*

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir do SVM de destino original ou do cluster de destino original. Esse comando interrompe o acesso do usuário a todo o SVM de destino original. Pode pretender parar o acesso ao volume de destino original utilizando outros métodos.

O exemplo a seguir interrompe o SVM de destino original:

```
cluster_dst::> vserver stop svm_backup
```

3. Atualize a relação invertida:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

   O exemplo a seguir atualiza a relação entre o volume do qual você está fornecendo dados, `volA_dst` ligado `svm_backup` e o volume de origem original, `volA` ligado `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

4. A partir do SVM de origem original ou do cluster de origem original, interrompa as transferências agendadas do relacionamento invertido:

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

   O exemplo a seguir interrompe as transferências agendadas entre o volume de destino original, `volA_dst` On (ligado `svm_backup`) e o volume de origem original `volA`, On (ligado `svm1`):

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

5. Quando a atualização final estiver concluída e o relacionamento indicar "Quiesced" para o status do relacionamento, execute o seguinte comando da fonte original SVM ou do cluster de origem original para quebrar o relacionamento invertido::

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem.

   O exemplo a seguir rompe a relação entre o volume de destino original, `volA_dst` ligado `svm_backup` e o volume de origem original, `volA` ligado `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. No SVM de origem original ou no cluster de origem original, exclua a relação de proteção de dados invertida:

   `snapmirror delete -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

   O exemplo a seguir exclui a relação inversa entre o volume de origem original, `volA` ligado `svm1` e o volume do qual você está fornecendo dados, `volA_dst` ligado `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Liberar a relação inversa do SVM de destino original ou do cluster de destino original.

   `snapmirror release -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > Você deve executar esse comando a partir do SVM de destino original ou do cluster de destino original.

   O exemplo a seguir libera a relação inversa entre o volume de destino original, `volA_dst` On (ligado `svm_backup`) e o volume de origem original `volA`, On (ligado `svm1`):

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Restabelecer a relação de proteção de dados original a partir do destino original:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir restabelece a relação entre o volume de origem original, `volA` ligado `svm1` e o volume de destino original `volA_dst`, ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Se necessário, inicie o SVM de destino original:

`vserver start -vserver SVM`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir inicia o SVM de destino original:

```
cluster_dst::> vserver start svm_backup
```

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Restaure arquivos de um volume de destino do SnapMirror

Restaure um único namespace de arquivo, LUN ou NVMe a partir de um destino do SnapMirror

É possível restaurar um único arquivo, LUN, um conjunto de arquivos ou LUNs de uma cópia Snapshot ou um namespace NVMe a partir de um volume de destino do SnapMirror. A partir do ONTAP 9.7, você também pode restaurar namespaces NVMe a partir de um destino síncrono SnapMirror. Pode restaurar ficheiros para o volume de origem original ou para um volume diferente.

O que você vai precisar

Para restaurar um arquivo ou LUN de um destino síncrono SnapMirror (suportado a partir do ONTAP 9.5), primeiro você deve excluir e liberar a relação.

Sobre esta tarefa

O volume para o qual você está restaurando arquivos ou LUNs (o volume de destino) deve ser um volume de leitura e gravação:

- O SnapMirror executa uma *restauração incremental* se os volumes de origem e destino tiverem uma cópia Snapshot comum (como é normalmente o caso quando você está restaurando para o volume de origem original).
- Caso contrário, o SnapMirror executa uma *restauração de linha de base*, na qual a cópia Snapshot especificada e todos os blocos de dados que ele faz referência são transferidos para o volume de destino.

Passos

1. Listar as cópias Snapshot no volume de destino:

   `volume snapshot show -vserver <SVM> -volume volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as cópias Snapshot `vserverB:secondary1` no destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure um único arquivo ou LUN ou um conjunto de arquivos ou LUNs de uma cópia Snapshot em um volume de destino do SnapMirror:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot -file-list <source_file_path,@destination_file_path>
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

   O comando a seguir restaura os `file1` arquivos e `file2` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` , para o mesmo local no sistema de arquivos ativo do volume de origem original `primary1` :

   ```
   cluster_dst::> snapmirror restore -source-path vserverB:secondary1
   -destination-path vserverA:primary1 -source-snapshot daily.2013-01-
   25_0010 -file-list /dir1/file1,/dir2/file2

   [Job 3479] Job is queued: snapmirror restore for the relationship with
   destination vserverA:primary1
   ```

O comando a seguir restaura os `file1` arquivos e `file2` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` para um local diferente no sistema de arquivos ativo do volume de origem original `primary1` .

O caminho do arquivo de destino começa com o símbolo at seguido pelo caminho do arquivo a partir da raiz do volume de origem original. Neste exemplo, `file1` é restaurado para `/dir1/file1.new` e file2 é restaurado para `/dir2.new/file2` ON `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

O comando a seguir restaura os `file1` arquivos e `file3` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` , para diferentes locais no sistema de arquivos ativo do volume de origem original `primary1` e restaura `file2` de `snap1` para o mesmo local no sistema de arquivos ativo `primary1` do .

Neste exemplo, o arquivo `file1` é restaurado para `/dir1/file1.new` e `file3` é restaurado para `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Restaure o conteúdo de um volume a partir de um destino SnapMirror

É possível restaurar o conteúdo de um volume inteiro a partir de uma cópia Snapshot em um volume de destino do SnapMirror. Pode restaurar o conteúdo do volume para o volume de origem original ou para um volume diferente.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para restaurar os dados. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

O volume de destino para a operação de restauração deve ser um dos seguintes:

- Um volume de leitura e gravação, nesse caso, o SnapMirror executa uma *restauração incremental*, desde que os volumes de origem e destino tenham uma cópia Snapshot comum (como normalmente ocorre

quando você está restaurando para o volume de origem original).

> O comando falhará se não houver uma cópia Snapshot comum. Não é possível restaurar o conteúdo de um volume para um volume de leitura e gravação vazio.

- Um volume de proteção de dados vazio, nesse caso, o SnapMirror executa uma *restauração de linha de base*, na qual a cópia Snapshot especificada e todos os blocos de dados que ele faz referência são transferidos para o volume de origem.

Restaurar o conteúdo de um volume é uma operação disruptiva. O tráfego SMB não deve estar em execução no volume primário do SnapVault quando uma operação de restauração está em execução.

Se o volume de destino para a operação de restauração tiver a compactação ativada e o volume de origem não tiver a compactação ativada, desative a compactação no volume de destino. Você precisa reativar a compactação após a conclusão da operação de restauração.

Todas as regras de quota definidas para o volume de destino são desativadas antes de a restauração ser executada. Você pode usar o `volume quota modify` comando para reativar regras de cota após a conclusão da operação de restauração.

Quando os dados em um volume são perdidos ou corrompidos, você pode reverter seus dados restaurando a partir de uma cópia Snapshot anterior.

Este procedimento substitui os dados atuais no volume de origem por dados de uma versão anterior da cópia Snapshot. Deve executar esta tarefa no cluster de destino.

Passos

Você pode restaurar o conteúdo de um volume usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

1. Clique em **proteção > relacionamentos** e, em seguida, clique no nome do volume de origem.
2. Clique em e selecione **Restore**.
3. Em **fonte**, o volume da fonte é selecionado por padrão. Clique em **outro volume** se quiser escolher um volume diferente da origem.
4. Em **destino**, escolha a cópia Snapshot que deseja restaurar.
5. Se a origem e o destino estiverem localizados em clusters diferentes, no cluster remoto, clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

CLI

1. Listar as cópias Snapshot no volume de destino:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra as cópias Snapshot `vserverB:secondary1` no destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure o conteúdo de um volume a partir de uma cópia Snapshot em um volume de destino do SnapMirror:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

Para obter a sintaxe completa do comando, consulte a página man.

> Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

O comando a seguir restaura o conteúdo do volume de origem original `primary1` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` :

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Remonte o volume restaurado e reinicie todos os aplicativos que usam o volume.

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Restauração de volume usando visão geral do SnapVault"

Atualizar uma relação de replicação manualmente

Talvez seja necessário atualizar manualmente uma relação de replicação se uma atualização falhar porque o volume de origem foi movido.

Sobre esta tarefa

O SnapMirror aborta quaisquer transferências de um volume de origem movido até que você atualize a relação de replicação manualmente.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas. Embora os volumes de origem e destino estejam sempre sincronizados nessas relações, a exibição do cluster secundário é sincronizada com o primário apenas por hora. Se você quiser exibir os dados pontuais no destino, você deve executar uma atualização manual executando o `snapmirror update` comando.

Passo

1. Atualizar manualmente uma relação de replicação:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. `snapmirror initialize`Use para reinicializar o relacionamento.

   O exemplo a seguir atualiza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Ressincronizar uma relação de replicação

É necessário ressincronizar uma relação de replicação depois de fazer um volume de destino gravável, depois de uma atualização falhar porque uma cópia Snapshot comum não existe nos volumes de origem e destino ou se você quiser alterar a política de replicação para a relação.

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para executar uma operação de ressincronização reversa para excluir uma relação de proteção existente e reverter as funções dos volumes de origem e destino. Em seguida, você usa o volume de destino para servir dados enquanto você reparar ou substituir a origem, atualizar a origem e restabelecer a configuração original dos sistemas.

Sobre esta tarefa

- Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.
- Os volumes que fazem parte de uma configuração de fan-out ou cascata podem levar mais tempo para ressincronizar. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

> O System Manager não é compatível com a ressincronização reversa com relacionamentos entre clusters. Você pode usar a CLI do ONTAP para realizar operações ressincronizadas revertidas com relacionamentos entre clusters.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para executar esta tarefa. Se você usar a CLI do ONTAP, o procedimento será o mesmo, independentemente de você estar criando um volume de destino gravável ou atualizando a relação de replicação.

Ressincronização reversa do System Manager

Depois de "quebre um relacionamento"fazer um destino gravável, volte a sincronizar a relação:

1. No cluster de destino, clique em **proteção > relacionamentos**.
2. Passe o Mouse sobre a relação quebrada que você deseja reverter, clique em e selecione **Reverse Resync**.
3. Na janela **Reverse Resync relation**, clique em **Reverse Resync**.
4. Em **relacionamentos**, monitore o progresso da ressincronização reversa visualizando **Status da transferência** para o relacionamento.

Próximas etapas

Quando a fonte original estiver disponível novamente, você poderá restabelecer a relação original quebrando a relação invertida e realizando outra operação ressincronizada reversa. O processo de ressincronização reversa copiará todas as alterações do site que está fornecendo dados para a fonte original e fará a fonte original ler-gravável novamente.

Ressincronizar o System Manager

1. Clique em **proteção > relacionamentos**.
2. Passe o Mouse sobre o relacionamento que você deseja ressincronizar e clique e selecione **Break**.
3. Quando o estado do relacionamento exibir "desagregado", clique e selecione **Resync**.
4. Em **relacionamentos**, monitore o progresso da ressincronização verificando o estado do relacionamento. O estado muda para "espelhado" quando a ressincronização é concluída.

CLI

1. Ressincronizar os volumes de origem e destino:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

Para obter a sintaxe completa do comando, consulte a página man.

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de `volA_dst` destino ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Excluir uma relação de replicação de volume

Você pode usar os `snapmirror delete` comandos e `snapmirror release` para excluir uma relação de replicação de volume. Em seguida, pode eliminar manualmente volumes de destino desnecessários.

Sobre esta tarefa

`snapmirror release`O comando exclui todas as cópias Snapshot criadas pelo SnapMirror da origem. Você pode usar a `-relationship-info-only` opção para preservar as cópias Snapshot.

Passos

1. Quiesce a relação de replicação:

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

2. (Opcional) quebre a relação de replicação se você precisar que o volume de destino seja um volume de leitura/gravação. Pode ignorar esta etapa se pretender eliminar o volume de destino ou se não necessitar de ler/escrever o volume:

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

3. Eliminar a relação de replicação:

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   Para obter a sintaxe completa do comando, consulte a página man.

   Você deve executar esse comando a partir do cluster de destino ou SVM de destino.

   O exemplo a seguir exclui a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

4. Liberar informações de relação de replicação da fonte SVM:

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

Para obter a sintaxe completa do comando, consulte a página man.

Você deve executar esse comando a partir do cluster de origem ou da SVM de origem.

O exemplo a seguir libera informações para a relação de replicação especificada da SVM de origem `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Gerenciar a eficiência de storage

O SnapMirror preserva a eficiência de storage nos volumes de origem e destino, exceto quando a compactação de dados pós-processamento está ativada no volume de destino. Nesse caso, toda a eficiência de storage é perdida no volume de destino. Para corrigir esse problema, você precisa desativar a compactação pós-processo no volume de destino, atualizar a relação manualmente e reativar a eficiência de storage.

Sobre esta tarefa

Você pode usar o `volume efficiency show` comando para determinar se a eficiência está ativada em um volume. Para obter mais informações, consulte as páginas de manual.

Você pode verificar se o SnapMirror está mantendo a eficiência de storage visualizando os logs de auditoria do SnapMirror e localizando a descrição da transferência. Se a descrição da transferência for exibida `transfer_desc=Logical Transfer with Storage Efficiency`, o SnapMirror manterá a eficiência do storage. Se a descrição da transferência for exibida `transfer_desc=Logical Transfer`, o SnapMirror não manterá a eficiência do storage. Por exemplo:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Antes de começar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

  "Peering de cluster e SVM"

- Você deve desativar a compressão pós-processo no volume de destino.
- Transferência lógica com armazenamento: A partir do ONTAP 9.3, a atualização manual não é mais necessária para reativar a eficiência de storage. Se o SnapMirror detetar que a compactação pós-processo foi desativada, ele reativará automaticamente a eficiência de storage na próxima atualização

agendada. Tanto a origem quanto o destino devem estar executando o ONTAP 9.3.

- A partir do ONTAP 9.3, os sistemas AFF gerenciam as configurações de eficiência de storage de maneira diferente dos sistemas FAS depois que um volume de destino é gravado:
  - Depois de fazer um volume de destino gravável usando o `snapmirror break` comando, a política de cache no volume é automaticamente definida como "'auto'" (o padrão).

    Esse comportamento é aplicável apenas a volumes do FlexVol e não se aplica a volumes do FlexGroup.

  - Na ressincronização, a política de armazenamento em cache é automaticamente definida como "nenhum", e a deduplicação e a compactação in-line são desativadas automaticamente, independentemente das configurações originais. Você deve modificar as configurações manualmente, conforme necessário.

Atualizações manuais com eficiência de storage habilitada podem ser demoradas. Você pode querer executar a operação em horas fora do pico.

Passos

1. Atualizar uma relação de replicação e reativar a eficiência de storage:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

Para obter a sintaxe completa do comando, consulte a página man.

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. `snapmirror initialize`Use para reinicializar o relacionamento.

O exemplo a seguir atualiza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino ligado `svm_backup` e `volA_dst` rehabilita a eficiência de storage:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Use a regulagem global do SnapMirror

A regulagem global da rede está disponível para todas as transferências SnapMirror e SnapVault em um nível por nó.

Sobre esta tarefa

A regulagem global da SnapMirror restringe a largura de banda usada pelas transferências SnapMirror e SnapVault de entrada e/ou saída. A restrição é aplicada em todo o cluster em todos os nós no cluster.

Por exemplo, se o acelerador de saída estiver definido para 100 Mbps, cada nó no cluster terá a largura de

banda de saída definida para 100 Mbps. Se a limitação global estiver desativada, ela será desativada em todos os nós.

Embora as taxas de transferência de dados sejam frequentemente expressas em bits por segundo (bps), os valores do acelerador devem ser inseridos em kilobytes por segundo (kbps).

> No ONTAP 9.9,1 e versões anteriores, o acelerador não tem efeito em `volume move` transferências ou transferências de espelho de compartilhamento de carga. A partir do ONTAP 9.10.0, você pode especificar uma opção para controlar uma operação de movimentação de volume. Para obter detalhes, consulte "Como mover o volume do acelerador em ONTAP 9.10 e mais tarde."

A regulagem global funciona com o recurso de aceleração por relacionamento para transferências SnapMirror e SnapVault. O acelerador por relação é aplicado até que a largura de banda combinada de transferências por relação exceda o valor do acelerador global, após o qual o acelerador global é aplicado. Um valor de aceleração `0` implica que a limitação global está desativada.

> A regulagem global do SnapMirror não tem efeito nas relações síncronas do SnapMirror quando elas estão em sincronia. No entanto, o acelerador afeta as relações síncronas do SnapMirror quando executam uma fase de transferência assíncrona, como uma operação de inicialização ou após um evento fora de sincronização. Por esse motivo, não é recomendável habilitar a limitação global com relacionamentos síncronos do SnapMirror.

Passos

1. Ativar a limitação global:

   `options -option-name replication.throttle.enable on|off`

   O exemplo a seguir mostra como ativar a limitação global do SnapMirror no `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Especifique a largura de banda total máxima usada pelas transferências recebidas no cluster de destino:

   `options -option-name replication.throttle.incoming.max_kbs <KBps>`

   A largura de banda mínima recomendada do acelerador é de 4 kilobytes por segundo (kbps) e o máximo é de até 2 terabytes por segundo (Tbps). O valor padrão para essa opção é `unlimited`, o que significa que não há limite na largura de banda total usada.

   O exemplo a seguir mostra como definir a largura de banda total máxima usada pelas transferências recebidas para 100 megabits por segundo (Mbps):

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 megabits por segundo (Mbps): 12500 kilobytes por segundo (kbps)

3. Especifique a largura de banda total máxima utilizada pelas transferências efetuadas no cluster de origem:

`options -option-name replication.throttle.outgoing.max_kbs <KBps>`

A largura de banda mínima recomendada do acelerador é de 4 kbps e o máximo é de até 2 Tbps. O valor padrão para essa opção é `unlimited`, o que significa que não há limite na largura de banda total usada. Os valores dos parâmetros estão em kilobytes por segundo (kbps).

O exemplo a seguir mostra como definir a largura de banda total máxima usada pelas transferências de saída para 100 Mbps:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Gerenciar a replicação do SnapMirror SVM

Saiba mais sobre a replicação do ONTAP SnapMirror SVM

Você pode usar o SnapMirror para criar uma relação de proteção de dados entre SVMs. Nesse tipo de relação, toda ou parte da configuração do SVM, de exportações de NFS e compartilhamentos de SMB a RBAC, são replicados, bem como os dados nos volumes proprietários do SVM.

Tipos de relacionamento suportados

Somente SVMs de fornecimento de dados podem ser replicadas. Os seguintes tipos de relacionamento de proteção de dados são compatíveis:

- *SnapMirror DR,* no qual o destino normalmente contém apenas as cópias Snapshot atualmente na origem.

  A partir do ONTAP 9.9,1, esse comportamento muda quando você está usando a política mirror-Vault. A partir do ONTAP 9.9,1, você pode criar diferentes políticas de Snapshot na origem e no destino. Além disso, as cópias snapshot no destino não são sobrescritas por cópias Snapshot na origem:

  - Eles não são sobrescritos da origem para o destino durante operações normais agendadas, atualizações e ressincronização
  - Eles não são excluídos durante operações de interrupção.
  - Eles não são excluídos durante operações flip-ressync. Quando você configura um relacionamento de desastre SVM usando a política de espelhamento de arquivos usando o ONTAP 9.9,1 e posterior, a política se comporta da seguinte forma:
  - As políticas de cópia Snapshot definidas pelo usuário na origem não são copiadas para o destino.
  - As políticas de cópia Snapshot definidas pelo sistema não são copiadas para o destino.
  - A associação de volume com políticas Snapshot definidas pelo usuário e pelo sistema não é copiada para o destino. COM SVM.
- A partir do ONTAP 9.2, *replicação unificada do SnapMirror,* na qual o destino é configurado para DR e retenção de longo prazo.

Para obter mais informações sobre a replicação unificada do SnapMirror, "Noções básicas de replicação unificada da SnapMirror"consulte .

O *policy type* da diretiva de replicação determina o tipo de relação que ela suporta. A tabela a seguir mostra os tipos de diretiva disponíveis.

Tipo de política	Tipo de relação
espelho assíncrono	SnapMirror DR
espelho-cofre	Replicação unificada

O XDP substitui o DP como o padrão de replicação SVM no ONTAP 9.4

A partir do ONTAP 9.4, as relações de proteção de dados do SVM passam por padrão no modo XDP. As relações de proteção de dados do SVM continuam como padrão no modo DP no ONTAP 9.3 e versões anteriores.

Relacionamentos existentes não são afetados pelo novo padrão. Se uma relação já for do tipo DP, ela continuará sendo do tipo DP. A tabela a seguir mostra o comportamento que você pode esperar.

Se especificar…	O tipo é…	A política padrão (se você não especificar uma política) é…
DP	XDP	Espelhamento AllSnapshots (SnapMirror DR)
Nada	XDP	Espelhamento AllSnapshots (SnapMirror DR)
XDP	XDP	MirrorAndVault (replicação unificada)

Detalhes sobre as alterações no padrão podem ser encontrados aqui: "O XDP substitui o DP como o padrão SnapMirror".

> ⓘ A independência de versão não é compatível com replicação SVM. Em uma configuração de recuperação de desastre do SVM, o SVM de destino deve estar em um cluster que executa a mesma versão de ONTAP do cluster de origem, para dar suporte a operações de failover e failback.

"Versões compatíveis do ONTAP para relacionamentos do SnapMirror"

Como as configurações da SVM são replicadas

O conteúdo de uma relação de replicação SVM é determinado pela interação dos seguintes campos:

- A `-identity-preserve true` opção `snapmirror create` do comando replica toda a configuração SVM.

  A `-identity-preserve false` opção replica apenas os volumes e as configurações de autenticação e autorização do SVM e as configurações de protocolo e serviço de nomes listadas em "Configurações replicadas em relacionamentos de recuperação de desastres da SVM".

- A `-discard-configs network` opção `snapmirror policy create` do comando exclui LIFs e configurações de rede relacionadas da replicação SVM, para uso nos casos em que as SVMs de origem e destino estão em sub-redes diferentes.
- A `-vserver-dr-protection unprotected` opção `volume modify` do comando exclui o volume especificado da replicação SVM.

Caso contrário, a replicação do SVM é quase idêntica à replicação de volume. Você pode usar praticamente o mesmo fluxo de trabalho para replicação de volume para SVM.

Detalhes do suporte

A tabela a seguir mostra os detalhes de suporte para replicação do SnapMirror SVM.

Recurso ou recurso	Detalhes do suporte
Tipos de implantação	• Origem única para destino único • Começando com ONTAP 9.4, fan-out. Você pode fazer fan-out apenas para dois destinos. Por padrão, somente um relacionamento verdadeiro que preserve identidade é permitido por SVM de origem.
Tipos de relacionamento	• Recuperação de desastres da SnapMirror • A partir do ONTAP 9.2, a replicação unificada do SnapMirror
Escopo de replicação	Apenas entre clusters. Não é possível replicar SVMs no mesmo cluster.
Proteção autônoma contra ransomware	• Suportado a partir de ONTAP 9.12,1. Para obter mais informações, "Proteção autônoma contra ransomware"consulte .
Grupos de consistência suporte assíncrono	A partir do ONTAP 9.14,1, há suporte para no máximo 32 relacionamentos de recuperação de desastres da SVM quando existem grupos de consistência. "Proteja um grupo de consistência"Consulte e "Limites do grupo de consistência" para obter mais informações.
FabricPool	A partir do ONTAP 9.6, a replicação do SnapMirror SVM é compatível com FabricPools.

MetroCluster	A partir do ONTAP 9.11,1, os dois lados de uma relação de recuperação de desastres do SVM em uma configuração MetroCluster podem funcionar como fonte de configurações adicionais de recuperação de desastres do SVM. A partir do ONTAP 9.5, a replicação do SnapMirror SVM é compatível com configurações do MetroCluster. • Em versões anteriores ao ONTAP 9.10.X, uma configuração do MetroCluster não pode ser o destino de uma relação de recuperação de desastres da SVM. • No ONTAP 9.10,1 e versões posteriores, uma configuração do MetroCluster pode ser o destino de uma relação de recuperação de desastres da SVM somente para fins de migração. Ela precisa atender a todos os requisitos necessários descritos na "TR-4966: Migração de um SVM para uma solução MetroCluster". • Somente um SVM ativo em uma configuração do MetroCluster pode ser a fonte de uma relação de recuperação de desastres do SVM. Uma fonte pode ser uma SVM de origem sincronizada antes do switchover ou um SVM de destino de sincronização após o switchover. • Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online. • Quando o SVM de origem sincronizada é a fonte de uma relação de recuperação de desastres do SVM, as informações de origem no relacionamento de recuperação de desastres do SVM são replicadas para o parceiro MetroCluster. • Durante os processos de switchover e switchback, a replicação para o destino de recuperação de desastres da SVM pode falhar. No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas de recuperação de desastres da SVM serão bem-sucedidas.

Grupo de consistência	Suportado a partir de ONTAP 9.14,1. Para obter mais informações, Proteja um grupo de consistênciaconsulte .
ONTAP S3	Não é compatível com recuperação de desastre do SVM.
SnapMirror síncrono	Não é compatível com recuperação de desastre do SVM.
Independência de versão	Não suportado.
Criptografia de volumes	• Volumes criptografados na origem são criptografados no destino. • Os servidores Onboard Key Manager ou KMIP devem ser configurados no destino. • Novas chaves de criptografia são geradas no destino. • Se o destino não contiver um nó que suporte a criptografia de volume .Encryption, a replicação será bem-sucedida, mas os volumes de destino não serão criptografados.

Configurações replicadas em relacionamentos de recuperação de desastres da SVM

A tabela a seguir mostra a interação `snapmirror create -identity-preserve` da opção e da `snapmirror policy create -discard-configs network` opção:

Configuração replicada		`-identity-preserve true`		`-identity-preserve false`
		Política sem `-discard -configs network` set	**Política com `-discard -configs network` SET**	
Rede	LIFs nas	Sim	Não	Não
Configuração do Kerberos LIF	Sim	Não	Não	SAN LIFs
Não	Não	Não	Políticas de firewall	Sim
Sim	Não	Políticas de serviço	Sim	Sim
Não	Rotas	Sim	Não	Não

Domínio de transmissão	Não	Não	Não	Sub-rede
Não	Não	Não	IPspace	Não
Não	Não	SMB	Servidor SMB	Sim
Sim	Não	Grupos locais e usuário local	Sim	Sim
Sim	Privilégio	Sim	Sim	Sim
Cópia de sombra	Sim	Sim	Sim	BranchCache
Sim	Sim	Sim	Opções de servidor	Sim
Sim	Sim	Segurança do servidor	Sim	Sim
Não	Diretório base, compartilhar	Sim	Sim	Sim
Link simbólico	Sim	Sim	Sim	Política de Fpolicy, Política de Fsecurity e Fsecurity NTFS
Sim	Sim	Sim	Mapeamento de nomes e mapeamento de grupos	Sim
Sim	Sim	Informações de auditoria	Sim	Sim
Sim	NFS	Políticas de exportação	Sim	Sim
Não	Regras de política de exportação	Sim	Sim	Não
Servidor NFS	Sim	Sim	Não	RBAC
Certificados de segurança	Sim	Sim	Não	Configuração de usuário de login, chave pública, função e função

Sim	Sim	Sim	SSL	Sim
Sim	Não	Serviços de nomes	DNS e DNS hosts	Sim
Sim	Não	Usuário UNIX e grupo UNIX	Sim	Sim
Sim	Kerberos Realm e blocos de chaves Kerberos	Sim	Sim	Não
Cliente LDAP e LDAP	Sim	Sim	Não	Grupo de rede
Sim	Sim	Não	NIS	Sim
Sim	Não	Acesso à Web e à Web	Sim	Sim
Não	Volume	Objeto	Sim	Sim
Sim	Cópias Snapshot e política do Snapshot	Sim	Sim	Sim
Política de Autodelete	Não	Não	Não	Política de eficiência
Sim	Sim	Sim	Política de cotas e regra de política de cotas	Sim
Sim	Sim	Fila de recuperação	Sim	Sim
Sim	Volume raiz	Namespace	Sim	Sim
Sim	Dados do utilizador	Não	Não	Não
Qtrees	Não	Não	Não	Quotas
Não	Não	Não	QoS em nível de arquivo	Não

Não	Não	Atributos: estado do volume raiz, garantia de espaço, tamanho, dimensionamento automático e número total de arquivos	Não	Não
Não	QoS de storage	Grupo de políticas de QoS	Sim	Sim
Sim	Fibre Channel (FC)	Não	Não	Não
ISCSI	Não	Não	Não	LUNs
Objeto	Sim	Sim	Sim	grupos
Não	Não	Não	portsets	Não
Não	Não	Números de série	Não	Não
Não	SNMP	v3 utilizadores	Sim	Sim

Limites de storage da recuperação de desastres da SVM

A tabela a seguir mostra o número máximo recomendado de volumes e as relações de recuperação de desastres do SVM com suporte por objeto de storage. Você deve estar ciente de que os limites geralmente dependem da plataforma. Consulte a "Hardware Universe" para saber os limites para a sua configuração específica.

Objeto de storage	Limite
SVM	300 volumes flexíveis
Par de HA	1.000 volumes flexíveis
Cluster	128 relacionamentos de desastre com SVM

Replique configurações da SVM

Fluxo de trabalho de replicação do SnapMirror SVM

A replicação do SnapMirror SVM envolve a criação do SVM de destino, a criação de um cronograma de trabalho de replicação e a criação e inicialização de um relacionamento do SnapMirror.

Você deve determinar qual fluxo de trabalho de replicação mais adequado às suas necessidades:

- "Replique toda uma configuração da SVM"
- "Excluir LIFs e configurações de rede relacionadas da replicação SVM"
- "Exponha a rede, o serviço de nomes e outras configurações da configuração SVM"

Critérios para colocar volumes em SVMs de destino

Ao replicar volumes da SVM de origem para o SVM de destino, é importante saber os critérios de seleção de agregados.

Os agregados são selecionados com base nos seguintes critérios:

- Os volumes são sempre colocados em agregados não-raiz.
- Agregados não-raiz são selecionados com base no espaço livre disponível e no número de volumes já hospedados no agregado.

  Agregados com mais espaço livre e menos volumes têm prioridade. O agregado com a prioridade mais alta é selecionado.

- Volumes de origem em agregados FabricPool são colocados em agregados FabricPool no destino com a mesma política de disposição em camadas.
- Se um volume na SVM de origem estiver localizado em um agregado de Flash Pool, o volume será colocado em um agregado de Flash Pool no SVM de destino, se esse agregado existir e tiver espaço livre suficiente.
- Se a `-space-guarantee` opção do volume replicado estiver definida como `volume`, somente agregados com espaço livre maior que o tamanho do volume serão considerados.
- O tamanho do volume aumenta automaticamente no SVM de destino durante a replicação, com base no tamanho do volume de origem.

  Se você quiser pré-reservar o tamanho no SVM de destino, você deve redimensionar o volume. O tamanho do volume não diminui automaticamente no SVM de destino com base na SVM de origem.

Se você quiser mover um volume de um agregado para outro, use o `volume move` comando na SVM de destino.

Replique toda uma configuração do ONTAP SVM

Você pode criar uma relação de recuperação de desastre do SVM (SVM DR) para replicar uma configuração do SVM para outra. Em caso de desastre no local principal, você pode ativar rapidamente o SVM de destino.

Antes de começar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato. Para obter mais informações, "Crie um relacionamento de pares de cluster"consulte e "Criar um relacionamento entre clusters entre pares".

Para obter a sintaxe completa do comando, consulte a página man.

Sobre esta tarefa

Este fluxo de trabalho pressupõe que você já está usando uma política padrão ou uma política de replicação personalizada.

A partir do ONTAP 9.9,1, quando você usa a política de espelhamento de arquivos, pode criar diferentes políticas de Snapshot na SVM de origem e destino. Além disso, as cópias Snapshot no destino não serão sobrescritas por cópias Snapshot na origem. Para obter mais informações, "Compreensão da replicação do SnapMirror SVM"consulte .

Conclua este procedimento a partir do destino. Se você precisar criar uma nova política de proteção, por exemplo, quando a VM de armazenamento de origem tiver o SMB configurado, crie a política e use a opção **Identity Preserve**. Para obter detalhes, "Crie políticas de proteção de dados personalizadas"consulte .

Passos

Você pode executar esta tarefa a partir do Gerenciador do sistema ou da CLI do ONTAP.

System Manager

1. No cluster de destino, clique em **proteção > relacionamentos**.
2. Em **relacionamentos**, clique em **proteger** e escolha **Storage VMs (DR)**.
3. Selecione uma política de proteção. Se você criou uma política de proteção personalizada, selecione-a e escolha o cluster de origem e a VM de storage que deseja replicar. Você também pode criar uma nova VM de armazenamento de destino inserindo um novo nome de VM de armazenamento.
4. Se desejado, altere as configurações de destino para substituir a preservação de identidade e incluir ou excluir interfaces e protocolos de rede.
5. Clique em **Salvar**.

CLI

1. Criar um SVM de destino:

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   O nome do SVM deve ser exclusivo nos clusters de origem e destino.

   O exemplo a seguir cria um SVM de destino chamado `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

2. No cluster de destino, crie um relacionamento de pares SVM usando o `vserver peer create` comando.

   Para obter mais informações, "Criar um relacionamento entre clusters entre pares"consulte .

3. Criar um agendamento de trabalho de replicação:

   ```
   job schedule cron create -name <job_name> -month <month> -dayofweek
   <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
   ```

   Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

   > O cronograma mínimo com suporte (RPO) para volumes do FlexVol em uma relação do SVM SnapMirror é de 15 minutos. O cronograma mínimo com suporte (RPO) para volumes do FlexGroup em uma relação do SVM SnapMirror é de 30 minutos.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

4. No SVM de destino ou no cluster de destino, crie uma relação de replicação:

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` .

O exemplo a seguir cria uma relação de DR do SnapMirror usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

O exemplo a seguir cria uma relação de replicação unificada usando a política padrão `MirrorAndVault`:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `async-mirror` , o exemplo a seguir cria uma relação de DR do SnapMirror:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `mirror-vault` , o exemplo a seguir cria uma relação de replicação unificada:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

5. Pare o SVM de destino:

```
vserver stop -vserver <SVM_name>
```

O exemplo a seguir interrompe um SVM de destino chamado SVM_backup:

```
cluster_dst::> vserver stop -vserver svm_backup
```

6. No SVM de destino ou no cluster de destino, inicialize a relação de replicação SVM:

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` .

O exemplo a seguir inicializa a relação entre a SVM de origem e `svm1` o SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Excluir LIFs e configurações de rede relacionadas da replicação SVM

Se as SVMs de origem e destino estiverem em sub-redes diferentes, você poderá usar a `-discard-configs network` opção `snapmirror policy create` do comando para excluir LIFs e configurações de rede relacionadas da replicação SVM.

Antes de começar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

Para obter mais informações, "Crie um relacionamento de pares de cluster"consulte e "Criar um relacionamento entre clusters entre pares".

Sobre esta tarefa

A `-identity-preserve` opção `snapmirror create` do comando deve ser definida como `true` quando você cria a relação de replicação SVM.

Para obter a sintaxe completa do comando, consulte a página man.

Passos

1. Criar um SVM de destino:

`vserver create -vserver SVM -subtype dp-destination`

O nome do SVM deve ser exclusivo nos clusters de origem e destino.

O exemplo a seguir cria um SVM de destino chamado `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. No cluster de destino, crie um relacionamento de pares SVM usando o `vserver peer create` comando.

   Para obter mais informações, "Criar um relacionamento entre clusters entre pares"consulte .

3. Criar uma agenda de trabalhos:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

   > O cronograma mínimo com suporte (RPO) para volumes do FlexVol em uma relação do SVM SnapMirror é de 15 minutos. O cronograma mínimo com suporte (RPO) para volumes do FlexGroup em uma relação do SVM SnapMirror é de 30 minutos.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Criar uma política de replicação personalizada:

   `snapmirror policy create -vserver SVM -policy policy -type async-mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria uma política de replicação personalizada para o SnapMirror DR que exclui LIFs:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_exclude_LIFs -type async-mirror -discard-configs network
   ```

   O exemplo a seguir cria uma política de replicação personalizada para replicação unificada que exclui LIFs:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

Considere a criação da mesma política de SnapMirror personalizada no cluster de origem para futuros cenários de failover e failback.

5. No SVM de destino ou no cluster de destino, execute o seguinte comando para criar uma relação de replicação:

   `snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule` *`schedule`* `-policy` *`policy`* `-identity-preserve true|false -discard -configs true|false`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja os exemplos abaixo.

   O exemplo a seguir cria uma relação de DR do SnapMirror que exclui LIFs:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
   -identity-preserve true
   ```

   O exemplo a seguir cria uma relação de replicação unificada da SnapMirror que exclui LIFs:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
   -identity-preserve true -discard-configs true
   ```

6. Pare o SVM de destino:

   `vserver stop`

   `SVM name`

   O exemplo a seguir interrompe o SVM de destino chamado SVM_backup:

   ```
   cluster_dst::> vserver stop -vserver svm_backup
   ```

7. No SVM de destino ou no cluster de destino, inicialize uma relação de replicação:

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir inicializa a relação entre a origem e `svm1` o destino `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Depois de terminar

Você deve configurar a rede e os protocolos no SVM de destino para acesso aos dados em caso de desastre.

Exclua a rede, o serviço de nomes e outras configurações da replicação SVM

Talvez você queira excluir a rede, o serviço de nomes e outras configurações de uma relação de replicação SVM para evitar conflitos ou diferenças de configuração com o SVM de destino.

Você pode usar `-identity-preserve false` a opção `snapmirror create` do comando para replicar apenas os volumes e as configurações de segurança de um SVM. Algumas configurações de protocolo e serviço de nomes também são preservadas.

Sobre esta tarefa

Para obter uma lista das configurações de protocolo e serviço de nomes preservadas, "Configurações replicadas em relacionamentos da SVM DR"consulte .

Para obter a sintaxe completa do comando, consulte a página man.

Antes de começar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

Para obter mais informações, "Crie um relacionamento de pares de cluster"consulte e "Criar um relacionamento entre clusters entre pares".

Passos

1. Criar um SVM de destino:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

   O nome do SVM deve ser exclusivo nos clusters de origem e destino.

   O exemplo a seguir cria um SVM de destino chamado `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. No cluster de destino, crie um relacionamento de pares SVM usando o `vserver peer create` comando.

   Para obter mais informações, "Criar um relacionamento entre clusters entre pares"consulte .

3. Criar um agendamento de trabalho de replicação:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

> O cronograma mínimo com suporte (RPO) para volumes do FlexVol em uma relação do SVM SnapMirror é de 15 minutos. O cronograma mínimo com suporte (RPO) para volumes do FlexGroup em uma relação do SVM SnapMirror é de 30 minutos.

O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Crie uma relação de replicação que exclua a rede, o serviço de nomes e outras configurações:

`snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja os exemplos abaixo. Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir cria uma relação de DR do SnapMirror usando a política padrão `MirrorAllSnapshots`. A relação exclui a rede, o serviço de nomes e outras configurações da replicação SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

O exemplo a seguir cria uma relação de replicação unificada usando a política padrão `MirrorAndVault`. A relação exclui a rede, o serviço de nomes e outras configurações:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `async-mirror` , o exemplo a seguir cria uma relação de DR do SnapMirror. A relação exclui a rede, o serviço de nomes e outras configurações da replicação SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `mirror-vault` , o exemplo a seguir cria uma relação de replicação unificada. A relação exclui a rede, o serviço de nomes e outras configurações da replicação SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

5. Pare o SVM de destino:

   `vserver stop`

   `SVM name`

   O exemplo a seguir interrompe um SVM de destino chamado dvs1:

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. Se você estiver usando SMB, você também deve configurar um servidor SMB.

   "Somente SMB: Criando um servidor SMB"Consulte .

7. No SVM de destino ou no cluster de destino, inicialize a relação de replicação SVM:

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

Depois de terminar

Você deve configurar a rede e os protocolos no SVM de destino para acesso aos dados em caso de desastre.

Especifique agregados a serem usados para relacionamentos de recuperação de desastres do ONTAP SVM

Após a criação de um SVM para recuperação de desastres, você pode usar a `aggr-list` opção com `vserver modify` comando para limitar quais agregados são usados para hospedar volumes de destino do SVM DR.

Passo

1. Criar um SVM de destino:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. Modifique a lista de agentes do SVM de recuperação de desastres para limitar os agregados usados para hospedar o volume do SVM de recuperação de desastres:

   `cluster_dest::> vserver modify -vserver` *`SVM`* `-aggr-list <comma-separated-list>`

Crie um servidor SMB para um SVM de destino do ONTAP em uma relação de recuperação de desastres

Se o SVM de origem tiver uma configuração SMB e você optar por definir `identity-preserve` como `false`, você deverá criar um servidor SMB para o SVM de destino. O servidor SMB é necessário para algumas configurações SMB, como compartilhamentos durante a inicialização do relacionamento SnapMirror.

Passos

1. Inicie o SVM de destino usando o `vserver start` comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Verifique se o SVM de destino está no `running` estado e se o subtipo está `dp-destination` usando o `vserver show` comando.

```
destination_cluster::> vserver show
                                  Admin      Operational Root
Vserver  Type    Subtype          State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

3. Crie um LIF usando o `network interface create` comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

4. Crie uma rota usando o `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Gerenciamento de rede"

5. Configure o DNS usando o `vserver services dns create` comando.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Adicione o controlador de domínio preferido usando o `vserver cifs domain preferred-dc add` comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Crie o servidor SMB usando o `vserver cifs create` comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Pare o SVM de destino usando o `vserver stop` comando.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Excluir volumes de uma relação de recuperação de desastres do ONTAP SVM

Por padrão, todos os volumes de dados RW da SVM de origem são replicados. Se você não quiser proteger todos os volumes na SVM de origem, use a `-vserver-dr -protection unprotected` opção `volume modify` do comando para excluir volumes da replicação SVM.

Passos

1. Excluir um volume da replicação do SVM:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir exclui o volume `volA_src` da replicação SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

   Se, posteriormente, quiser incluir um volume na replicação SVM que você excluiu originalmente, execute o

seguinte comando:

`volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection protected`

O exemplo a seguir inclui o volume `volA_src` na replicação da SVM:

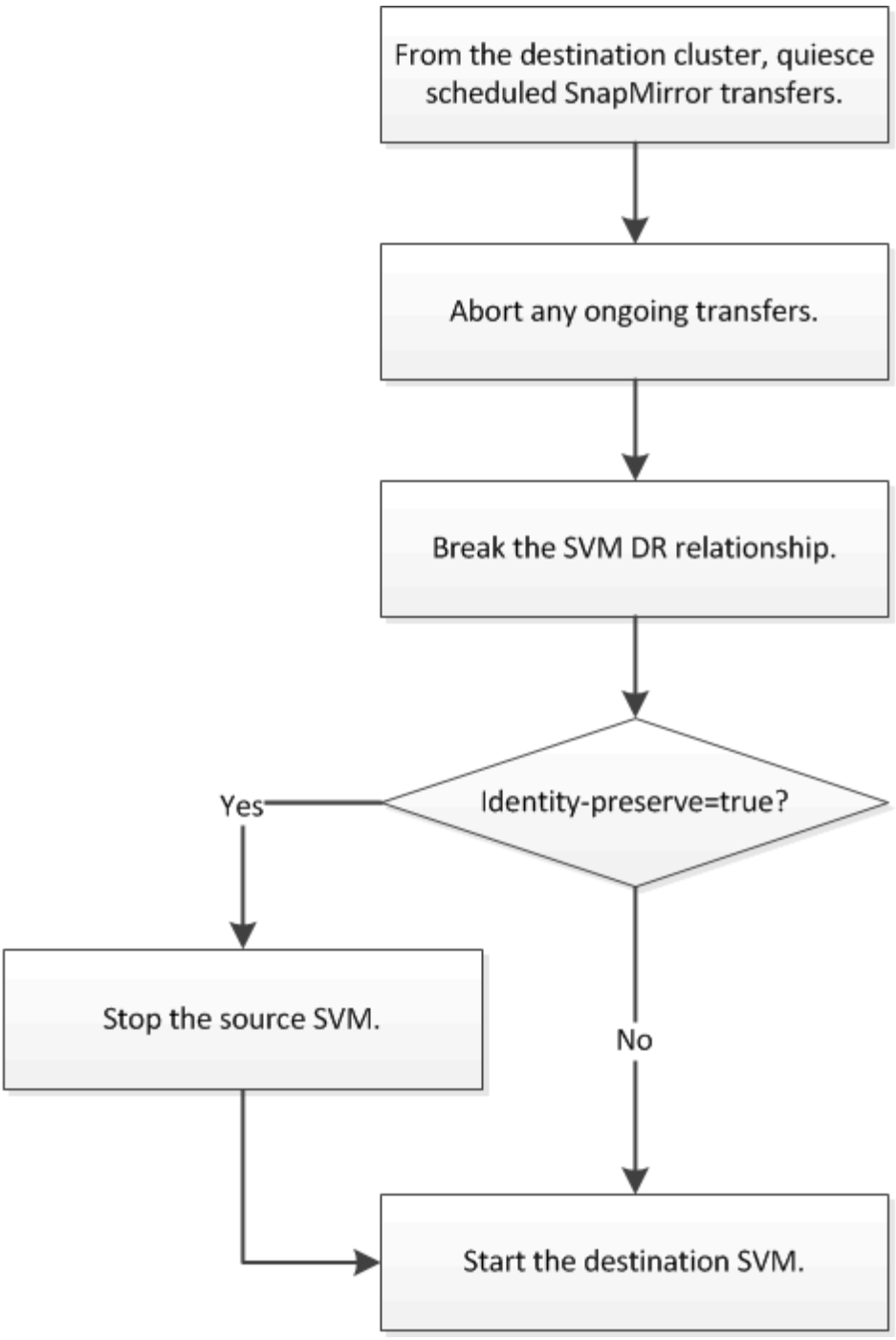
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Crie e inicialize a relação de replicação SVM conforme descrito em "Replicação de toda uma configuração de SVM".

Fornecer dados de um destino com SVM DR

Fluxo de trabalho de recuperação de desastre do ONTAP SVM

Para se recuperar de um desastre e servir dados do SVM de destino, você precisa ativar o SVM de destino. A ativação do SVM de destino envolve a interrupção das transferências agendadas do SnapMirror, o cancelamento das transferências contínuas do SnapMirror, a quebra da relação de replicação, a interrupção da SVM de origem e a inicialização do SVM de destino.



Configurar o volume de destino do ONTAP SVM como gravável

Você precisa fazer com que os volumes de destino do SVM sejam graváveis antes de fornecer dados aos clientes.

O procedimento é em grande parte idêntico ao procedimento para replicação de volume, com uma exceção. Se você definir `-identity-preserve true` quando criou a relação de replicação SVM, será necessário parar o SVM de origem antes de ativar o SVM de destino.

Sobre esta tarefa

Para obter a sintaxe completa do comando, consulte a página man.

Em um cenário de recuperação de desastres, você não pode executar uma atualização do SnapMirror da SVM de origem para o SVM de destino de recuperação de desastres porque sua SVM de origem e seus dados ficarão inacessíveis e porque as atualizações desde o último ressync podem estar ruins ou corrompidas.

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para ativar uma VM de armazenamento de destino após um desastre. A ativação da VM de storage de destino torna os volumes de destino do SVM graváveis e permite que você forneça dados aos clientes.

Passos

Você pode executar esta tarefa a partir do Gerenciador do sistema ou da CLI do ONTAP.

System Manager

1. Se o cluster de origem estiver acessível, verifique se o SVM está parado: Navegue até **Storage > Storage VMs** e verifique a coluna **State** para o SVM.
2. Se o estado da SVM de origem for "em execução", pare-o: Selecione ⋮ e escolha **Stop**.
3. No cluster de destino, localize a relação de proteção desejada: Navegue até **proteção > relacionamentos**.
4. Passe o Mouse sobre o nome da VM de armazenamento de origem desejada, clique ⋮ em e escolha **Ativar destino Storage VM**.
5. Na janela **Ativar VM** de armazenamento de destino, selecione **Ativar a VM de armazenamento de destino e quebre a relação**.
6. Clique em **Ativar**.

CLI

1. No SVM de destino ou no cluster de destino, pare as transferências agendadas para o destino:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir interrompe as transferências agendadas entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

2. A partir do SVM de destino ou do cluster de destino, interrompa as transferências contínuas para o destino:

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir interrompe as transferências contínuas entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

3. No SVM de destino ou no cluster de destino, interrompa a relação de replicação:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir rompe a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

4. Se você definir `-identity-preserve true` quando criou a relação de replicação SVM, pare o SVM de origem:

```
vserver stop -vserver <SVM>
```

O exemplo a seguir interrompe o SVM de origem `svm1` :

```
cluster_src::> vserver stop svm1
```

5. Inicie o SVM de destino:

```
vserver start -vserver <SVM>
```

O exemplo a seguir inicia o SVM de destino `svm_backup` :

```
cluster_dst::> vserver start svm_backup
```

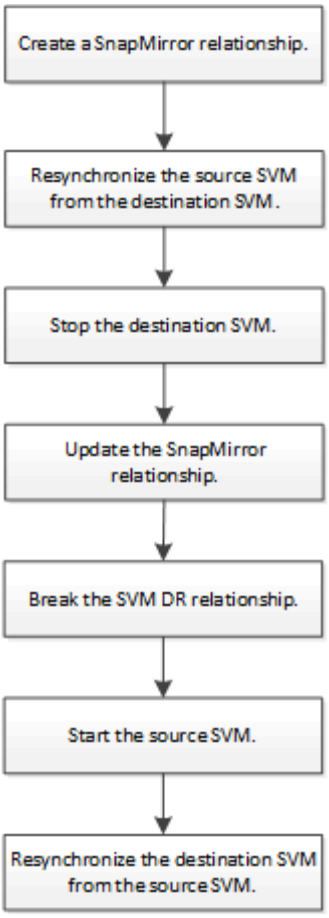
Depois de terminar

Configurar volumes de destino do SVM para acesso aos dados, conforme descrito "Configurar o volume de destino para acesso aos dados"em .

Reative o SVM de origem

Fluxo de trabalho de reativação do SVM de origem ONTAP

Se o SVM de origem existir após um desastre, você poderá reativá-lo e protegê-lo recriando a relação de recuperação de desastres da SVM.



Reative o SVM original da fonte do ONTAP

É possível restabelecer a relação de proteção de dados original entre a fonte e o SVM de destino, quando não precisar mais fornecer dados do destino. O procedimento é em grande parte idêntico ao procedimento para replicação de volume, com uma exceção. É necessário interromper o SVM de destino antes de reativar o SVM de origem.

Antes de começar

Se você tiver aumentado o tamanho do volume de destino ao fornecer dados a partir dele, antes de reativar o volume de origem, você deve aumentar manualmente o dimensionamento máximo no volume de origem original para garantir que ele possa crescer o suficiente.

"Quando um volume de destino cresce automaticamente"

Sobre esta tarefa

A partir do ONTAP 9.11,1, você pode reduzir o tempo de ressincronização durante um ensaio de recuperação de desastres usando a opção CLI do `snapmirror resync` comando enquanto executa uma ressincronização `-quick-resync true`reversa de uma relação SVM DR. Uma ressincronização rápida pode reduzir o tempo necessário para retornar à produção ignorando as operações de reconstrução e restauração do data warehouse.

> A ressincronização rápida não preserva a eficiência de storage dos volumes de destino. A ativação da ressincronização rápida pode aumentar o espaço de volume usado pelos volumes de destino.

Este procedimento pressupõe que a linha de base no volume de origem original está intacta. Se a linha de base não estiver intacta, você deverá criar e inicializar a relação entre o volume do qual você está fornecendo dados e o volume de origem original antes de executar o procedimento.

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para reativar uma VM de armazenamento de origem após um desastre. A reativação da VM de armazenamento de origem interrompe a VM de armazenamento de destino e rehabilita a replicação da origem para o destino.

Quando você usa o System Manager para reativar a VM de armazenamento de origem, o System Manager executa as seguintes operações em segundo plano:

- Cria uma relação de DR SVM reversa do destino original para a fonte original usando o SnapMirror Resync
- Pára o SVM de destino
- Atualiza a relação do SnapMirror
- Quebra o relacionamento SnapMirror
- Reinicia o SVM original
- Emite uma ressincronização SnapMirror da origem original de volta ao destino original
- Limpa as relações SnapMirror

Passos

Você pode executar esta tarefa a partir do Gerenciador do sistema ou da CLI do ONTAP.

System Manager

1. No cluster de destino, clique em **proteção > relacionamentos** e localize a relação de proteção desejada.
2. Passe o Mouse sobre o nome do relacionamento de origem, clique em e selecione **reativar VM de armazenamento de origem**.
3. Na janela **reativar VM** de armazenamento de origem, clique em **reativar**.
4. Em **relacionamentos**, monitore o progresso da reativação da fonte visualizando **Status da transferência** para o relacionamento de proteção. Quando a reativação estiver concluída, o estado do relacionamento deve retornar para "espelhado".

CLI

1. A partir do SVM de origem original ou do cluster de origem original, crie uma relação SVM DR reversa usando a mesma configuração, política e configuração de preservação de identidade que a relação SVM DR original:

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir cria uma relação entre o SVM a partir do qual você está fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

2. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para reverter a relação de proteção de dados:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

> O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. Use `snapmirror initialize` para reinicializar o relacionamento.

O exemplo a seguir inverte a relação entre o SVM de origem original e `svm1` o SVM a partir do qual você está fornecendo dados, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Exemplo usando a opção -Quick-Resync:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. Quando você quiser restabelecer o acesso aos dados à fonte original SVM, pare o SVM de destino original para desconetar todos os clientes conectados ao SVM de destino original.

```
vserver stop -vserver <SVM>
```

O exemplo a seguir interrompe o SVM de destino original que está fornecendo dados no momento:

```
cluster_dst::> vserver stop svm_backup
```

4. Verifique se o SVM de destino original está no estado parado usando o `vserver show` comando.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para executar a atualização final da relação invertida para transferir todas as alterações do SVM de destino original para o SVM de origem original:

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir atualiza a relação entre o SVM de destino original a partir do qual você está fornecendo dados,`svm_backup`e o SVM de origem original `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

6. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para interromper as transferências agendadas para o relacionamento invertido:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir interrompe as transferências agendadas entre o SVM que você está fornecendo dados, `svm_backup` e o SVM original `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. Quando a atualização final estiver concluída e o relacionamento indicar "Quiesced" para o status do relacionamento, execute o seguinte comando da fonte original SVM ou do cluster de origem original para quebrar o relacionamento invertido:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir rompe a relação entre o SVM de destino original do qual você estava fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

8. Se o SVM de origem original tiver sido interrompido anteriormente, a partir do cluster de origem original, inicie o SVM de origem original:

```
vserver start -vserver <SVM>
```

O exemplo a seguir inicia a fonte original SVM:

```
cluster_src::> vserver start svm1
```

9. A partir do SVM de destino original ou do cluster de destino original, restabeleça a relação de proteção de dados original:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir restabelece a relação entre a fonte original SVM e `svm1` o SVM de destino original `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para excluir a relação de proteção de dados invertida:

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir exclui a relação inversa entre o SVM de destino original e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. No SVM de destino original ou no cluster de destino original, solte a relação de proteção de dados invertida:

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir libera a relação inversa entre o SVM de destino original, SVM_backup e a fonte original SVM, `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Reative o SVM original de fonte do ONTAP para volumes do FlexGroup

É possível restabelecer a relação de proteção de dados original entre a fonte e o SVM de destino, quando não precisar mais fornecer dados do destino. Para reativar o SVM de origem original quando você estiver usando o FlexGroup volumes, você precisa executar algumas etapas adicionais, incluindo excluir a relação original do SVM DR e liberar a relação original antes de reverter a relação. Você também precisa liberar o relacionamento invertido e recriar o relacionamento original antes de parar as transferências agendadas.

Passos

1. No SVM de destino original ou no cluster de destino original, exclua a relação de DR original do SVM:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir exclui a relação original entre a fonte original SVM, svm1 e o SVM de destino original `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. A partir do SVM de origem original ou do cluster de origem original, solte a relação original e mantenha as cópias Snapshot intactas:

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir libera a relação original entre a fonte original SVM, svm1 e o SVM de destino original, `svm_backup`.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. A partir do SVM de origem original ou do cluster de origem original, crie uma relação SVM DR reversa usando a mesma configuração, política e configuração de preservação de identidade que a relação SVM DR original:

`snapmirror create -source-path SVM: -destination-path SVM:`

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir cria uma relação entre o SVM a partir do qual você está fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para reverter a relação de proteção de dados:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

   > O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. Use `snapmirror initialize` para reinicializar o relacionamento.

   O exemplo a seguir inverte a relação entre o SVM de origem original e `svm1` o SVM a partir do qual você está fornecendo dados, `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

5. Quando você quiser restabelecer o acesso aos dados à fonte original SVM, pare o SVM de destino original para desconetar todos os clientes conectados ao SVM de destino original.

   `vserver stop -vserver SVM`

   O exemplo a seguir interrompe o SVM de destino original que está fornecendo dados no momento:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

6. Verifique se o SVM de destino original está no estado parado usando o `vserver show` comando.

```
cluster_dst::> vserver show
                                  Admin      Operational Root
Vserver        Type    Subtype    State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default    stopped    stopped     rv
aggr1
```

7. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para executar a atualização final da relação invertida para transferir todas as alterações do SVM de destino original para o SVM de origem original:

   `snapmirror update -source-path` *SVM*`:` `-destination-path` *SVM*`:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir atualiza a relação entre o SVM de destino original a partir do qual você está fornecendo dados,`svm_backup`e o SVM de origem original `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para interromper as transferências agendadas para o relacionamento invertido:

   `snapmirror quiesce -source-path` *SVM*`:` `-destination-path` *SVM*`:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir interrompe as transferências agendadas entre o SVM que você está fornecendo dados, `svm_backup` e o SVM original `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

9. Quando a atualização final estiver concluída e o relacionamento indicar "Quiesced" para o status do relacionamento, execute o seguinte comando da fonte original SVM ou do cluster de origem original para quebrar o relacionamento invertido:

   `snapmirror break -source-path` *SVM*`:` `-destination-path` *SVM*`:`

Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir rompe a relação entre o SVM de destino original do qual você estava fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

10. Se o SVM de origem original tiver sido interrompido anteriormente, a partir do cluster de origem original, inicie o SVM de origem original:

    `vserver start -vserver` *SVM*

    O exemplo a seguir inicia a fonte original SVM:

    ```
    cluster_src::> vserver start svm1
    ```

11. No SVM de origem original ou no cluster de origem original, exclua a relação SVM DR invertida:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir exclui a relação inversa entre o SVM de destino original, SVM_backup e a fonte original SVM `svm1`:

    ```
    cluster_src::> snapmirror delete -source-path svm_backup: -destination
    -path svm1:
    ```

12. Do SVM de destino original ou do cluster de destino original, libere a relação inversa enquanto mantém as cópias Snapshot intactas:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir libera a relação inversa entre o SVM de destino original, SVM_backup e a fonte original SVM, svm1:

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. A partir do SVM de destino original ou do cluster de destino original, recrie a relação original. Use a mesma configuração, política e configuração de preservação de identidade que a relação original do SVM DR:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir cria uma relação entre a fonte original SVM e `svm1` o SVM de destino original `svm_backup`:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. A partir do SVM de destino original ou do cluster de destino original, restabeleça a relação de proteção de dados original:

    `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

    > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir restabelece a relação entre a fonte original SVM e `svm1` o SVM de destino original `svm_backup`:

    ```
    cluster_dst::> snapmirror resync -source-path svm1: -destination-path
    svm_backup:
    ```

Ressincronize os dados em um SVM de destino do ONTAP

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para ressincronizar os dados e os detalhes de configuração da VM de armazenamento de origem para a VM de armazenamento de destino em um relacionamento de proteção quebrado e restabelecer o relacionamento.

O ONTAP 9.11,1 introduz uma opção para ignorar uma reconstrução completa do data warehouse quando você executa um ensaio de recuperação de desastres, permitindo que você retorne à produção mais rapidamente.

Você executa a operação ressincronizada somente a partir do destino da relação original. A ressincronização exclui todos os dados na VM de armazenamento de destino mais recentes que os dados na VM de

armazenamento de origem.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para executar esta tarefa.

System Manager

1. No destino, selecione a relação de proteção desejada: Clique em **proteção > relacionamentos**.
2. Opcionalmente, selecione **execute uma ressincronização rápida** para ignorar uma reconstrução completa do data warehouse durante um ensaio de recuperação de desastres.
3. Clique ⋮ e clique em **Resync**.
4. Em **relacionamentos**, monitore o progresso da ressincronização visualizando **Status da transferência** para o relacionamento.

CLI

1. A partir do cluster de destino, ressincronize a relação:

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

Converter uma relação de recuperação de desastres em volume do ONTAP em uma relação de SVM DR

É possível converter relações de replicação entre volumes para uma relação de replicação entre as máquinas virtuais de armazenamento (SVMs) que possuem os volumes, desde que cada volume na origem (exceto o volume raiz) esteja sendo replicado e cada volume na origem (incluindo o volume raiz) tenha o mesmo nome do volume no destino.

Sobre esta tarefa

Use o `volume rename` comando quando a relação SnapMirror estiver inativa para renomear volumes de destino, se necessário.

Passos

1. No SVM de destino ou no cluster de destino, execute o seguinte comando para ressincronizar os volumes de origem e destino:

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   > Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

   O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA` ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

2. Crie uma relação de replicação SVM entre as SVMs de origem e destino, conforme descrito em "Replicação de configurações da SVM".

   Você deve usar a `-identity-preserve true` opção `snapmirror create` do comando ao criar sua relação de replicação.

3. Pare o SVM de destino:

   `vserver stop -vserver` *SVM*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir interrompe o SVM de destino `svm_backup` :

```
cluster_dst::> vserver stop svm_backup
```

4. No SVM de destino ou no cluster de destino, execute o seguinte comando para ressincronizar as SVMs de origem e destino:

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.
   >
   > Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

   O exemplo a seguir ressincroniza a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Exclua uma relação de replicação do ONTAP SVM

Você pode usar os `snapmirror delete` comandos e `snapmirror release` para excluir uma relação de replicação SVM. Em seguida, pode eliminar manualmente volumes de destino desnecessários.

Sobre esta tarefa

`snapmirror release`O comando exclui todas as cópias Snapshot criadas pelo SnapMirror da origem. Você pode usar a `-relationship-info-only` opção para preservar as cópias Snapshot.

Para obter a sintaxe de comando completa nos comandos, consulte a página man.

Passos

1. Execute o seguinte comando a partir do SVM de destino ou do cluster de destino para quebrar a relação de replicação:

   `snapmirror break -source-path` *SVM*`: -destination-path` *SVM*`:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir rompe a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

2. Execute o seguinte comando do SVM de destino ou do cluster de destino para excluir a relação de replicação:

   `snapmirror delete -source-path` *SVM*`: -destination-path` *SVM*`:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir exclui a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

3. Execute o seguinte comando a partir do cluster de origem ou SVM de origem para liberar as informações de relação de replicação da SVM de origem:

   `snapmirror release -source-path` *SVM*`: -destination-path` *SVM*`:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir libera informações para a relação de replicação especificada da SVM de origem `svm1` :

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

Gerenciar a replicação de volume raiz do SnapMirror

Gerenciar a visão geral da replicação de volume raiz do SnapMirror

Cada SVM em um ambiente nas tem um namespace único. O volume SVM *root,* contendo sistema operacional e informações relacionadas, é o ponto de entrada para a hierarquia do namespace. Para garantir que os dados permaneçam acessíveis aos clientes em caso de interrupção de nó ou failover, crie uma cópia espelhada de compartilhamento de carga do volume raiz do SVM.

O principal objetivo dos espelhos de compartilhamento de carga para volumes raiz do SVM não é mais para compartilhamento de carga; em vez disso, seu objetivo é a recuperação de desastres.

- Se o volume raiz estiver temporariamente indisponível, o espelhamento de compartilhamento de carga fornece automaticamente acesso somente leitura aos dados do volume raiz.
- Se o volume raiz estiver permanentemente indisponível, você poderá promover um dos volumes de compartilhamento de carga para fornecer acesso de gravação aos dados de volume raiz.

Criar e inicializar relações de espelhamento de compartilhamento de carga

Você deve criar um espelhamento de compartilhamento de carga (LSM) para cada volume raiz da SVM que forneça dados nas no cluster. Para clusters que consistam em dois ou mais pares de HA, considere espelhos de compartilhamento de carga dos volumes raiz do SVM para garantir que o namespace permaneça acessível aos clientes caso ambos os nós de um par de HA falhem. Os espelhos de compartilhamento de carga não são adequados para clusters que consistam em um único par de HA.

Sobre esta tarefa

Se você criar um LSM no mesmo nó e o nó não estiver disponível, você terá um único ponto de falha e não terá uma segunda cópia para garantir que os dados permaneçam acessíveis aos clientes. Mas quando você cria o LSM em um nó diferente daquele que contém o volume raiz ou em um par de HA diferente, seus dados ainda estarão acessíveis no caso de uma interrupção.

Por exemplo, em um cluster de quatro nós com um volume raiz em três nós:

- Para o volume raiz no nó 1 do HA 1, crie o LSM no nó HA 2 do HA 1 ou no nó HA 2 do HA 2.
- Para o volume raiz no nó 2 do HA 1, crie o LSM no nó HA 2 do HA 1 ou no nó HA 2 do HA 2.
- Para o volume raiz no nó 1 do HA 2, crie o LSM no nó HA 1 do HA 1 ou no nó HA 1 do HA 2.

Passos

1. Criar um volume de destino para o LSM:

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

O volume de destino deve ser igual ou maior em tamanho do que o volume raiz.

É uma prática recomendada nomear o volume de raiz e destino com sufixos, como `_root` e `_m1`.

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria um volume de espelhamento de compartilhamento de carga para o volume raiz `svm1_root` no `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Crie um cronograma de trabalho de replicações".
3. Crie uma relação de espelhamento de compartilhamento de carga entre o volume raiz da SVM e o volume de destino do LSM:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria uma relação de espelhamento de compartilhamento de carga entre o volume raiz `svm1_root` e o volume de espelhamento de compartilhamento de carga `svm1_m1` :

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

O atributo de tipo do espelho de compartilhamento de carga muda de `DP` para `LS`.

4. Inicialize o espelho de partilha de carga:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir inicializa o espelho de compartilhamento de carga para o volume raiz `svm1_root` :

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

Atualize uma relação de espelhamento de compartilhamento de carga

As relações de espelhamento de compartilhamento de carga (LSM) são atualizadas automaticamente para volumes raiz do SVM depois que um volume no SVM é montado ou desmontado e durante `volume create` operações que incluem a opção "caminho de junção". Você pode atualizar manualmente uma relação LSM se desejar que ela seja atualizada antes da próxima atualização agendada.

As relações de espelhamento de compartilhamento de carga são atualizadas automaticamente nas seguintes circunstâncias:

- É hora de uma atualização agendada
- Uma operação de montagem ou desmontagem é realizada em um volume no volume raiz do SVM
- Um `volume create` comando é emitido que inclui a `juntion-path` opção

Passo

1. Atualize manualmente uma relação de espelhamento de compartilhamento de carga:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   O exemplo a seguir atualiza a relação de espelhamento de compartilhamento de carga para o volume raiz `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

Promova um espelho de compartilhamento de carga

Se um volume raiz estiver permanentemente indisponível, você poderá promover o volume de espelhamento de carga (LSM) para fornecer acesso de gravação aos dados de volume raiz.

O que você vai precisar

Tem de utilizar comandos avançados de nível de privilégio para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Promover um volume LSM:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar

este comando.

```
snapmirror promote -destination-path <SVM:volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir promove o volume `svm1_m2` como o novo volume raiz da SVM:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Introduza `y`. O ONTAP torna o volume LSM um volume de leitura/gravação e exclui o volume raiz original se ele estiver acessível.

> O volume raiz promovido pode não ter todos os dados que estavam no volume raiz original se a última atualização não ocorrer recentemente.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

4. Renomeie o volume promovido seguindo a convenção de nomenclatura usada para o volume raiz:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   O exemplo a seguir renomeia o volume promovido `svm1_m2` com o nome `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Proteja o volume raiz renomeado, conforme descrito na etapa 3 até a etapa 4 em "Criando e inicializando relações de espelhamento de compartilhamento de carga".

Fazer backup na nuvem

Faça backup dos dados na nuvem usando o SnapMirror

A partir do ONTAP 9.9,1, é possível fazer backup dos dados na nuvem e restaurar os dados do storage de nuvem para um volume diferente usando o Gerenciador do sistema. Você pode usar o StorageGRID ou o ONTAP S3 como armazenamento de objetos na nuvem.

Antes de usar o recurso de nuvem do SnapMirror, você deve solicitar uma chave de licença da API de nuvem do SnapMirror no site de suporte da NetApp: "Solicite a chave de licença da API de nuvem da SnapMirror". Seguindo as instruções, você deve fornecer uma descrição simples da sua oportunidade de negócio e solicitar a chave API enviando um e-mail para o endereço de e-mail fornecido. Você deve receber uma resposta por e-mail dentro de 24 horas com mais instruções sobre como adquirir a chave da API.

Adicionar um armazenamento de objetos na nuvem

Antes de configurar os backups na nuvem do SnapMirror, é necessário adicionar um armazenamento de objetos em nuvem do StorageGRID ou do ONTAP S3.

Passos

1. Clique em **proteção > Visão geral > Cloud Object Stores**.
2. Clique + Add em .

Faça backup usando a política padrão

Você pode configurar rapidamente um backup na nuvem do SnapMirror para um volume existente usando a política de proteção de nuvem padrão, DailyBackup.

Passos

1. Clique em **proteção > Visão geral** e selecione **fazer backup de volumes para o Cloud**.
2. Se esta for a primeira vez que fizer o backup na nuvem, insira sua chave de licença da API da nuvem do SnapMirror no campo de licença, conforme indicado.
3. Clique em **autenticar e continuar**.
4. Selecione um volume de origem.
5. Selecione um armazenamento de objetos na nuvem.
6. Clique em **Salvar**.

Crie uma política de backup personalizada na nuvem

Se você não quiser usar a política de nuvem padrão do DailyBackup para seus backups na nuvem do SnapMirror, você pode criar sua própria política.

Passos

1. Clique em **proteção > Visão geral > Configurações de política local** e selecione **políticas de proteção**.
2. Clique em **Add** e insira os novos detalhes da política.
3. Na seção **tipo de política**, selecione **fazer backup na nuvem** para indicar que você está criando uma política de nuvem.

4. Clique em **Salvar**.

Crie uma cópia de segurança a partir da página volumes

Você pode usar a página System Manager **volumes** quando quiser selecionar e criar backups na nuvem para vários volumes ao mesmo tempo ou quando quiser usar uma política de proteção personalizada.

Passos

1. Clique em **armazenamento > volumes**.
2. Selecione os volumes que deseja fazer backup na nuvem e clique em **proteger**.
3. Na janela **Protect volume**, clique em **More Options** (mais opções).
4. Selecione uma política.

   Você pode selecionar a política padrão, DailyBackup ou uma política de nuvem personalizada criada.

5. Selecione um armazenamento de objetos na nuvem.
6. Clique em **Salvar**.

Restauração a partir da nuvem

Você pode usar o System Manager para restaurar dados de backup do storage de nuvem para um volume diferente no cluster de origem.

> Se você estiver usando o ONTAP 9.16,1 e estiver executando uma restauração de arquivo único na nuvem do SnapMirror para um volume FlexGroup, você só deverá restaurar arquivos para um novo diretório no volume FlexGroup.

Passos

1. No cluster de origem de uma relação SnapMirror-para-nuvem, clique em **armazenamento > volumes**.
2. Selecione o volume que pretende restaurar.
3. Selecione a guia **fazer backup para a nuvem**.
4. Clique ⋮ ao lado do volume de origem que deseja restaurar para exibir o menu e selecione **Restaurar**.
5. Em **fonte**, selecione uma VM de armazenamento e, em seguida, insira o nome do volume para o qual deseja que os dados sejam restaurados.
6. Em **destino**, selecione a cópia Snapshot que deseja restaurar.
7. Clique em **Salvar**.

Excluir uma relação de nuvem do SnapMirror

Você pode usar o System Manager para excluir uma relação de nuvem.

Passos

1. Clique em **armazenamento > volumes** e selecione o volume que deseja excluir.
2. Clique ⋮ ao lado do volume de origem e selecione **Excluir**.
3. Selecione **Excluir o endpoint do armazenamento de objetos na nuvem (opcional)** se você quiser excluir o endpoint do armazenamento de objetos na nuvem.
4. Clique em **Excluir**.

Remover um armazenamento de objetos na nuvem

Você pode usar o System Manager para remover um armazenamento de objetos na nuvem se ele não fizer parte de um relacionamento de backup na nuvem. Quando um armazenamento de objetos em nuvem faz parte de uma relação de backup em nuvem, ele não pode ser excluído.

Passos

1. Clique em **proteção > Visão geral > Cloud Object Stores**.
2. Selecione o armazenamento de objetos que deseja excluir, clique ⋮ e selecione **Excluir**.

Faça backup dos dados usando o serviço de backup e recuperação do BlueXP

A partir do ONTAP 9,9.1, você pode usar o Gerenciador de sistema para fazer backup de dados na nuvem usando o serviço de backup e recuperação do BlueXP (anteriormente Cloud Backup Service).

O serviço de backup e recuperação do BlueXP é compatível com volumes de leitura-gravação FlexVol e volumes de proteção de dados (DP). A partir do ONTAP 9.12.1, o serviço de backup e recuperação do BlueXP é compatível com FlexGroup volumes e SnapLock volumes.

Saiba mais "Backup e recuperação do BlueXP"sobre o .

Antes de começar

Você deve executar os seguintes procedimentos para estabelecer uma conta no BlueXP . Para a conta de serviço, você precisa criar a função como "Administrador da conta". (Outras funções de conta de serviço não têm o Privileges necessário para estabelecer uma conexão do Gerenciador de sistema.)

1. "Crie uma conta no BlueXP ".
2. "Crie um conetor no BlueXP " com um dos seguintes fornecedores de nuvem:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > ⓘ A partir do ONTAP 9.10.1, você pode selecionar o StorageGRID como um fornecedor de backup em nuvem, mas somente se o BlueXP for implantado no local. O BlueXP Connector deve ser instalado no local e disponível por meio do aplicativo software como serviço (SaaS) da BlueXP .

3. "Assine o serviço de backup e recuperação do BlueXP no BlueXP" (requer a licença apropriada).
4. "Gere uma chave de acesso e uma chave secreta usando o BlueXP ".

Registre o cluster no BlueXP

Você pode Registrar o cluster no BlueXP usando o BlueXP ou o Gerenciador de sistema.

Passos

1. No System Manager, vá para **Visão geral da proteção**.
2. Em **Backup e recuperação BlueXP** , forneça os seguintes detalhes:

- ID do cliente
- Chave secreta do cliente

3. Selecione **Registe-se e continue**.

Ative o backup e a recuperação do BlueXP

Depois que o cluster é registrado no BlueXP , você precisa habilitar o backup e a recuperação do BlueXP e iniciar o primeiro backup na nuvem.

Passos

1. No Gestor do sistema, selecione **proteção > Descrição geral** e, em seguida, desloque-se para a secção **Cloud Backup Service**.
2. Insira **Client ID** e **Client Secret**.

> A partir do ONTAP 9.10.1, você pode aprender sobre o custo de usar a nuvem selecionando **Saiba mais sobre o custo de usar a nuvem**.

3. Selecione **conetar e ativar o Cloud Backup Service**.
4. Na página **Ativar backup e recuperação do BlueXP** , forneça os seguintes detalhes, dependendo do provedor selecionado.

Para este provedor de nuvem…	Introduza os seguintes dados…
Azure	• ID de subscrição do Azure • Região • Nome do grupo de recursos (existente ou novo)
AWS	• ID da conta da AWS • Chave de acesso • Chave secreta • Região
Projeto Google Cloud (GCP)	• Nome do projeto Google Cloud • Chave de acesso ao Google Cloud • Chave secreta do Google Cloud • Região
StorageGRID (ONTAP 9.10.1 e posterior, e somente para implantação local do BlueXP)	• Servidor • Chave de Acesso SG • Chave secreta SG

5. Selecione uma **Política de proteção**:
   - **Política existente**: Escolha uma política existente.
   - **Nova Política**: Especifique um nome e configure um agendamento de transferência.

A partir do ONTAP 9.10,1, você pode especificar se deseja ativar o arquivamento com o Azure ou a AWS.

Se você habilitar o arquivamento para um volume com o Azure ou AWS, não será possível desativar o arquivamento.

Se você habilitar o arquivamento para o Azure ou AWS, especifique o seguinte:

- O número de dias após os quais o volume é arquivado.
- O número de cópias de segurança a reter no arquivo. Especifique "0" (zero) para arquivar até o backup mais recente.
- Para AWS, selecione a classe de armazenamento de arquivo.

6. Selecione os volumes que pretende efetuar uma cópia de segurança.
7. Selecione **Guardar**.

Edite a política de proteção usada para backup e recuperação do BlueXP

Você pode alterar a política de proteção usada com o backup e a recuperação do BlueXP .

Passos

1. No Gestor do sistema, selecione **proteção > Descrição geral** e, em seguida, desloque-se para a secção **Cloud Backup Service**.
2. Selecione e, em seguida, **Editar**.
3. Selecione uma **Política de proteção**:
   - **Política existente**: Escolha uma política existente.
   - **Nova Política**: Especifique um nome e configure um agendamento de transferência.

A partir do ONTAP 9.10,1, você pode especificar se deseja ativar o arquivamento com o Azure ou a AWS.

Se você habilitar o arquivamento para um volume com o Azure ou AWS, não será possível desativar o arquivamento.

Se você habilitar o arquivamento para o Azure ou AWS, especifique o seguinte:

- O número de dias após os quais o volume é arquivado.
- O número de cópias de segurança a reter no arquivo. Especifique "0" (zero) para arquivar até o backup mais recente.
- Para AWS, selecione a classe de armazenamento de arquivo.

4. Selecione **Guardar**.

Proteger novos volumes ou LUNs na nuvem

Ao criar um novo volume ou LUN, você pode estabelecer uma relação de proteção SnapMirror que permite fazer backup na nuvem para o volume ou LUN.

Antes de começar

- Você deve ter uma licença SnapMirror.
- LIFs entre clusters devem ser configurados.
- NTP deve ser configurado.
- O cluster deve estar executando o ONTAP 9.9,1.

Sobre esta tarefa

Não é possível proteger novos volumes ou LUNs na nuvem nas seguintes configurações de cluster:

- O cluster não pode estar em um ambiente MetroCluster.
- O SVM-DR não é compatível.
- Não é possível fazer backup do FlexGroups usando backup e recuperação do BlueXP .

Passos

1. Ao provisionar um volume ou LUN, na página **proteção** no Gerenciador de sistema, marque a caixa de seleção **Ativar SnapMirror (local ou remoto)**.
2. Selecione o tipo de política de backup e recuperação do BlueXP .
3. Se o serviço de backup e recuperação do BlueXP não estiver habilitado, selecione **Ativar backup usando o serviço de backup e recuperação do BlueXP** .

Proteger volumes ou LUNs existentes na nuvem

É possível estabelecer uma relação de proteção SnapMirror para volumes e LUNs existentes.

Passos

1. Selecione um volume ou LUN existente e selecione **Protect**.
2. Na página **proteger volumes**, especifique **Backup usando o serviço de backup e recuperação BlueXP** para a política de proteção.
3. Selecione **Protect**.
4. Na página **proteção**, marque a caixa de seleção **Ativar SnapMirror (local ou remoto)**.
5. Selecione **conetar e ativar o backup e a recuperação do BlueXP** .

Restaurar dados de arquivos de backup

Você pode executar operações de gerenciamento de backup, como restauração de dados, atualização de relacionamentos e exclusão de relacionamentos, somente quando usar a interface do BlueXP . "Restaurar dados de arquivos de backup"Consulte para obter mais informações.

Detalhes técnicos do SnapMirror

Use a correspondência de padrão de nome de caminho

Você pode usar a correspondência de padrões para especificar os caminhos de origem e destino nos `snapmirror` comandos.

`snapmirror` os comandos usam nomes de caminho totalmente qualificados no seguinte formato: `vserver:volume`. Você pode abreviar o nome do caminho não inserindo o nome do SVM. Se você fizer isso, o `snapmirror` comando assumirá o contexto local SVM do usuário.

Supondo que o SVM seja chamado de "'vserver1'" e o volume seja chamado de "'vol1'", o nome do caminho totalmente qualificado é `vserver1:vol1`.

Você pode usar o asterisco (*) nos caminhos como um curinga para selecionar nomes de caminho correspondentes e totalmente qualificados. A tabela a seguir fornece exemplos de como usar o caractere curinga para selecionar um intervalo de volumes.

`*`	Corresponde a todos os caminhos.
`vs*`	Faz a correspondência de todos os SVMs e volumes com nomes SVM que começam com `vs`.
`:*src`	Corresponde a todos os SVMs com nomes de volume que contêm o `src` texto.
`:vol`	Corresponde a todos os SVMs com nomes de volume começando com `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------ ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

Use consultas estendidas para agir em muitos relacionamentos do SnapMirror

Você pode usar *consultas estendidas* para executar operações do SnapMirror em muitos relacionamentos do SnapMirror ao mesmo tempo. Por exemplo, você pode ter várias relações SnapMirror não inicializadas que deseja inicializar usando um comando.

Sobre esta tarefa

Você pode aplicar consultas estendidas às seguintes operações do SnapMirror:

- Inicializando relacionamentos não inicializados
- Retomando relacionamentos quiesced
- Ressincronizar relacionamentos quebrados
- Atualizando relacionamentos ociosos
- A abortar transferências de dados de relacionamento

Passo

1. Execute uma operação SnapMirror em muitos relacionamentos:

   snapmirror command `{-state state } *`

   O comando a seguir inicializa as relações SnapMirror que estão em um `Uninitialized` estado:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

Garanta uma cópia Snapshot comum em uma implantação de cofre-espelho

Você pode usar o `snapmirror snapshot-owner create` comando para preservar uma cópia Snapshot rotulada no secundário em uma implantação do mirror-Vault. Isso garante que existe uma cópia Snapshot comum para a atualização da relação do Vault.

Sobre esta tarefa

Se você usar uma combinação de fan-out do mirror-Vault ou implantação em cascata, você deve ter em mente que as atualizações falharão se uma cópia Snapshot comum não existir nos volumes de origem e destino.

Esse nunca é um problema para a relação de espelhamento em uma implantação em fan-out ou cascata do mirror-Vault, já que o SnapMirror sempre cria uma cópia Snapshot do volume de origem antes de executar a atualização.

No entanto, pode ser um problema para a relação do Vault, uma vez que o SnapMirror não cria uma cópia Snapshot do volume de origem quando atualiza uma relação do Vault. Você precisa usar o `snapmirror snapshot-owner create` para garantir que haja pelo menos uma cópia Snapshot comum na origem e no destino da relação do Vault.

Passos

1. No volume de origem, atribua um proprietário à cópia Snapshot rotulada que deseja preservar:

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   O exemplo a seguir é designado `ApplicationA` como o proprietário da `snap1` cópia Snapshot:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

2. Atualize a relação do espelho, conforme descrito em "Atualizar manualmente uma relação de replicação".

   Alternativamente, você pode esperar pela atualização agendada do relacionamento espelhado.

3. Transfira a cópia Snapshot rotulada para o destino do Vault:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir transfere a `snap1` cópia Snapshot

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   A cópia Snapshot rotulada será preservada quando a relação do Vault for atualizada.

4. No volume de origem, remova o proprietário da cópia Snapshot rotulada:

   ```
   snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot
   snapshot -owner owner
   ```

   Os exemplos a seguir são removidos `ApplicationA` como o proprietário da `snap1` cópia Snapshot:

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

Versões compatíveis do ONTAP para relacionamentos do SnapMirror

Os volumes de origem e destino devem estar executando versões compatíveis do ONTAP antes de criar uma relação de proteção de dados do SnapMirror. Antes de atualizar o ONTAP, você deve verificar se sua versão atual do ONTAP é compatível com a versão de destino do ONTAP para relacionamentos do SnapMirror.

Relacionamentos de replicação unificada

Para relacionamentos SnapMirror do tipo "XDP", usando versões locais ou Cloud Volumes ONTAP:

Começando com ONTAP 9.9,0:

- As versões do ONTAP 9.x,0 são versões somente na nuvem e oferecem suporte a sistemas Cloud Volumes ONTAP. O asterisco (*) após a versão de lançamento indica uma versão somente na nuvem.

> O ONTAP 9.16,0 é uma exceção à regra somente de nuvem fornecendo suporte "Sistemas ASA R2"para o . Os sistemas ASA R2 suportam relações SnapMirror apenas com outros sistemas ASA R2.

- As versões do ONTAP 9.x,1 são versões gerais e oferecem suporte a sistemas locais e Cloud Volumes ONTAP.

> Quando "balanceamento de capacidade avançado" o está ativado em volumes em clusters que executam o ONTAP 9.16.1 ou posterior, as transferências SnapMirror não são compatíveis com clusters que executam versões do ONTAP anteriores ao ONTAP 9.16.1.

> A interoperabilidade é bidirecional.

Interoperabilidade para ONTAP versão 9,3 e posterior

Versão ONTAP…	**Interopera com essas versões anteriores do ONTAP…**																				
	9.16.1	9.16.0	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9,9.0*	9,8	9,7	9,6	9,5	9,4	9,3
9.16.1	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.16.0	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.15.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.15.0*	Não	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.14.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não
9.14.0*	Não	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.13.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não
9.13.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não
9.12.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não
9.12.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	Não	Não	Não	Não

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…																					
9.11.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.11.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.10.1	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.10.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.9.1	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,9.0*	Não	Não	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,8	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,7	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,6	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,5	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
9,4	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	
9,3	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**

Relações síncronas da SnapMirror

O SnapMirror síncrono não é compatível com instâncias de nuvem do ONTAP.

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…											
	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.16.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não
9.15.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não

9.14.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.13.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.12.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.11.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não
9.10.1	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.9.1	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,8	Não	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não
9,7	Não	Não	Não	**Sim**	**Sim**	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
9,6	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**
9,5	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**

Relações de recuperação de desastres do SnapMirror SVM

Para dados de recuperação de desastres da SVM e proteção contra SVM:

A recuperação de desastres da SVM é compatível apenas entre clusters que executam a mesma versão do ONTAP. **A independência de versão não é suportada para replicação SVM**.

Na recuperação de desastres do SVM para migração SVM:

- A replicação é suportada em uma única direção de uma versão anterior do ONTAP na origem para a mesma ou posterior versão do ONTAP no destino.
- A versão do ONTAP no cluster de destino não deve ser mais do que duas versões principais no local mais recentes ou duas versões principais da nuvem mais recentes, como mostrado na tabela abaixo.
  - A replicação não é compatível com casos de uso de proteção de dados de longo prazo.

O asterisco (*) após a versão de lançamento indica uma versão somente na nuvem.

Para determinar o suporte, localize a versão de origem na coluna da tabela à esquerda e, em seguida, localize a versão de destino na linha superior (DR/migração para versões semelhantes e migração apenas para versões mais recentes).

Fonte	Destino																			
	9,3	9,4	9,5	9,6	9,7	9,8	9,9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1
9,3	DR/migração	Migração	Migração	Migração	Migração																	
9,4		DR/migração	Migração	Migração	Migração	Migração																

9,5			DR/migração	Migração	Migração	Migração	Migração														
9,6				DR/migração	Migração	Migração	Migração	Migração													
9,7					DR/migração	Migração	Migração	Migração	Migração												
9,8						DR/migração	Migração	Migração	Migração	Migração											
9,9.0*							DR/migração	Migração	Migração	Migração	Migração										
9.9.1								DR/migração	Migração	Migração	Migração	Migração									
9.10.0*									DR/migração	Migração	Migração	Migração	Migração								
9.10.1										DR/migração	Migração	Migração	Migração	Migração							
9.11.0*											DR/migração	Migração	Migração	Migração	Migração						
9.11.1												DR/migração	Migração	Migração	Migração	Migração					
9.12.0*													DR/migração	Migração	Migração	Migração	Migração				

9.12.1														DR/migração	Migração	Migração	Migração	Migração				
9.13.0*															DR/migração	Migração	Migração	Migração	Migração			
9.13.1																DR/migração	Migração	Migração	Migração	Migração		
9.14.0*																	DR/migração	Migração	Migração	Migração	Migração	
9.14.1																		DR/migração	Migração	Migração	Migração	Migração
9.15.0*																			DR/migração	Migração	Migração	Migração
9.15.1																				DR/migração	Migração	Migração
9.16.0																					DR/migração	Migração
9.16.1																						DR/migração

Relacionamentos de recuperação de desastres da SnapMirror

Para relações SnapMirror do tipo "DP" e do tipo de política "'assíncrono-mirror'":

Os espelhos do tipo DP não podem ser inicializados a partir do ONTAP 9.11,1 e são completamente obsoletos no ONTAP 9.12,1. Para obter mais informações, "Depreciação de relacionamentos SnapMirror de proteção de dados"consulte .

Na tabela a seguir, a coluna à esquerda indica a versão do ONTAP no volume de origem e a linha superior indica as versões do ONTAP que você pode ter no volume de destino.

Fonte	Destino											
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3	9,2	9,1	9
9.11.1	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.10.1	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.9.1	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não
9,8	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
9,7	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não
9,6	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
9,5	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não
9,4	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não
9,3	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não
9,2	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não
9,1	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não
9	Não	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim

A interoperabilidade não é bidirecional.

Limitações do SnapMirror

Você deve estar ciente das limitações básicas do SnapMirror antes de criar um relacionamento de proteção de dados.

- Um volume de destino pode ter apenas um volume de origem.

  Um volume de origem pode ter vários volumes de destino. O volume de destino pode ser o volume de origem para qualquer tipo de relação de replicação do SnapMirror.

- Dependendo do modelo do array, você pode distribuir um máximo de oito ou dezesseis volumes de destino a partir de um único volume de origem. Consulte "Hardware Universe"para obter detalhes sobre sua configuração específica.
- Não é possível restaurar arquivos para o destino de uma relação de DR do SnapMirror.
- Os volumes SnapVault de origem ou destino não podem ser de 32 bits.
- O volume de origem de uma relação SnapVault não deve ser um volume FlexClone.

  A relação funcionará, mas a eficiência oferecida pelos volumes FlexClone não será preservada.

Arquivamento e conformidade com a tecnologia SnapLock

O que é SnapLock

O SnapLock é uma solução de conformidade de alto desempenho para organizações que usam storage WORM para reter arquivos de forma não modificada para fins regulatórios e de governança.

O SnapLock ajuda a impedir a exclusão, alteração ou renomeação de dados para atender a regulamentações como SEC 17aa-4(f), HIPAA, FINRA, CFTC e GDPR. Com o SnapLock, você pode criar volumes de propósito especial nos quais arquivos podem ser armazenados e comprometidos com um estado não apagável e não gravável por um período de retenção designado ou indefinidamente. O SnapLock permite que essa retenção seja realizada no nível do arquivo por meio de protocolos padrão de arquivo aberto, como CIFS e NFS. Os protocolos de arquivos abertos compatíveis com o SnapLock são NFS (versões 2, 3 e 4) e CIFS (SMB 1,0, 2,0 e 3,0).

Com o SnapLock, você envia arquivos e cópias Snapshot para storage WORM e define períodos de retenção para dados protegidos WORM. O storage WORM do SnapLock usa a tecnologia NetApp Snapshot e pode utilizar a replicação SnapMirror e os backups SnapVault como a tecnologia base para fornecer proteção de recuperação de backup para dados. Saiba mais sobre o armazenamento WORM"Armazenamento WORM em conformidade com NetApp SnapLock - TR-4526": .

Você pode usar uma aplicação para comprometer arquivos WORM em NFS ou CIFS, ou usar o recurso de auto-commit do SnapLock para comprometer arquivos para WORM automaticamente. Você pode usar um arquivo anexado *WORM* para reter dados gravados de forma incremental, como informações de log. Para obter mais informações, "Use o modo de adição de volume para criar arquivos anexados WORM"consulte .

O SnapLock é compatível com métodos de proteção de dados que devem atender à maioria dos requisitos de conformidade:

- Você pode usar o SnapLock for SnapVault para proteger cópias Snapshot WORM no storage secundário. "Armazene cópias Snapshot no WORM"Consulte .
- Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres. "Espelhar arquivos WORM"Consulte .

SnapLock é um recurso baseado em licença do NetApp ONTAP. Uma única licença permite que você use o SnapLock em modo de conformidade estrita, para satisfazer mandatos externos, como a regra SEC 17a-4(f), e um modo empresarial mais solto, para atender aos regulamentos internos exigidos para a proteção de ativos digitais. As licenças SnapLock fazem parte do "ONTAP One"pacote de software.

O SnapLock é compatível com todos os sistemas AFF e FAS, bem como com o ONTAP Select. O SnapLock não é uma solução somente de software; é uma solução integrada de hardware e software. Essa distinção é importante para regulamentações WORM rígidas, como a SEC 17a-4(f), que requer uma solução integrada de hardware e software. Para obter mais informações, "SEC Orientação aos corretores-concessionários sobre a utilização de suportes de armazenamento eletrónicos"consulte .

O que você pode fazer com o SnapLock

Depois de configurar o SnapLock, você pode concluir as seguintes tarefas:

- "Armazene dados no WORM"
- "Armazene cópias Snapshot no WORM para storage secundário"
- "Espelhar arquivos WORM para recuperação de desastres"
- "Retenha arquivos WORM durante o litígio usando retenção legal"

- "Exclua arquivos WORM usando o recurso de exclusão privilegiada"
- "Defina o período de retenção do arquivo"
- "Mover um volume SnapLock"
- "Bloqueie uma cópia Snapshot para proteção contra ataques de ransomware"
- "Reveja a utilização do SnapLock com o Registo de Auditoria"
- "Use APIs do SnapLock"

Modos SnapLock Compliance e Enterprise

Os modos SnapLock Compliance e Enterprise diferem principalmente no nível em que cada modo protege arquivos WORM:

Modo SnapLock	Nível de proteção	Exclusão de arquivo WORM durante a retenção
Modo de conformidade	No nível do disco	Não pode ser eliminado
Modo empresarial	No nível do ficheiro	Pode ser excluído pelo administrador de conformidade usando um procedimento auditado de "exclusão privilegiada"

Após o período de retenção ter terminado, você é responsável por excluir quaisquer arquivos que você não precisa mais. Uma vez que um arquivo tenha sido comprometido com WORM, esteja em conformidade ou no modo Enterprise, ele não poderá ser modificado, mesmo depois que o período de retenção expirou.

Não é possível mover um arquivo WORM durante ou após o período de retenção. Você pode copiar um arquivo WORM, mas a cópia não reterá suas características WORM.

A tabela a seguir mostra as diferenças nos recursos suportados pelos modos SnapLock Compliance e Enterprise:

Capacidade	SnapLock Compliance	SnapLock Enterprise
Ative e exclua arquivos usando exclusão privilegiada	Não	Sim
Reinicializar os discos	Não	Sim
Destruir agregados e volumes SnapLock durante o período de retenção	Não	Sim, com exceção do volume de log de auditoria do SnapLock
Renomeie agregados ou volumes	Não	Sim
Use discos que não sejam NetApp	Não	Sim (com "Virtualização FlexArray")

Use o volume SnapLock para o log de auditoria	Sim	Sim, começando com ONTAP 9.5

Recursos suportados e não suportados com o SnapLock

A tabela a seguir mostra os recursos compatíveis com o modo SnapLock Compliance, o modo SnapLock Enterprise ou ambos:

Recurso	Compatível com SnapLock Compliance	Compatível com SnapLock Enterprise
Grupos de consistência	Não	Não
Volumes criptografados	Sim, começando com ONTAP 9.2. Saiba mais Criptografia e SnapLocksobre o .	Sim, começando com ONTAP 9.2. Saiba mais Criptografia e SnapLocksobre o .
FabricPools em agregados SnapLock	Não	Sim, começando com ONTAP 9.8. Saiba mais FabricPool em agregados SnapLock Enterprisesobre o .
Agregados Flash Pool	Sim, começando com ONTAP 9.1.	Sim, começando com ONTAP 9.1.
FlexClone	Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock.	Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock.
Volumes FlexGroup	Sim, começando com ONTAP 9.11,1. Saiba mais [flexgroup]sobre o .	Sim, começando com ONTAP 9.11,1. Saiba mais [flexgroup]sobre o .
LUNs	Não. Saiba mais sobre Suporte LUN o SnapLock.	Não. Saiba mais sobre Suporte LUN o SnapLock.
Configurações do MetroCluster	Sim, começando com ONTAP 9.3. Saiba mais Suporte à MetroClustersobre o .	Sim, começando com ONTAP 9.3. Saiba mais Suporte à MetroClustersobre o .
Verificação multi-admin (MAV)	Sim, começando com ONTAP 9.13,1. Saiba mais Suporte MAVsobre o .	Sim, começando com ONTAP 9.13,1. Saiba mais Suporte MAVsobre o .
SAN	Não	Não
Single-file SnapRestore	Não	Sim

Sincronização ativa do SnapMirror	Não	Não
SnapRestore	Não	Sim
SMTape	Não	Não
SnapMirror síncrono	Não	Não
SSDs	Sim, começando com ONTAP 9.1.	Sim, começando com ONTAP 9.1.
Recursos de eficiência de storage	Sim, começando com ONTAP 9.9,1. Saiba mais suporte à eficiência de storagesobre o .	Sim, começando com ONTAP 9.9,1. Saiba mais suporte à eficiência de storagesobre o .

FabricPool em agregados SnapLock Enterprise

FabricPools são compatíveis com agregados SnapLock Enterprise a partir de ONTAP 9.8. No entanto, sua equipe de conta precisa abrir uma solicitação de variação de produto, documentando que você entende que os dados do FabricPool dispostos em camadas em uma nuvem pública ou privada não são mais protegidos pelo SnapLock porque um administrador da nuvem pode excluir esses dados.

Todos os dados categorizados pelo FabricPool em uma nuvem pública ou privada não são mais protegidos pelo SnapLock porque eles podem ser excluídos por um administrador de nuvem.

Volumes FlexGroup

O SnapLock suporta volumes FlexGroup a partir do ONTAP 9.11,1; no entanto, os seguintes recursos não são suportados:

- Guarda legal
- Retenção baseada em evento
- SnapLock para SnapVault (suportado a partir do ONTAP 9.12,1)

Você também deve estar ciente dos seguintes comportamentos:

- O relógio de conformidade de volume (VCC) de um volume FlexGroup é determinado pelo VCC do componente raiz. Todos os constituintes não-raiz terão seu VCC estreitamente sincronizado com o VCC raiz.
- As propriedades de configuração do SnapLock são definidas apenas no FlexGroup como um todo. Os constituintes individuais não podem ter propriedades de configuração diferentes, como o tempo de retenção padrão e o período de confirmação automática.

Suporte LUN

Os LUNs são compatíveis com volumes SnapLock somente em cenários em que as cópias Snapshot criadas em um volume que não seja SnapLock são transferidas para um volume SnapLock para proteção como parte da relação de cofre do SnapLock. LUNs não são compatíveis com volumes SnapLock de leitura/gravação. No entanto, as cópias Snapshot à prova de violações são compatíveis com volumes de origem e volumes de destino do SnapMirror que contêm LUNs.

Suporte à MetroCluster

O suporte a SnapLock nas configurações do MetroCluster difere entre o modo SnapLock Compliance e o modo SnapLock Enterprise.

SnapLock Compliance

- A partir do ONTAP 9.3, o SnapLock Compliance é compatível com agregados MetroCluster sem espelhamento.
- A partir do ONTAP 9.3, o SnapLock Compliance é compatível com agregados espelhados, mas somente se o agregado for usado para hospedar volumes de log de auditoria do SnapLock.
- As configurações de SnapLock específicas do SVM podem ser replicadas para locais primários e secundários usando o MetroCluster.

SnapLock Enterprise

- A partir do ONTAP 9, os agregados SnapLock Enterprise são compatíveis.
- A partir do ONTAP 9.3, os agregados SnapLock Enterprise com exclusão privilegiada são suportados.
- As configurações de SnapLock específicas da SVM podem ser replicadas para ambos os locais usando o MetroCluster.

Configurações do MetroCluster e relógios de conformidade

As configurações do MetroCluster usam dois mecanismos de relógio de conformidade, o Relógio de conformidade de volume (VCC) e o Relógio de conformidade do sistema (SCC). O VCC e o SCC estão disponíveis para todas as configurações do SnapLock. Quando você cria um novo volume em um nó, seu VCC é inicializado com o valor atual do SCC nesse nó. Depois que o volume é criado, o volume e o tempo de retenção do arquivo são sempre rastreados com o VCC.

Quando um volume é replicado para outro local, seu VCC também é replicado. Quando ocorre uma mudança de volume, do local A ao local B, por exemplo, o VCC continua a ser atualizado no local B, enquanto o SCC no local A pára quando o local A fica offline.

Quando o local A é colocado de volta online e o retorno de volume é executado, o relógio do local A SCC é reiniciado enquanto o VCC do volume continua a ser atualizado. Como o VCC é atualizado continuamente, independentemente das operações de comutação e switchback, os tempos de retenção de arquivos não dependem dos relógios SCC e não se esticam.

Suporte a verificação multi-admin (MAV)

A partir do ONTAP 9.13,1, um administrador de cluster pode ativar explicitamente a verificação de vários administradores em um cluster para exigir aprovação de quorum antes de algumas operações do SnapLock serem executadas. Quando o MAV está ativado, as propriedades de volume do SnapLock, como tempo de retenção padrão, tempo de retenção mínimo, tempo de retenção máximo, modo de adição de volume, período de confirmação automática e exclusão privilegiada, exigirão aprovação de quorum. Saiba mais "MAV"sobre o .

Eficiência de storage

A partir do ONTAP 9.9,1, o SnapLock é compatível com recursos de eficiência de storage, como compactação de dados, deduplicação entre volumes e compressão adaptável para volumes e agregados SnapLock. Para obter mais informações sobre eficiência de storage, "Visão geral da eficiência de storage da ONTAP"consulte .

Criptografia

A ONTAP oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados

em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

Isenção de responsabilidade: a NetApp não pode garantir que arquivos WORM protegidos por SnapLock em unidades ou volumes de criptografia automática serão recuperáveis se a chave de autenticação for perdida ou se o número de tentativas de autenticação falhadas exceder o limite especificado e resultar em que a unidade seja permanentemente bloqueada. Você é responsável por garantir contra falhas de autenticação.

A partir do ONTAP 9.2, os volumes criptografados são compatíveis com agregados SnapLock.

Transição de 7 modos

Você pode migrar volumes SnapLock do modo 7 para o ONTAP usando o recurso transição baseada em cópia (CBT) da ferramenta de transição de modo 7D. O modo SnapLock do volume de destino, conformidade ou empresa deve corresponder ao modo SnapLock do volume de origem. Não é possível usar a transição livre de cópias (CFT) para migrar volumes do SnapLock.

Configurar o SnapLock

Configurar o SnapLock

Antes de usar o SnapLock, você precisa configurar o SnapLock executando várias tarefas, "Instale a licença SnapLock"como para cada nó que hospeda um agregado com um volume SnapLock, inicializar o "Relógio de conformidade", criar um agregado SnapLock para clusters que executam versões do ONTAP anteriores ao ONTAP 9.10,1 e "Crie e monte um volume SnapLock"muito mais.

Inicialize o Relógio de conformidade

O SnapLock usa o *volume Compliance Clock* para garantir contra adulteração que pode alterar o período de retenção de arquivos WORM. Você deve primeiro inicializar o *System ComplianceClock* em cada nó que hospeda um agregado SnapLock.

A partir do ONTAP 9.14,1, é possível inicializar ou reinicializar o Relógio de conformidade do sistema quando não houver volumes SnapLock ou nenhum volume com o bloqueio de cópia Snapshot ativado. A capacidade de reinicializar permite que os administradores de sistema redefinam o relógio de conformidade do sistema em casos em que ele pode ter sido inicializado incorretamente ou corrigir a deriva de clock no sistema. No ONTAP 9.13,1 e versões anteriores, depois de inicializar o Relógio de conformidade em um nó, você não poderá iniciá-lo novamente.

Antes de começar

Para reinicializar o Relógio de conformidade:

- Todos os nós no cluster devem estar no estado de integridade.
- Todos os volumes devem estar online.
- Nenhum volume pode estar presente na fila de recuperação.
- Nenhum volume SnapLock pode estar presente.
- Nenhum volume com bloqueio de cópia Snapshot ativado pode estar presente.

Requisitos gerais para inicializar o Relógio de conformidade:

- Você deve ser um administrador de cluster para executar esta tarefa.
- "A licença SnapLock deve ser instalada no nó".

Sobre esta tarefa

O tempo no relógio de conformidade do sistema é herdado pelo *volume Compliance Clock*, o último dos quais controla o período de retenção para arquivos WORM no volume. O volume Compliance Clock é inicializado automaticamente quando você cria um novo volume SnapLock.

> A configuração inicial do relógio de conformidade do sistema baseia-se no relógio do sistema de hardware atual. Por esse motivo, você deve verificar se a hora e o fuso horário do sistema estão corretos antes de inicializar o relógio de conformidade do sistema em cada nó. Depois de inicializar o relógio de conformidade do sistema em um nó, você não poderá iniciá-lo novamente quando os volumes SnapLock ou volumes com bloqueio ativado estiverem presentes.

Passos

Você pode usar a CLI do ONTAP para inicializar o Relógio de conformidade ou, a partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para inicializar o Relógio de conformidade.

System Manager

1. Navegue até **Cluster > Overview**.
2. Na seção **nodes**, clique em **Initialize SnapLock Compliance Clock**.
3. Para exibir a coluna **Relógio de conformidade** e verificar se o Relógio de conformidade foi inicializado, na seção **Cluster > Visão geral > nós**, clique em **Mostrar/Ocultar** e selecione **Relógio SnapLock Compliance**.

CLI

1. Inicializar o relógio de conformidade do sistema:

   `snaplock compliance-clock initialize -node` *`node_name`*

   O comando a seguir inicializa o relógio de conformidade do sistema em `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. Quando solicitado, confirme se o relógio do sistema está correto e se deseja inicializar o Relógio de conformidade:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Repita este procedimento para cada nó que hospeda um agregado SnapLock.

Ativar a ressincronização do relógio de conformidade para um sistema configurado por NTP

Pode ativar a funcionalidade de sincronização da hora do Relógio SnapLock Compliance quando um servidor NTP está configurado.

O que você vai precisar

- Esta funcionalidade está disponível apenas no nível de privilégio avançado.
- Você deve ser um administrador de cluster para executar esta tarefa.
- "A licença SnapLock deve ser instalada no nó".
- Esse recurso está disponível somente para plataformas Cloud Volumes ONTAP, ONTAP Select e VSIM.

Sobre esta tarefa

Quando o daemon de relógio seguro SnapLock deteta uma inclinação além do limite, o ONTAP usa a hora do

sistema para redefinir os relógios de conformidade do sistema e do volume. Um período de 24 horas é definido como o limite de inclinação. Isso significa que o relógio de conformidade do sistema é sincronizado com o relógio do sistema somente se o desvio tiver mais de um dia de idade.

O daemon SnapLock secure clock deteta um desvio e altera o Relógio de conformidade para a hora do sistema. Qualquer tentativa de modificar a hora do sistema para forçar o Relógio de conformidade a sincronizar com a hora do sistema falha, uma vez que o Relógio de conformidade sincroniza com a hora do sistema apenas se a hora do sistema for sincronizada com a hora NTP.

Passos

1. Ative o recurso de sincronização da hora do Relógio SnapLock Compliance quando um servidor NTP está configurado:

   `snaplock compliance-clock ntp`

   O comando a seguir habilita o recurso de sincronização da hora do relógio de conformidade do sistema:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. Quando solicitado, confirme se os servidores NTP configurados são confiáveis e se o canal de comunicação é seguro para habilitar o recurso:
3. Verifique se o recurso está ativado:

   `snaplock compliance-clock ntp show`

   O comando a seguir verifica se o recurso de sincronização da hora do relógio de conformidade do sistema está ativado:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Crie um agregado SnapLock

Use a opção volume `-snaplock-type` para especificar um tipo de volume Compliance ou Enterprise SnapLock. Para versões anteriores ao ONTAP 9.10,1, é necessário criar um agregado SnapLock separado. A partir do ONTAP 9.10,1, os volumes SnapLock e não SnapLock podem existir no mesmo agregado; portanto, você não será mais necessário criar um agregado SnapLock separado se estiver usando o ONTAP 9.10,1.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- O SnapLock "a licença deve ser instalada"no nó. Esta licença está incluída "ONTAP One"no .
- "O Relógio de conformidade no nó tem de ser inicializado".
- Se você tiver particionado os discos como "root", "d.ATA1" e "d.ata2", você deve garantir que os discos sobressalentes estejam disponíveis.

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1, agregados SnapLock e não SnapLock existentes são atualizados para dar suporte à existência de volumes SnapLock e não SnapLock. No entanto, os atributos de volume SnapLock existentes não são atualizados automaticamente. Por exemplo, os campos de compactação de dados, deduplicação entre volumes e deduplicação em segundo plano entre volumes permanecem inalterados. Os novos volumes SnapLock criados com agregados existentes têm os mesmos valores padrão que os volumes que não são SnapLock, e os valores padrão para novos volumes e agregados dependem de plataforma.

Considerações de reversão

Se você precisar reverter para uma versão do ONTAP anterior a 9.10.1, precisará mover todos os volumes SnapLock Compliance, SnapLock Enterprise e SnapLock para seus próprios agregados SnapLock.

Sobre esta tarefa

- Não é possível criar agregados de conformidade para LUNs FlexArray, mas agregados SnapLock Compliance são compatíveis com LUNs FlexArray.
- Não é possível criar agregados de conformidade com a opção SyncMirror.
- Você pode criar agregados de conformidade espelhados em uma configuração do MetroCluster somente se o agregado for usado para hospedar volumes de log de auditoria do SnapLock.

> Em uma configuração MetroCluster, o SnapLock Enterprise é compatível com agregados espelhados e sem espelhamento. O SnapLock Compliance é compatível apenas com agregados sem espelhamento.

Passos

1. Criar um agregado SnapLock:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

A página de manual do comando contém uma lista completa de opções.

O comando a seguir cria um agregado SnapLock `Compliance` nomeado `aggr1` com três discos `node1` no :

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

Criar e montar volumes SnapLock

Você precisa criar um volume SnapLock para os arquivos ou cópias Snapshot que deseja comprometer com o estado WORM. A partir do ONTAP 9.10,1, qualquer volume criado, independentemente do tipo de agregado, é criado por padrão como um volume não SnapLock. Você deve usar a `-snaplock-type` opção para criar explicitamente um volume SnapLock especificando conformidade ou empresa como o tipo SnapLock. Por padrão, o tipo SnapLock está definido como `non-snaplock`.

Antes de começar

- O agregado SnapLock deve estar online.
- Você deve "Verifique se uma licença SnapLock está instalada". Se uma licença do SnapLock não estiver instalada no nó, você deve "instale"fazê-lo. 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".
- "O Relógio de conformidade no nó tem de ser inicializado".

Sobre esta tarefa

Com as permissões de SnapLock adequadas, você pode destruir ou renomear um volume de empresa a qualquer momento. Não é possível destruir um volume de conformidade até que o período de retenção tenha decorrido. Você nunca pode renomear um volume de conformidade.

Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock. O volume do clone será do mesmo tipo de SnapLock que o volume pai.

> LUNs não são compatíveis com volumes SnapLock. Os LUNs são compatíveis com volumes SnapLock somente em cenários em que as cópias Snapshot criadas em um volume que não seja SnapLock são transferidas para um volume SnapLock para proteção como parte da relação de cofre do SnapLock. LUNs não são compatíveis com volumes SnapLock de leitura/gravação. No entanto, as cópias Snapshot à prova de violações são compatíveis com volumes de origem e volumes de destino do SnapMirror que contêm LUNs.

Execute esta tarefa usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

A partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para criar um volume SnapLock.

Passos

1. Navegue até **Storage > volumes** e clique em **Add**.
2. Na janela **Adicionar volume**, clique em **mais Opções**.
3. Introduza as novas informações de volume, incluindo o nome e o tamanho do volume.
4. Selecione **Ativar SnapLock** e escolha o tipo SnapLock, Compliance ou Enterprise.
5. Na seção **Auto-commit Files**, selecione **Modified** e insira o tempo que um arquivo deve permanecer inalterado antes que ele seja automaticamente comprometido. O valor mínimo é de 5 minutos e o valor máximo é de 10 anos.
6. Na seção **retenção de dados**, selecione o período de retenção mínimo e máximo.
7. Selecione o período de retenção padrão.
8. Clique em **Salvar**.
9. Selecione o novo volume na página **volumes** para verificar as configurações do SnapLock.

CLI

1. Criar um volume SnapLock:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Para obter uma lista completa de opções, consulte a página de manual do comando. As opções a seguir não estão disponíveis para volumes SnapLock: `-nvfail` `-atime-update` , , `-is -autobalance-eligible` `-space-mgmt-try-first` , E `vmalign`.

O comando a seguir cria um volume SnapLock `Compliance` chamado `vol1` `aggr1` On `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

Monte um volume SnapLock

É possível montar um volume SnapLock em um caminho de junção no namespace SVM para acesso de cliente nas.

O que você vai precisar

O volume SnapLock deve estar online.

Sobre esta tarefa

- É possível montar um volume SnapLock somente sob a raiz do SVM.
- Não é possível montar um volume regular sob um volume SnapLock.

Passos

1. Montar um volume SnapLock:

   volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir monta um volume SnapLock nomeado `vol1` para o caminho de junção `/sales` no `vs1` namespace:

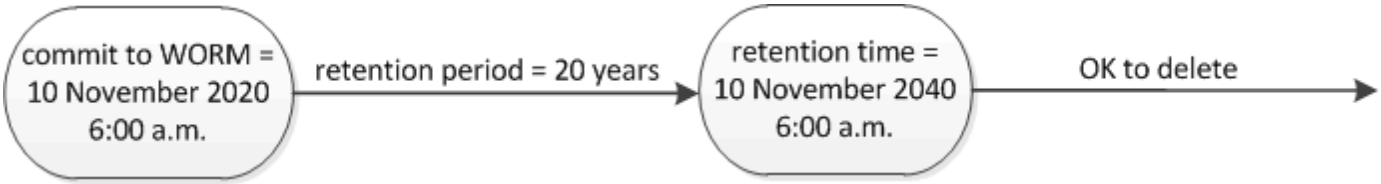
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Defina o tempo de retenção

Você pode definir o tempo de retenção de um arquivo explicitamente ou usar o período de retenção padrão para o volume para obter o tempo de retenção. A menos que você defina o tempo de retenção explicitamente, o SnapLock usará o período de retenção padrão para calcular o tempo de retenção. Você também pode definir a retenção de arquivos após um evento.

Sobre o período de retenção e o tempo de retenção

O *período de retenção* para um arquivo WORM especifica a duração do tempo em que o arquivo deve ser retido depois de ser comprometido com o estado WORM. O *tempo de retenção* para um arquivo WORM é o tempo após o qual o arquivo não precisa mais ser retido. Um período de retenção de 20 anos para um arquivo comprometido com o estado WORM em 10 de novembro de 2020 6:00, por exemplo, permitiria um tempo de retenção de 10 de novembro de 2040 6:00



> A partir do ONTAP 9.10,1, você pode definir um tempo de retenção até 26 de outubro de 3058 e um período de retenção de até 100 anos. Quando você estende as datas de retenção, as políticas mais antigas são convertidas automaticamente. No ONTAP 9.9,1 e versões anteriores, a menos que você defina o período de retenção padrão como infinito, o tempo de retenção máximo suportado é 19 2071 de janeiro (GMT).

Considerações importantes sobre replicação

Ao estabelecer uma relação SnapMirror com um volume de origem SnapLock usando uma data de retenção posterior a 19th 2071 de janeiro (GMT), o cluster de destino deve estar executando o ONTAP 9.10,1 ou posterior ou a transferência SnapMirror falhará.

Considerações importantes de reversão

O ONTAP impede que você reverta um cluster do ONTAP 9.10,1 para uma versão anterior do ONTAP quando houver arquivos com um período de retenção posterior a "19 de janeiro de 2071 8:44:07 AM".

Compreender os períodos de retenção

Um volume SnapLock Compliance ou empresa tem quatro períodos de retenção:

- Período de retenção mínimo (`min`), com um padrão de 0
- Período máximo de retenção (`max`), com um incumprimento de 30 anos
- Período de retenção padrão, com um padrão igual a `min` para o modo de conformidade e o modo Enterprise começando com ONTAP 9.10,1. Nas versões do ONTAP anteriores ao ONTAP 9.10,1, o período de retenção padrão depende do modo:
  - Para o modo de conformidade, o padrão é igual a `max`.
  - Para o modo Enterprise, o padrão é igual a `min`.
- Período de retenção não especificado.

  A partir do ONTAP 9.8, é possível definir o período de retenção de arquivos em um volume como `unspecified`, para permitir que o arquivo seja mantido até que você defina um tempo de retenção absoluto. Você pode definir um arquivo com tempo de retenção absoluto para retenção não especificada e voltar para retenção absoluta, desde que o novo tempo de retenção absoluta seja posterior ao tempo absoluto definido anteriormente.

  A partir do ONTAP 9.12,1, os arquivos WORM com o período de retenção definido como têm a garantia de ter um período de retenção definido `unspecified` para o período de retenção mínimo configurado para o volume SnapLock. Quando você altera o período de retenção de arquivos de `unspecified` para um tempo de retenção absoluto, o novo tempo de retenção especificado deve ser maior do que o tempo de retenção mínimo já definido no arquivo.

Portanto, se você não definir o tempo de retenção explicitamente antes de armazenar um arquivo em modo de conformidade no estado WORM e não modificar os padrões, o arquivo será retido por 30 anos. Da mesma forma, se você não definir o tempo de retenção explicitamente antes de armazenar um arquivo no modo Enterprise no estado WORM e não modificar os padrões, o arquivo será retido por 0 anos ou, efetivamente, não será de todo.

Defina o período de retenção padrão

Você pode usar o `volume snaplock modify` comando para definir o período de retenção padrão para arquivos em um volume SnapLock.

O que você vai precisar

O volume SnapLock deve estar online.

Sobre esta tarefa

A tabela a seguir mostra os valores possíveis para a opção período de retenção padrão:

> O período de retenção predefinido deve ser superior ou igual a (>) o período de retenção mínimo e inferior ou igual a (>) o período de retenção máximo.

Valor	Unidade	Notas
0 - 65535	segundos	
0 - 24	horas	

Valor	Unidade	Notas
0 - 365	dias	
0 - 12	meses	
0 - 100	anos	Começando com ONTAP 9.10,1. Para versões anteriores do ONTAP, o valor é 0 - 70.
máx	-	Use o período de retenção máximo.
mín	-	Use o período de retenção mínimo.
infinito	-	Guarde os arquivos para sempre.
não especificado	-	Guarde os arquivos até que um período de retenção absoluto seja definido.

Os valores e intervalos para os períodos de retenção máximo e mínimo são idênticos, exceto para `max` e `min`, que não são aplicáveis. Para obter mais informações sobre esta tarefa, "Defina a visão geral do tempo de retenção"consulte .

Você pode usar o `volume snaplock show` comando para exibir as configurações do período de retenção do volume. Para obter mais informações, consulte a página man para o comando.

Depois que um arquivo foi comprometido com o estado WORM, você pode estender, mas não reduzir o período de retenção.

Passos

1. Defina o período de retenção padrão para arquivos em um volume SnapLock:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-default -retention-period` *`default_retention_period`* `-minimum-retention-period` *`min_retention_period`* `-maximum-retention-period` *`max_retention_period`*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   Os exemplos a seguir pressupõem que os períodos de retenção mínimo e máximo não foram modificados anteriormente.

   O comando a seguir define o período de retenção padrão para um volume de conformidade ou empresa para 20 dias:

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

O comando a seguir define o período de retenção padrão para um volume de conformidade para 70 anos:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

O comando a seguir define o período de retenção padrão para um volume Enterprise para 10 anos:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Os comandos a seguir definem o período de retenção padrão para um volume Enterprise para 10 dias:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

O comando a seguir define o período de retenção padrão para um volume de conformidade como infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Defina o tempo de retenção de um arquivo explicitamente

Você pode definir o tempo de retenção de um arquivo explicitamente modificando seu último tempo de acesso. Você pode usar qualquer comando ou programa adequado em NFS ou CIFS para modificar o último tempo de acesso.

Sobre esta tarefa

Depois que um arquivo foi comprometido com WORM, você pode estender, mas não reduzir o tempo de retenção. O tempo de retenção é armazenado `atime` no campo para o arquivo.

> Não é possível definir explicitamente o tempo de retenção de um arquivo como `infinite`. Esse valor só está disponível quando você usa o período de retenção padrão para calcular o tempo de retenção.

Passos

1. Use um comando ou programa adequado para modificar a última hora de acesso para o arquivo cujo tempo de retenção você deseja definir.

   Em um shell UNIX, use o seguinte comando para definir um tempo de retenção de 21 de novembro de 2020 6:00 em um arquivo chamado `document.txt`:

```
touch -a -t 202011210600 document.txt
```

Você pode usar qualquer comando ou programa adequado para modificar a última hora de acesso no Windows.

Defina o período de retenção do arquivo após um evento

A partir do ONTAP 9.3, você pode definir quanto tempo um arquivo é retido após um evento ocorrer usando o recurso SnapLock *retenção baseada em eventos (EBR)*.

O que você vai precisar

- Você deve ser um administrador do SnapLock para executar esta tarefa.

  "Crie uma conta de administrador do SnapLock"

- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Sobre esta tarefa

A política de retenção *evento* define o período de retenção para o arquivo após o evento ocorrer. A política pode ser aplicada a um único arquivo ou a todos os arquivos em um diretório.

- Se um arquivo não for um arquivo WORM, ele será comprometido com o estado WORM durante o período de retenção definido na política.
- Se um arquivo for um arquivo WORM ou um arquivo anexado WORM, seu período de retenção será estendido pelo período de retenção definido na política.

Você pode usar um volume de modo de conformidade ou de modo empresarial.

As políticas EBR não podem ser aplicadas a ficheiros sob retenção legal.

Para uma utilização avançada, "Storage WORM em conformidade com NetApp SnapLock"consulte .

usando EBR para estender o período de retenção de arquivos WORM já existentes
O EBR é conveniente quando você deseja estender o período de retenção de arquivos WORM já existentes. Por exemplo, pode ser política da sua empresa manter os Registros W-4 de funcionários em forma não modificada por três anos após o funcionário mudar uma eleição de retenção. Outra política da empresa pode exigir que os Registros W-4 sejam mantidos por cinco anos após o término do funcionário. Nessa situação, você pode criar uma política de EBR com um período de retenção de cinco anos. Depois que o funcionário for rescindido (o "evento"), você aplicará a política EBR ao Registro W-4 do funcionário, fazendo com que seu período de retenção seja estendido. Isso geralmente será mais fácil do que estender o período de retenção manualmente, especialmente quando um grande número de arquivos está envolvido.

Passos

1. Criar uma política EBR:

   ```
   snaplock event-retention policy create -vserver SVM_name -name policy_name
   -retention-period retention_period
   ```

O comando a seguir cria a política de EBR `employee_exit vs1` com um período de retenção de dez anos:

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name
employee_exit -retention-period 10years
```

2. Aplicar uma política EBR:

snaplock event-retention apply -vserver *SVM_name* -name *policy_name* -volume *volume_name* -path *path_name*

O comando a seguir aplica a diretiva EBR `employee_exit vs1` a todos os arquivos no diretório `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name
employee_exit -volume vol1 -path /d1
```

Criar um log de auditoria

Se você estiver usando o ONTAP 9.9,1 ou anterior, primeiro você deve criar um agregado SnapLock e, em seguida, criar um log de auditoria protegido por SnapLock antes de executar uma exclusão privilegiada ou movimentação de volume SnapLock. O log de auditoria Registra a criação e exclusão de contas de administrador do SnapLock, modificações no volume de log, se a exclusão privilegiada está ativada, operações de exclusão privilegiada e operações de movimentação de volume do SnapLock.

A partir do ONTAP 9.10,1, você não cria mais um agregado SnapLock. Você deve usar a opção -SnapLock -type para "Crie explicitamente um volume SnapLock"especificando conformidade ou empresa como o tipo SnapLock.

Antes de começar

Se você estiver usando o ONTAP 9.9,1 ou anterior, será necessário ser um administrador de cluster para criar um agregado SnapLock.

Sobre esta tarefa

Não é possível excluir um log de auditoria até que o período de retenção do arquivo de log tenha decorrido. Não é possível modificar um registo de auditoria mesmo depois de decorrido o período de retenção. Isso é verdade para os modos SnapLock Compliance e Enterprise.

> No ONTAP 9.4 e anteriores, não é possível usar um volume SnapLock Enterprise para o log de auditoria. Você deve usar um volume SnapLock Compliance. No ONTAP 9.5 e posterior, você pode usar um volume SnapLock Enterprise ou um volume SnapLock Compliance para o log de auditoria. Em todos os casos, o volume do log de auditoria deve ser montado no caminho de `/snaplock_audit_log` junção . Nenhum outro volume pode usar este caminho de junção.

Você pode encontrar os logs de auditoria do SnapLock `/snaplock_log` no diretório sob a raiz do volume de log de auditoria, em subdiretórios `privdel_log` nomeados (operações de exclusão privilegiadas) e `system_log` (tudo o resto). Os nomes dos arquivos de log de auditoria contêm o carimbo de data/hora da

primeira operação registrada, facilitando a pesquisa de Registros pelo tempo aproximado em que as operações foram executadas.

- Você pode usar o `snaplock log file show` comando para exibir os arquivos de log no volume de log de auditoria.
- Você pode usar o `snaplock log file archive` comando para arquivar o arquivo de log atual e criar um novo, o que é útil nos casos em que você precisa Registrar informações de log de auditoria em um arquivo separado.

Para obter mais informações, consulte as páginas man para os comandos.

Um volume de proteção de dados não pode ser usado como um volume de log de auditoria do SnapLock.

Passos

1. Crie um agregado SnapLock.

   Crie um agregado SnapLock

2. No SVM que você deseja configurar para o log de auditoria, crie um volume SnapLock.

   Crie um volume SnapLock

3. Configure o SVM para o log de auditoria:

   `snaplock log create -vserver` *`SVM_name`* `-volume` *`snaplock_volume_name`* `-max-log -size` *`size`* `-retention-period` *`default_retention_period`*

   O período de retenção padrão mínimo para arquivos de log de auditoria é de seis meses. Se o período de retenção de um arquivo afetado for maior do que o período de retenção do log de auditoria, o período de retenção do log herdará o período de retenção do arquivo. Assim, se o período de retenção para um arquivo excluído usando exclusão privilegiada for de 10 meses, e o período de retenção do log de auditoria for de 8 meses, o período de retenção do log será estendido para 10 meses. Para obter mais informações sobre o tempo de retenção e o período de retenção padrão, "Defina o tempo de retenção"consulte .

   O comando a seguir configura-se `SVM1` para o log de auditoria usando o volume SnapLock `logVol` . O log de auditoria tem um tamanho máximo de 20 GB e é mantido por oito meses.

   ```
   SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
   20GB -retention-period 8months
   ```

4. No SVM que você configurou para o log de auditoria, monte o volume SnapLock no caminho de `/snaplock_audit_log` junção .

   Monte um volume SnapLock

Verifique as configurações do SnapLock

Use os `volume file fingerprint start` comandos e `volume file`

`fingerprint dump` para visualizar as principais informações sobre arquivos e volumes, incluindo o tipo de arquivo (normal, WORM ou WORM anexado), a data de expiração do volume e assim por diante.

Passos

1. Gerar uma impressão digital de arquivo:

   `volume file fingerprint start -vserver <SVM_name> -file <file_path>`

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   O comando gera um Session ID que você pode usar como entrada para o `volume file fingerprint dump` comando.

   > Você pode usar o `volume file fingerprint show` comando com o Session ID para monitorar o andamento da operação de impressão digital. Certifique-se de que a operação foi concluída antes de tentar exibir a impressão digital.

2. Exibir a impressão digital do arquivo:

   `volume file fingerprint dump -session-id <session_ID>`

   ```
   svm1::> volume file fingerprint dump -session-id 33619976
           Vserver:svm1
           Session-ID:33619976
           Volume:slc_vol
           Path:/vol/slc_vol/f1
           Data
   Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

   Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
   Algorithm:SHA256
           Fingerprint Scope:data-and-metadata
           Fingerprint Start Time:1460612586
           Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
           Fingerprint Version:3
           **SnapLock License:available**
           Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
           Volume MSID:2152884007
           Volume DSID:1028
           Hostname:my_host
           Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
           Volume Containing Aggregate:slc_aggr1
   ```

```
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Gerenciar arquivos WORM

Gerenciar arquivos WORM

Você pode gerenciar arquivos WORM das seguintes maneiras:

- "Armazene dados no WORM"
- "Armazene cópias Snapshot em WORM em um destino de cofre"
- "Espelhar arquivos WORM para recuperação de desastres"
- "Retenha arquivos WORM durante o litígio"
- "Exclua arquivos WORM"

Armazene dados no WORM

Você pode comprometer arquivos para WORM (uma gravação, muitas leituras) manualmente ou armazená-los automaticamente. Você também pode criar arquivos anexados WORM.

Armazene dados em WORM manualmente

Armazene um arquivo no WORM manualmente, fazendo o arquivo somente leitura. Você pode usar qualquer comando ou programa adequado sobre NFS ou CIFS para alterar o atributo de leitura e gravação de um arquivo para somente leitura. Você pode optar por enviar arquivos manualmente se quiser garantir que um aplicativo tenha terminado de gravar em um arquivo para que o arquivo não seja comprometido prematuramente ou se houver problemas de dimensionamento para o scanner de confirmação automática por causa de um grande número de volumes.

O que você vai precisar

- O arquivo que você deseja confirmar deve residir em um volume SnapLock.
- O ficheiro tem de ser gravável.

Sobre esta tarefa

O volume ComplianceClock Time é gravado `ctime` no campo do arquivo quando o comando ou programa é executado. A hora do ComplianceClock determina quando o tempo de retenção para o arquivo foi atingido.

Passos

1. Use um comando ou programa adequado para alterar o atributo de leitura e gravação de um arquivo para somente leitura.

   Em um shell UNIX, use o seguinte comando para criar um arquivo chamado `document.txt` somente leitura:

   ```
   chmod -w document.txt
   ```

   Em um shell do Windows, use o seguinte comando para criar um arquivo chamado `document.txt` somente leitura:

   ```
   attrib +r document.txt
   ```

Armazene dados no WORM automaticamente

O recurso de autocommit do SnapLock permite que você armazene arquivos no WORM automaticamente. O recurso de confirmação automática vincula um arquivo ao estado WORM em um volume SnapLock se o arquivo não for alterado durante o período de confirmação automática. O recurso de confirmação automática está desativado por padrão.

O que você vai precisar

- Os arquivos que você deseja confirmar automaticamente devem residir em um volume SnapLock.
- O volume SnapLock deve estar online.
- O volume SnapLock deve ser um volume de leitura e gravação.

O recurso de confirmação automática do SnapLock verifica todos os arquivos no volume e envia um arquivo se ele atender ao requisito de confirmação automática. Pode haver um intervalo de tempo entre quando o arquivo está pronto para o autocommit e quando ele é realmente confirmado pelo scanner de autocommit SnapLock. No entanto, o arquivo ainda está protegido de modificações e exclusão pelo sistema de arquivos assim que for elegível para autocommit.

Sobre esta tarefa

O *autocommit period* especifica o período de tempo em que os arquivos devem permanecer inalterados antes de serem autocommitidos. A alteração de um arquivo antes do término do período de confirmação automática reinicia o período de confirmação automática do arquivo.

A tabela a seguir mostra os valores possíveis para o período de confirmação automática:

Valor	Unidade	Notas
nenhum	-	O padrão.
5 - 5256000	minutos	-
1 - 87600	horas	-
1 - 3650	dias	-
1 - 120	meses	-
1 - 10	anos	-

O valor mínimo é de 5 minutos e o valor máximo é de 10 anos.

Passos

1. Arquivos AUTOCOMMIT em um volume SnapLock para WORM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-autocommit -period` *`autocommit_period`*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir autocommits os arquivos no `vol1` volume do SVM VS1, desde que os arquivos permaneçam inalterados por 5 horas:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

Crie um arquivo anexado WORM

Um arquivo anexado WORM retém os dados gravados de forma incremental, como entradas de log. Você pode usar qualquer comando ou programa adequado para criar um arquivo anexado WORM ou usar o

recurso SnapLock *volume append mode* para criar arquivos anexados WORM por padrão.

Use um comando ou programa para criar um arquivo anexado WORM

Você pode usar qualquer comando ou programa adequado em NFS ou CIFS para criar um arquivo anexado WORM. Um arquivo anexado WORM retém os dados gravados de forma incremental, como entradas de log. Os dados são anexados ao arquivo em blocos de 256 KB. À medida que cada pedaço é escrito, o pedaço anterior se torna protegido WORM. Não é possível eliminar o ficheiro até que o período de retenção tenha decorrido.

O que você vai precisar

O arquivo WORM anexado deve residir em um volume SnapLock.

Sobre esta tarefa

Os dados não precisam ser gravados sequencialmente no bloco ativo de 256 KB. Quando os dados são gravados no byte n 256KB e 1 do arquivo, o segmento anterior de 256 KB fica protegido por WORM.

Qualquer gravação não ordenada além do bloco ativo de 256 KB atual resultará na redefinição do bloco ativo de 256KB para o último deslocamento e fará com que as gravações em desvios mais antigos falhem com um erro 'Read Only File System (ROFS)'. Os desvios de gravação dependem do aplicativo cliente. Um cliente que não esteja em conformidade com a semântica de gravação de arquivo WORM append pode causar o encerramento incorreto do conteúdo de gravação. Portanto, é recomendável garantir que o cliente siga as restrições de deslocamento para gravações não ordenadas ou garantir gravações síncronas montando o sistema de arquivos no modo síncrono.

Passos

1. Use um comando ou programa adequado para criar um arquivo de comprimento zero com o tempo de retenção desejado.

   Em um shell UNIX, use o seguinte comando para definir um tempo de retenção de 21 de novembro de 2020 6:00 em um arquivo de comprimento zero chamado `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Use um comando ou programa adequado para alterar o atributo de leitura e gravação do arquivo para somente leitura.

   Em um shell UNIX, use o seguinte comando para criar um arquivo chamado `document.txt` somente leitura:

   ```
   chmod 444 document.txt
   ```

3. Use um comando ou programa adequado para alterar o atributo de leitura e gravação do arquivo de volta para gravável.

   Esta etapa não é considerada um risco de conformidade porque não há dados no arquivo.

   Em um shell UNIX, use o seguinte comando para fazer um arquivo chamado `document.txt` gravável:

```
chmod 777 document.txt
```

4. Use um comando ou programa adequado para começar a gravar dados no arquivo.

   Em um shell UNIX, use o seguinte comando para gravar dados no `document.txt`:

```
echo test data >> document.txt
```

   Altere as permissões de arquivo de volta para somente leitura quando você não precisar mais anexar dados ao arquivo.

Use o modo de adição de volume para criar arquivos anexados WORM

A partir do ONTAP 9.3, você pode usar o recurso SnapLock *volume append mode* (VAM) para criar arquivos anexados WORM por padrão. Um arquivo anexado WORM retém os dados gravados de forma incremental, como entradas de log. Os dados são anexados ao arquivo em blocos de 256 KB. À medida que cada pedaço é escrito, o pedaço anterior se torna protegido WORM. Não é possível eliminar o ficheiro até que o período de retenção tenha decorrido.

O que você vai precisar

- O arquivo WORM anexado deve residir em um volume SnapLock.
- O volume SnapLock deve estar desmontado e vazio de cópias Snapshot e arquivos criados pelo usuário.

Sobre esta tarefa

Os dados não precisam ser gravados sequencialmente no bloco ativo de 256 KB. Quando os dados são gravados no byte n 256KB e 1 do arquivo, o segmento anterior de 256 KB fica protegido por WORM.

Se você especificar um período de auto-commit para o volume, os arquivos anexados WORM que não são modificados por um período maior do que o período de auto-commit são comprometidos com WORM.

O VAM não é compatível com volumes de log de auditoria do SnapLock.

Passos

1. Ativar VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir habilita o VAM no `vol1` volume de SVM`vs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. Use um comando ou programa adequado para criar arquivos com permissões de gravação.

Por padrão, os arquivos são anexados WORM.

Armazene snapshots em WORM em um destino de cofre

Você pode usar o SnapLock for SnapVault para proteger snapshots WORM no storage secundário. Você executa todas as tarefas básicas do SnapLock no destino do Vault. O volume de destino é montado automaticamente somente leitura, portanto, não é necessário comprometer explicitamente os snapshots para WORM.

Antes de começar

- Se você quiser usar o Gerenciador do sistema para configurar o relacionamento, os clusters de origem e destino devem estar executando o ONTAP 9.15,1 ou posterior.
- No cluster de destino:
  - "Instale a licença SnapLock".
  - "Inicialize o Relógio de conformidade".
  - Se você estiver usando a CLI com uma versão do ONTAP anterior a 9.10.1, "Crie um agregado SnapLock".
- A política de proteção deve ser do tipo "Vault".
- Os agregados de origem e destino devem ser de 64 bits.
- O volume de origem não pode ser um volume SnapLock.
- Se você estiver usando a CLI do ONTAP, os volumes de origem e destino devem ser criados no "clusters com peered" e "SVMs"no .

Sobre esta tarefa

O volume de origem pode usar armazenamento NetApp ou não NetApp. Para armazenamento que não seja NetApp, você deve usar a virtualização FlexArray.

Não é possível renomear um snapshot com compromisso com o estado WORM.

Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock.

LUNs não são compatíveis com volumes SnapLock. Os LUNs são compatíveis com volumes SnapLock somente em cenários em que os snapshots criados em um volume que não seja SnapLock são transferidos para um volume SnapLock para proteção como parte da relação de cofre do SnapLock. LUNs não são compatíveis com volumes SnapLock de leitura/gravação. No entanto, snapshots à prova de violações são compatíveis com volumes de origem do SnapMirror e volumes de destino que contêm LUNs.

A partir do ONTAP 9.10,1, os volumes SnapLock e não SnapLock podem existir no mesmo agregado; portanto, você não será mais necessário criar um agregado SnapLock separado se estiver usando o ONTAP 9.10,1. Você usa a opção volume '-SnapLock-type' para especificar um tipo de volume Compliance ou Enterprise SnapLock. Nas versões do ONTAP anteriores ao ONTAP 9.10,1, o modo SnapLock, Compliance ou Enterprise é herdado do agregado. Os volumes de destino flexíveis de versão não são suportados. A definição de idioma do volume de destino tem de corresponder à definição de idioma do volume de origem.

Um volume SnapLock que é um destino do Vault tem um período de retenção padrão atribuído a ele. O valor para este período é inicialmente definido para um mínimo de 0 anos para volumes SnapLock Enterprise e um máximo de 30 anos para volumes SnapLock Compliance. Primeiro, cada snapshot do NetApp é comprometido

com esse período de retenção padrão. O período de retenção pode ser estendido mais tarde, se necessário. Para obter mais informações, "Defina a visão geral do tempo de retenção"consulte .

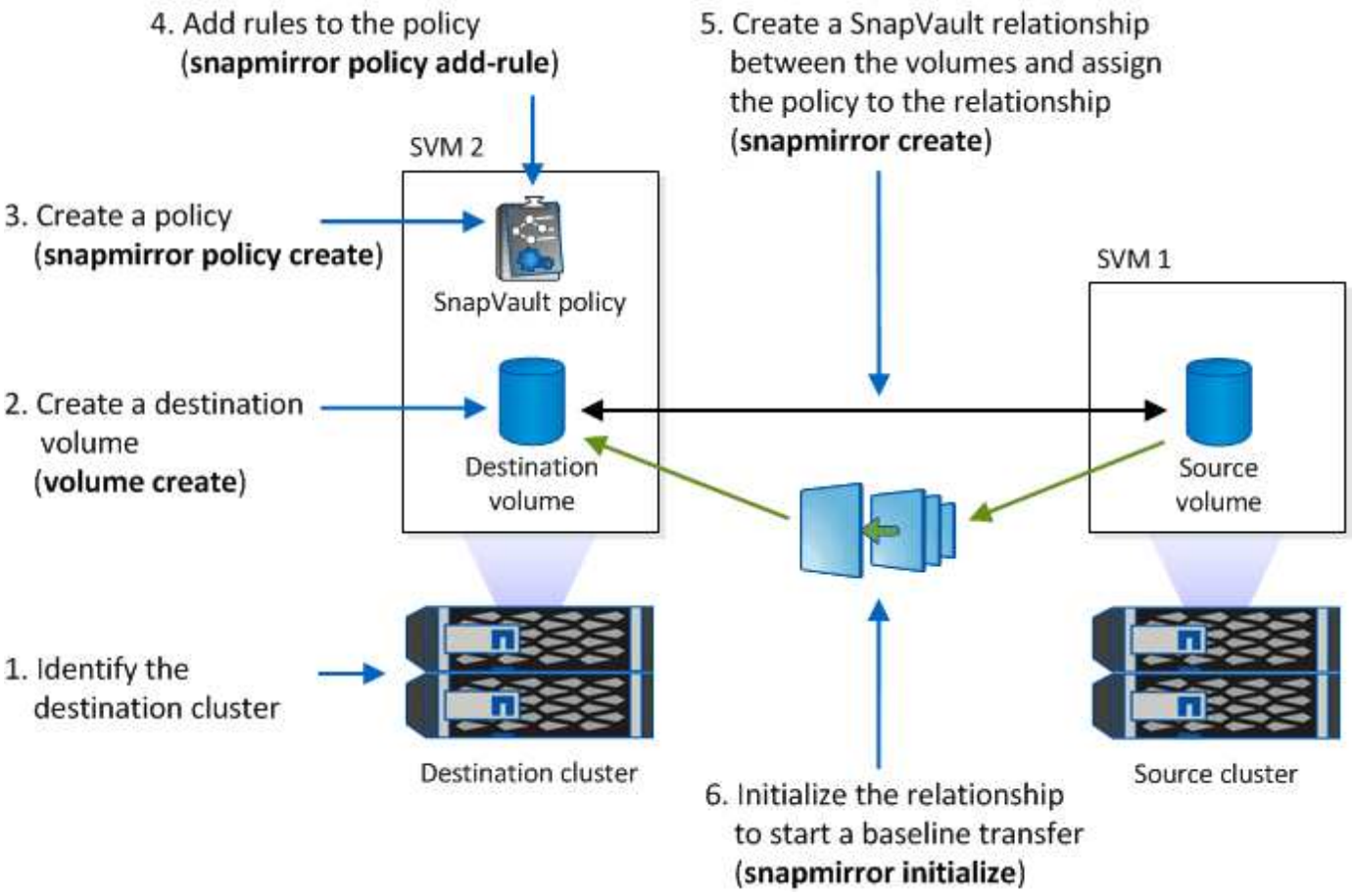
A partir do ONTAP 9.14.1, é possível especificar períodos de retenção para rótulos SnapMirror específicos na política SnapMirror da relação SnapMirror para que os snapshots replicados da origem para o volume de destino sejam retidos pelo período de retenção especificado na regra. Se nenhum período de retenção for especificado, o período de retenção padrão do volume de destino será usado.

A partir do ONTAP 9.13.1, é possível restaurar instantaneamente um instantâneo bloqueado no volume SnapLock de destino de uma relação de Vault do SnapLock criando um FlexClone com a `snaplock-type` opção definida `non-snaplock` e especificando o instantâneo como o "pai-instantâneo" ao executar a operação de criação de clone de volume. Saiba mais "Criando um volume FlexClone com um tipo SnapLock"sobre o .

Para configurações do MetroCluster, você deve estar ciente do seguinte:

- Você pode criar uma relação do SnapVault apenas entre SVMs de origem sincronizada, e não entre uma SVM de origem sincronizada e um SVM de destino sincronizado.
- Você pode criar uma relação de SnapVault a partir de um volume em uma SVM de origem sincronizada até um SVM de fornecimento de dados.
- Você pode criar uma relação de SnapVault de um volume em uma SVM de fornecimento de dados a um volume de DP em uma fonte sincronizada SVM.

A ilustração a seguir mostra o procedimento para inicializar um relacionamento de Vault do SnapLock:



Passos

Você pode usar a CLI do ONTAP para criar uma relação de cofre do SnapLock ou, a partir do ONTAP 9.15,1, você pode usar o Gerenciador do sistema para criar uma relação de cofre do SnapLock.

System Manager

1. Navegue até **Storage > volumes** e selecione **Add**.
2. Na janela **Adicionar volume**, escolha **mais opções**.
3. Introduza o nome do volume, o tamanho, a política de exportação e o nome da partilha.
4. Selecione **Bloquear instantâneos de destino para evitar a exclusão** e, na seção **método de bloqueio**, escolha **SnapLock for SnapVault**. Esta seleção não é exibida se o tipo de diretiva selecionado não for do tipo "Vault", se a licença SnapLock não estiver instalada ou se o Relógio de conformidade não for inicializado.
5. Se ainda não estiver ativado, selecione **Inicializar Relógio SnapLock Compliance**.
6. Salve suas alterações.

CLI

1. No cluster de destino, crie um volume do tipo de destino SnapLock `DP` igual ou superior ao volume de origem:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise> -type DP
   -size <size>
   ```

   O comando a seguir cria um volume 2GBD SnapLock Compliance nomeado `dstvolB` no `SVM2` agregado `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

2. No cluster de destino, "defina o período de retenção padrão".
3. "Crie uma nova relação de replicação" Entre a fonte que não é SnapLock e o novo destino SnapLock que você criou.

   Este exemplo cria uma nova relação SnapMirror com o volume SnapLock de destino `dstvolB` usando uma política de `XDPDefault` para Vault snapshots rotulados diariamente e semanalmente em uma programação por hora:

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

   > "Crie uma política de replicação personalizada" ou a "programação personalizada" se os padrões disponíveis não forem adequados.

4. No SVM de destino, inicialize a relação SnapVault criada:

   ```
   snapmirror initialize -destination-path <destination_path>
   ```

O comando a seguir inicializa a relação entre o volume de origem `srcvolA` ligado `SVM1` e o volume de destino `dstvolB` no `SVM2`:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. Depois que a relação for inicializada e ociosa, use o `snapshot show` comando no destino para verificar o tempo de expiração do SnapLock aplicado aos snapshots replicados.

   Este exemplo lista os instantâneos no volume `dstvolB` que têm o rótulo SnapMirror e a data de expiração do SnapLock:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

Informações relacionadas

"Peering de cluster e SVM"

"Backup de volume usando o SnapVault"

Espelhar arquivos WORM para recuperação de desastres

Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres e outros fins. O volume de origem e o volume de destino devem ser configurados para o SnapLock, e ambos os volumes devem ter o mesmo modo SnapLock, conformidade ou empresa. Todas as principais propriedades SnapLock do volume e dos arquivos são replicadas.

Pré-requisitos

Os volumes de origem e destino devem ser criados em clusters com SVMs com peered. Para obter mais informações, "Peering de cluster e SVM"consulte .

Sobre esta tarefa

- A partir do ONTAP 9.5, você pode replicar arquivos WORM com a relação SnapMirror do tipo XDP (proteção de dados estendida) em vez da relação de tipo DP (proteção de dados). O modo XDP é independente da versão do ONTAP e é capaz de diferenciar arquivos armazenados no mesmo bloco, facilitando a ressincronização de volumes replicados em modo de conformidade. Para obter informações sobre como converter uma relação de tipo DP existente em uma relação do tipo XDP, "Proteção de dados"consulte .
- Uma operação ressincronizada em uma relação de SnapMirror tipo DP falha para um volume de modo de conformidade se o SnapLock determinar que isso resultará em perda de dados. Se uma operação ressincronizada falhar, você pode usar o `volume clone create` comando para fazer um clone do volume de destino. Em seguida, é possível sincronizar novamente o volume de origem com o clone.
- Uma relação SnapMirror do tipo XDP entre volumes compatíveis com SnapLock suporta uma ressincronização após uma pausa, mesmo que os dados no destino tenham divergido da origem após a quebra.

Em uma ressincronização, quando a divergência de dados é detetada entre a origem do destino além do snapshot comum, um novo snapshot é cortado no destino para capturar essa divergência. O novo snapshot e o snapshot comum são bloqueados com um tempo de retenção da seguinte forma:

- O tempo de expiração do volume do destino
- Se o tempo de expiração do volume estiver no passado ou não tiver sido definido, o instantâneo será bloqueado por um período de 30 dias
- Se o destino tiver retenção legal, o período de expiração do volume real é mascarado e aparece como "indefinido"; no entanto, o instantâneo é bloqueado durante o período de expiração do volume real.

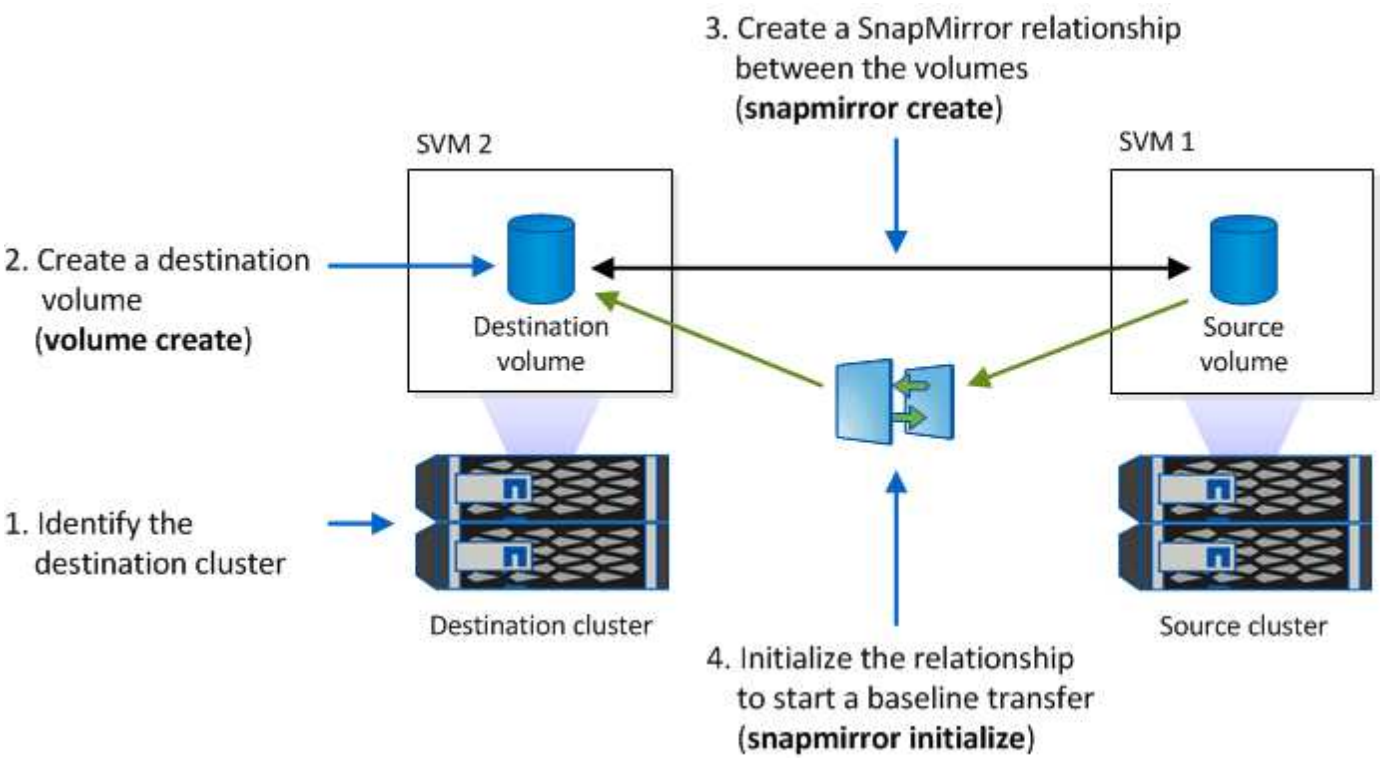
Se o volume de destino tiver um período de expiração posterior à origem, o período de expiração do destino será retido e não será substituído pelo período de expiração do volume de origem após a ressincronização.

Se o destino tiver retenções legais que diferem da origem, não é permitido fazer uma ressincronização. A origem e o destino devem ter retenção legal idêntica ou todas as retenção legal no destino devem ser liberadas antes de uma ressincronização ser tentada.

Uma cópia Snapshot bloqueada no volume de destino criada para capturar os dados divergentes pode ser copiada para a origem usando a CLI executando o `snapmirror update -s snapshot` comando. O instantâneo uma vez copiado continuará a ser bloqueado na origem também.

- As relações de proteção de dados do SVM não são compatíveis.
- Relacionamentos de proteção de dados de compartilhamento de carga não são suportados.

A ilustração a seguir mostra o procedimento para inicializar uma relação SnapMirror:



System Manager

A partir do ONTAP 9.12,1, você pode usar o System Manager para configurar a replicação do SnapMirror de arquivos WORM.

Passos

1. Navegue até **Storage > volumes**.
2. Clique em **Mostrar/Ocultar** e selecione **tipo SnapLock** para exibir a coluna na janela **volumes**.
3. Localize um volume SnapLock.
4. Clique ⋮ e selecione **Protect**.
5. Escolha o cluster de destino e a VM de armazenamento de destino.
6. Clique em **mais opções**.
7. Selecione **Mostrar políticas legadas** e selecione **DPDefault (legacy)**.
8. Na seção **Detalhes da Configuração do destino**, selecione **Substituir agendamento de transferência** e selecione **hora a hora**.
9. Clique em **Salvar**.
10. À esquerda do nome do volume de origem, clique na seta para expandir os detalhes do volume e, no lado direito da página, revise os detalhes de proteção SnapMirror remota.
11. No cluster remoto, navegue até **relacionamentos de proteção**.
12. Localize a relação e clique no nome do volume de destino para visualizar os detalhes da relação.
13. Verifique se o tipo de SnapLock do volume de destino e outras informações do SnapLock.

CLI

1. Identificar o cluster de destino.
2. No cluster de destino, "Instale a licença SnapLock" "Inicialize o Relógio de conformidade", e, se estiver a utilizar uma versão do ONTAP anterior a 9.10.1, "Crie um agregado SnapLock".
3. No cluster de destino, crie um volume de tipo de destino SnapLock `DP` com o mesmo tamanho ou maior do que o volume de origem:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > ⓘ A partir do ONTAP 9.10,1, os volumes SnapLock e não SnapLock podem existir no mesmo agregado; portanto, você não será mais necessário criar um agregado SnapLock separado se estiver usando o ONTAP 9.10,1. Você usa a opção volume -SnapLock-type para especificar um tipo de volume Compliance ou Enterprise SnapLock. Em versões do ONTAP anteriores ao ONTAP 9.10,1, o modo SnapLock --conformidade ou empresa — é herdado do agregado. Os volumes de destino flexíveis de versão não são suportados. A definição de idioma do volume de destino tem de corresponder à definição de idioma do volume de origem.

   O comando a seguir cria um volume SnapLock de 2 GB `Compliance` nomeado `dstvolB SVM2` no agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. No SVM de destino, crie uma política de SnapMirror:

   snapmirror policy create -vserver *SVM_name* -policy *policy_name*

   O comando a seguir cria a política toda a SVM `SVM1-mirror` :

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. No SVM de destino, crie um agendamento do SnapMirror:

   job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*

   O comando a seguir cria uma programação SnapMirror chamada `weekendcron`:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. No SVM de destino, crie uma relação SnapMirror:

   snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*

   O comando a seguir cria uma relação SnapMirror entre o volume de origem `srcvolA` ligado `SVM1` e o volume de destino ligado `SVM2` e `dstvolB` atribui a política `SVM1-mirror` e a programação `weekendcron`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   O tipo XDP está disponível no ONTAP 9.5 e posterior. Você deve usar o tipo DP no ONTAP 9.4 e anterior.

7. No SVM de destino, inicialize a relação SnapMirror:

   snapmirror initialize -destination-path *destination_path*

   O processo de inicialização executa uma *transferência de linha de base* para o volume de destino. O SnapMirror faz uma cópia Snapshot do volume de origem e transfere a cópia e todos os blocos de dados que ele faz referência ao volume de destino. Ele também transfere quaisquer outras cópias Snapshot no volume de origem para o volume de destino.

O comando a seguir inicializa a relação entre o volume de origem `srcvolA` ligado `SVM1` e o volume de destino `dstvolB` no `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Informações relacionadas

"Peering de cluster e SVM"

"Preparação para recuperação de desastres em volume"

"Proteção de dados"

Retenha arquivos WORM durante o litígio usando retenção legal

A partir do ONTAP 9.3, você pode reter arquivos WORM em modo de conformidade durante um litígio usando o recurso *retenção legal*.

Antes de começar

- Você deve ser um administrador do SnapLock para executar esta tarefa.

  "Crie uma conta de administrador do SnapLock"

- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Sobre esta tarefa

Um arquivo sob uma retenção legal se comporta como um arquivo WORM com um período de retenção indefinido. É da sua responsabilidade especificar quando o período de retenção Legal termina.

O número de arquivos que você pode colocar em uma retenção legal depende do espaço disponível no volume.

Passos

1. Iniciar uma retenção legal:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   O comando a seguir inicia uma retenção Legal para todos os arquivos no `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Terminar uma retenção legal:

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   O comando a seguir termina uma retenção Legal para todos os arquivos no `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Exclua a visão geral de arquivos WORM

Você pode excluir arquivos WORM do modo empresarial durante o período de retenção usando o recurso de exclusão privilegiada. Antes de poder utilizar esta funcionalidade, tem de criar uma conta de administrador do SnapLock e, em seguida, utilizar a conta, ativar a funcionalidade.

Crie uma conta de administrador do SnapLock

Você deve ter o administrador do SnapLock Privileges para executar uma exclusão privilegiada. Esses Privileges são definidos na função vsadmin-SnapLock. Se ainda não tiver sido atribuída essa função, você poderá solicitar ao administrador do cluster que crie uma conta de administrador SVM com a função de administrador do SnapLock.

O que você vai precisar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Passos

1. Crie uma conta de administrador do SVM com a função de administrador do SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   O comando a seguir permite que a conta de administrador SVM `SnapLockAdmin` com a função predefinida `vsadmin-snaplock` acesse `SVM1` usando uma senha:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

Ative o recurso de exclusão privilegiada

Você deve habilitar explicitamente o recurso de exclusão privilegiada no volume Enterprise que contém os arquivos WORM que você deseja excluir.

Sobre esta tarefa

O valor `-privileged-delete` da opção determina se a exclusão privilegiada está ativada. Os valores possíveis são `enabled`, `disabled`, e `permanently-disabled`.

> `permanently-disabled` é o estado do terminal. Não é possível ativar a exclusão privilegiada no volume depois de definir o estado como `permanently-disabled`.

Passos

1. Ativar exclusão privilegiada para um volume SnapLock Enterprise:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   O comando a seguir habilita o recurso de exclusão privilegiada para o volume Enterprise `dataVol` `SVM1` no :

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

Exclua arquivos WORM do modo empresarial

Você pode usar o recurso de exclusão privilegiada para excluir arquivos WORM do modo empresarial durante o período de retenção.

O que você vai precisar

- Você deve ser um administrador do SnapLock para executar esta tarefa.
- Você deve ter criado um log de auditoria do SnapLock e habilitado o recurso de exclusão privilegiada no volume empresa.

Sobre esta tarefa

Não é possível usar uma operação de exclusão privilegiada para excluir um arquivo WORM expirado. Use o `volume file retention show` comando para visualizar o tempo de retenção do arquivo WORM que você deseja excluir. Para obter mais informações, consulte a página man para o comando.

Passo

1. Excluir um arquivo WORM em um volume empresarial:

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   O comando a seguir exclui o arquivo `/vol/dataVol/f1` no SVM`SVM1`:

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```

Mover um volume SnapLock

A partir do ONTAP 9.8, é possível mover um volume SnapLock para um agregado de destino do mesmo tipo, seja empresa para empresa ou conformidade com a

conformidade. Você deve ter a função de segurança do SnapLock para mover um volume do SnapLock.

Crie uma conta de administrador de segurança do SnapLock

Você deve ter o administrador de segurança do SnapLock Privileges para executar uma movimentação de volume do SnapLock. Este privilégio é concedido a você com a função *SnapLock*, introduzida no ONTAP 9.8. Se ainda não tiver sido atribuída essa função, pode pedir ao administrador do cluster para criar um utilizador de segurança do SnapLock com esta função de segurança do SnapLock.

O que você vai precisar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Sobre esta tarefa

A função SnapLock está associada ao administrador SVM, diferentemente da função vsadmin-SnapLock, que é associada ao SVM de dados.

Passo

1. Crie uma conta de administrador do SVM com a função de administrador do SnapLock:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   O comando a seguir permite que a conta de administrador SVM `SnapLockAdmin` com a função predefinida `snaplock` acesse o administrador SVM `cluster1` usando uma senha:

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

Mover um volume SnapLock

Você pode usar o `volume move` comando para mover um volume SnapLock para um agregado de destino.

O que você vai precisar

- Você precisa ter criado um log de auditoria protegido pela SnapLock antes de executar a movimentação de volume do SnapLock.

  "Criar um log de auditoria".

- Se você estiver usando uma versão do ONTAP anterior à ONTAP 9.10,1, o agregado de destino deve ser o mesmo tipo de SnapLock que o volume do SnapLock que deseja mover, seja de conformidade ou de empresa para empresa. A partir do ONTAP 9.10,1, essa restrição é removida e um agregado pode incluir volumes de Compliance e Enterprise SnapLock, bem como volumes que não são SnapLock.
- Você deve ser um usuário com a função de segurança do SnapLock.

Passos

1. Usando uma conexão segura, faça login no LIF de gerenciamento de clusters do ONTAP:

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Mover um volume SnapLock:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
-aggregate destination_aggregate_name
```

3. Verificar o estado da operação de deslocação do volume:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
volume,phase,vserver
```

Bloqueie um snapshot para proteção contra ataques de ransomware

A partir do ONTAP 9.12.1, você pode bloquear um snapshot em um volume que não é SnapLock a fim de proteger contra ataques de ransomware. Bloquear instantâneos garante que eles não podem ser excluídos acidentalmente ou maliciosamente.

Você usa o recurso SnapLock Compliance clock para bloquear snapshots por um período especificado, de modo que eles não possam ser excluídos até que o tempo de expiração seja atingido. O bloqueio de snapshots torna-os invioláveis, protegendo-os contra ameaças de ransomware. Use snapshots bloqueados para recuperar dados se um volume for comprometido por um ataque de ransomware.

A partir do ONTAP 9.14.1, o bloqueio de snapshot é compatível com snapshots de retenção de longo prazo nos destinos de cofre do SnapLock e em volumes de destino que não sejam da SnapLock SnapMirror. O bloqueio de instantâneos é ativado definindo o período de retenção usando regras de política do SnapMirror associadas a um etiqueta de política existente. A regra substitui o período de retenção padrão definido no volume. Se não houver período de retenção associado ao rótulo SnapMirror, o período de retenção padrão do volume será usado.

Requisitos e considerações de snapshot à prova de violações

- Se você estiver usando a CLI do ONTAP, todos os nós do cluster devem estar executando o ONTAP 9.12,1 ou posterior. Se você estiver usando o Gerenciador de sistema, todos os nós devem estar executando o ONTAP 9.13,1 ou posterior.
- "A licença SnapLock deve ser instalada no cluster". Esta licença está incluída no "ONTAP One".
- "O relógio de conformidade no cluster deve ser inicializado".
- Quando o bloqueio de snapshot está ativado em um volume, é possível atualizar os clusters para uma versão do ONTAP posterior ao ONTAP 9.12.1. No entanto, não é possível reverter para uma versão anterior do ONTAP até que todos os snapshots bloqueados tenham atingido a data de expiração e sejam excluídos e o bloqueio de snapshot seja desativado.
- Quando um instantâneo é bloqueado, o tempo de expiração do volume é definido para o tempo de expiração do instantâneo. Se mais de um snapshot estiver bloqueado, o tempo de expiração do volume refletirá o maior tempo de expiração entre todos os snapshots.
- O período de retenção para instantâneos bloqueados tem precedência sobre a contagem de manutenção de instantâneos, o que significa que o limite de contagem de manter não é honrado se o período de retenção de instantâneos para instantâneos bloqueados não tiver expirado.
- Em um relacionamento do SnapMirror, você pode definir um período de retenção em uma regra de política de cofre de espelho e o período de retenção é aplicado para snapshots replicados no destino se o volume de destino tiver o bloqueio de snapshot ativado. O período de retenção tem precedência sobre a contagem de manutenção; por exemplo, os instantâneos que não passaram a expiração serão retidos

mesmo se a contagem de manutenção for excedida.

- Você pode renomear um instantâneo em um volume que não seja SnapLock. As operações de renomeação de snapshot no volume primário de uma relação de SnapMirror são refletidas no volume secundário somente se a política for EspelrorAllinstantâneos. Para outros tipos de diretiva, o instantâneo renomeado não é propagado durante as atualizações.
- Se você estiver usando a CLI do ONTAP, você poderá restaurar um snapshot bloqueado com o `volume snapshot restore` comando somente se o snapshot bloqueado for o mais recente. Se houver instantâneos não expirados depois do que o que está sendo restaurado, a operação de restauração de snapshot falhará.

Recursos compatíveis com snapshots à prova de violações

- "Cloud Volumes ONTAP"
- Volumes FlexGroup

  O bloqueio de snapshot é compatível com volumes FlexGroup. O bloqueio instantâneo ocorre apenas no instantâneo constituinte raiz. A exclusão do volume FlexGroup só é permitida se o tempo de expiração do componente raiz tiver passado.

- Conversão de FlexVol para FlexGroup

  Você pode converter um FlexVol volume com snapshots bloqueados em um volume FlexGroup. Os instantâneos permanecem bloqueados após a conversão.

- Assíncrono com SnapMirror

  O relógio de conformidade deve ser inicializado na origem e no destino.

- SVM DR

  O relógio de conformidade deve ser inicializado na origem e no destino.

- Clone de volume e clone de arquivo

  É possível criar clones de volume e clones de arquivos a partir de um snapshot bloqueado.

Funcionalidades não suportadas

Os seguintes recursos atualmente não são compatíveis com snapshots à prova de violações:

- Grupos de consistência
- FabricPool
- Volumes FlexCache
- SMtape
- Sincronização ativa do SnapMirror
- Regras de política do SnapMirror usando o `-schedule` parâmetro
- SnapMirror síncrono
- Mobilidade de dados SVM (usada para migrar ou realocar um SVM de um cluster de origem para um cluster de destino)

Ative o bloqueio de instantâneos ao criar um volume

A partir do ONTAP 9.12.1, é possível ativar o bloqueio de instantâneos ao criar um novo volume ou ao modificar um volume existente usando a `-snapshot-locking-enabled` opção com os `volume create` comandos e `volume modify` na CLI. A partir do ONTAP 9.13.1, você pode usar o Gerenciador do sistema para ativar o bloqueio de instantâneos.

System Manager

1. Navegue até **Storage > volumes** e selecione **Add**.
2. Na janela **Adicionar volume**, escolha **mais opções**.
3. Introduza o nome do volume, o tamanho, a política de exportação e o nome da partilha.
4. Selecione **Ativar bloqueio instantâneo**. Esta seleção não é apresentada se a licença SnapLock não estiver instalada.
5. Se ainda não estiver ativado, selecione **Inicializar Relógio SnapLock Compliance**.
6. Salve suas alterações.
7. Na janela **volumes**, selecione o volume que você atualizou e escolha **Visão geral**.
8. Verifique se **SnapLock Snapshot Locking** é exibido como **Enabled**.

CLI

1. Para criar um novo volume e habilitar o bloqueio de instantâneos, digite o seguinte comando:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-snapshot-locking -enabled true`

   O comando a seguir habilita o bloqueio instantâneo em um novo volume chamado vol1:

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
-locking-enabled true
Warning: snapshot locking is being enabled on volume “vol1” in
Vserver “vs1”. It cannot be disabled until all locked snapshots are
past their expiry time. A volume with unexpired locked snapshots
cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

Ative o bloqueio instantâneo em um volume existente

A partir do ONTAP 9.12.1, é possível ativar o bloqueio de snapshot em um volume existente usando a CLI do ONTAP. A partir do ONTAP 9.13.1, você pode usar o Gerenciador do sistema para habilitar o bloqueio instantâneo em um volume existente.

System Manager

1. Navegue até **Storage > volumes**.
2. Selecione ⋮ e escolha **Editar > volume**.
3. Na janela **Editar volume**, localize a seção Configurações de instantâneos (locais) e selecione **Ativar bloqueio instantâneo**.

   Esta seleção não é apresentada se a licença SnapLock não estiver instalada.
4. Se ainda não estiver ativado, selecione **Inicializar Relógio SnapLock Compliance**.
5. Salve suas alterações.
6. Na janela **volumes**, selecione o volume que você atualizou e escolha **Visão geral**.
7. Verifique se **SnapLock Snapshot Locking** é exibido como **Enabled**.

CLI

1. Para modificar um volume existente para habilitar o bloqueio de instantâneos, digite o seguinte comando:

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

Crie uma política de snapshot bloqueado e aplique retenção

A partir do ONTAP 9.12.1, você pode criar políticas de snapshot para aplicar um período de retenção de snapshot e aplicar a política a um volume para bloquear snapshots para o período especificado. Também é possível bloquear um instantâneo definindo manualmente um período de retenção. A partir do ONTAP 9.13.1, você pode usar o Gerenciador do sistema para criar políticas de bloqueio de snapshot e aplicá-las a um volume.

Crie uma política de bloqueio de instantâneos

System Manager

1. Navegue até **Storage > Storage VMs** e selecione uma VM de armazenamento.
2. Selecione **Definições**.
3. Localize **políticas de instantâneos** e →selecione .
4. Na janela **Add Snapshot Policy** (Adicionar política de instantâneo*), introduza o nome da política.
5. + Add Selecione .
6. Forneça os detalhes da programação do snapshot, incluindo o nome da programação, o máximo de snapshots a serem mantidos e o período de retenção do SnapLock.
7. Na coluna **período de retenção do SnapLock**, insira o número de horas, dias, meses ou anos para reter os instantâneos. Por exemplo, uma política de snapshot com um período de retenção de 5 dias bloqueia um snapshot por 5 dias a partir do momento em que é criado e não pode ser excluído durante esse período. Os seguintes intervalos de período de retenção são suportados:
   - Anos: 0 - 100
   - Meses: 0 - 1200
   - Dias: 0 - 36500
   - Horário: 0h - 24H.
8. Salve suas alterações.

CLI

1. Para criar uma política de snapshot, digite o seguinte comando:

   `volume snapshot policy create -policy policy_name -enabled true -schedule1 schedule1_name -count1 maximum_Snapshot_copies -retention-period1 _retention_period`

   O comando a seguir cria uma política de bloqueio de snapshot:

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   Um snapshot não será substituído se estiver sob retenção ativa; ou seja, a contagem de retenção não será honrada se houver snapshots bloqueados que ainda não expiraram.

Aplique uma política de bloqueio a um volume

System Manager

1. Navegue até **Storage > volumes**.
2. Selecione ⋮ e escolha **Editar > volume**.
3. Na janela **Editar volume**, selecione **Agendar instantâneos**.
4. Selecione a política de bloqueio de instantâneos a partir da lista.
5. Se o bloqueio instantâneo ainda não estiver ativado, selecione **Ativar bloqueio instantâneo**.
6. Salve suas alterações.

CLI

1. Para aplicar uma política de bloqueio de instantâneos a um volume existente, digite o seguinte comando:

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

Aplicar período de retenção durante a criação manual de instantâneos

Você pode aplicar um período de retenção de snapshot ao criar manualmente um snapshot. O bloqueio instantâneo deve estar ativado no volume; caso contrário, a definição do período de retenção é ignorada.

System Manager

1. Navegue até **Storage > volumes** e selecione um volume.
2. Na página de detalhes do volume, selecione a guia **Snapshots**.
3. + Add Selecione .
4. Introduza o nome do instantâneo e o tempo de expiração do SnapLock. Você pode selecionar o calendário para escolher a data e a hora de expiração da retenção.
5. Salve suas alterações.
6. Na página **volumes > instantâneos**, selecione **Mostrar/Ocultar** e escolha **tempo de expiração do SnapLock** para exibir a coluna **tempo de expiração do SnapLock** e verificar se o tempo de retenção está definido.

CLI

1. Para criar um instantâneo manualmente e aplicar um período de retenção de bloqueio, digite o seguinte comando:

   ```
   volume snapshot create -volume volume_name -snapshot snapshot_copy_name
   -snaplock-expiry-time expiration_date_time
   ```

   O comando a seguir cria um novo snapshot e define o período de retenção:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Aplicar período de retenção a um instantâneo existente

System Manager

1. Navegue até **Storage > volumes** e selecione um volume.
2. Na página de detalhes do volume, selecione a guia **Snapshots**.
3. Selecione o instantâneo, selecione ⋮ e escolha **Modificar tempo de expiração do SnapLock**. Você pode selecionar o calendário para escolher a data e a hora de expiração da retenção.
4. Salve suas alterações.
5. Na página **volumes > instantâneos**, selecione **Mostrar/Ocultar** e escolha **tempo de expiração do SnapLock** para exibir a coluna **tempo de expiração do SnapLock** e verificar se o tempo de retenção está definido.

CLI

1. Para aplicar manualmente um período de retenção a um instantâneo existente, digite o seguinte comando:

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   O exemplo a seguir aplica um período de retenção a um instantâneo existente:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Modificar uma política existente para aplicar retenção a longo prazo

Em um relacionamento do SnapMirror, você pode definir um período de retenção em uma regra de política de cofre de espelho e o período de retenção é aplicado para snapshots replicados no destino se o volume de destino tiver o bloqueio de snapshot ativado. O período de retenção tem precedência sobre a contagem de manutenção; por exemplo, os instantâneos que não passaram a expiração serão retidos mesmo se a contagem de manutenção for excedida.

A partir do ONTAP 9.14.1, é possível modificar uma política SnapMirror existente adicionando uma regra para definir a retenção de snapshots a longo prazo. A regra é usada para substituir o período de retenção de volume padrão nos destinos do Vault do SnapLock e em volumes de destino que não sejam do SnapLock SnapMirror.

1. Adicionar uma regra a uma política SnapMirror existente:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   O exemplo a seguir cria uma regra que aplica um período de retenção de 6 meses à política existente chamada "lockvault":

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
-label test1 -keep 10 -retention-period "6 months"
```

APIs da SnapLock

Você pode usar APIs Zephyr para integrar com a funcionalidade SnapLock em scripts ou automação de fluxo de trabalho. As APIs usam mensagens XML em HTTP, HTTPS e Windows DCE/RPC. Saiba mais no "Documentação de automação do ONTAP".

interrupção de impressão digital de ficheiros

Abortar uma operação de impressão digital do ficheiro.

file-fingerprint-dump

Exibir informações de impressão digital do arquivo.

file-fingerprint-get-iter

Exibir o status das operações de impressão digital do arquivo.

ficheiro-impressão digital-iniciar

Gerar uma impressão digital de arquivo.

SnapLock-archive-vserver-log

Arquive o arquivo de log de auditoria ativo.

SnapLock-create-vserver-log

Criar uma configuração de log de auditoria para um SVM.

SnapLock-delete-vserver-log

Excluir uma configuração de log de auditoria de um SVM.

SnapLock-file-privileged-delete

Execute uma operação de exclusão privilegiada.

retenção de arquivos-get-SnapLock

Obtenha o período de retenção de um arquivo.

SnapLock-get-node-compliance-clock

Obtenha a data e a hora do nó ComplianceClock.

SnapLock-get-vserver-ative-log-files-iter

Apresentar o estado dos ficheiros de registo ativos.

SnapLock-get-vserver-log-iter

Exibir a configuração do log de auditoria.

SnapLock-modify-vserver-log

Modificar a configuração do log de auditoria de um SVM.

retenção de arquivo-conjunto-SnapLock

Defina o tempo de retenção para um arquivo.

relógio de conformidade do nó definido por SnapLock

Defina a data e a hora do nó ComplianceClock.

SnapLock-volume-set-privileged-delete

Defina a opção de exclusão privilegiada em um volume SnapLock Enterprise.

volume-get-SnapLock-attrs

Obtenha os atributos de um volume SnapLock.

volume-set-SnapLock-attrs

Defina os atributos de um volume SnapLock.

Grupos de consistência

Visão geral dos grupos de consistência

Um grupo de consistência é uma coleção de volumes que são gerenciados como uma única unidade. No ONTAP, os grupos de consistência fornecem gerenciamento fácil e uma garantia de proteção para um workload de aplicações que abrange vários volumes.

Use grupos de consistência para simplificar o gerenciamento de storage. Imagine que você tem um banco de dados importante abrangendo vinte LUNs. Você pode gerenciar os LUNs individualmente ou tratar os LUNs como um conjunto de dados solitário, organizando-os em um único grupo de consistência.

Grupos de consistência facilitam o gerenciamento do workload de aplicações, com políticas de proteção locais e remotas facilmente configuradas e cópias Snapshot simultâneas de uma coleção de volumes em um momento consistente com falhas ou consistentes com aplicações. As cópias snapshot de um grupo de consistência permitem a restauração do workload de uma aplicação inteira.

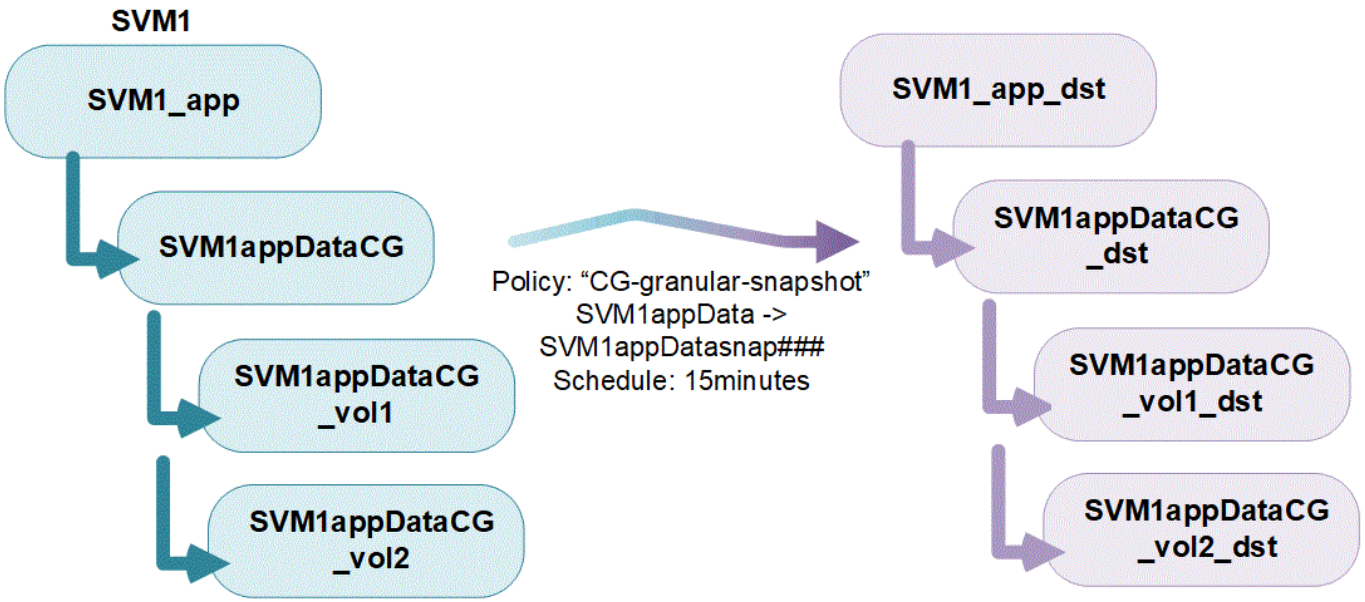
Saiba mais sobre grupos de consistência

Os grupos de consistência são compatíveis com qualquer FlexVol volume, independentemente do protocolo (nas, SAN ou NVMe) e podem ser gerenciados pela API REST do ONTAP ou no Gerenciador de sistema no

item de menu **armazenamento > grupos de consistência**. A partir do ONTAP 9.14,1, os grupos de consistência podem ser gerenciados com a CLI do ONTAP.

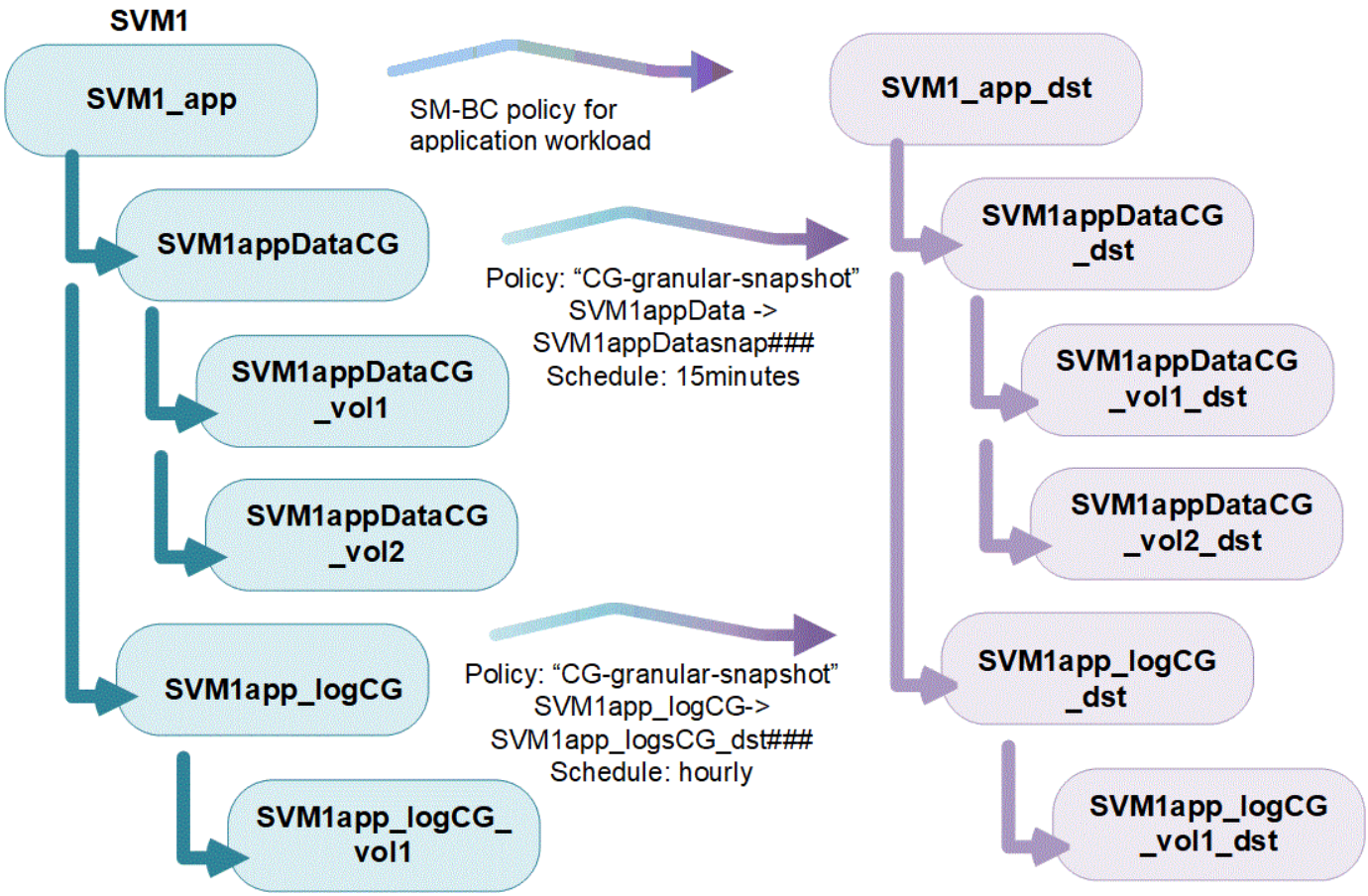
Grupos de consistência podem existir como entidades individuais - como uma coleção de volumes - ou em uma relação hierárquica, que consiste em outros grupos de consistência. Os volumes individuais podem ter sua própria política de Snapshot granular de volume. Além disso, pode haver uma política de Snapshot em todo o grupo de consistência. O grupo de consistência só pode ter uma relação de sincronização ativa do SnapMirror e uma política SnapMirror compartilhada, que pode ser usada para recuperar todo o grupo de consistência.

O diagrama a seguir ilustra como você pode usar um grupo de consistência individual. Os dados de um aplicativo hospedado em `SVM1` dois volumes: `vol1` E `vol2`. Uma política de Snapshot no grupo de consistência captura cópias Snapshot dos dados a cada 15 minutos.



Workloads de aplicações maiores podem exigir vários grupos de consistência. Nessas situações, você pode criar grupos hierárquicos de consistência, em que um único grupo de consistência se torna os componentes filhos de um grupo de consistência pai. O grupo de consistência pai pode incluir até cinco grupos filhos. Assim como em grupos de consistência individuais, uma política de proteção de sincronização ativa remota do SnapMirror pode ser aplicada a toda a configuração de grupos de consistência (pai e filhos) para recuperar a carga de trabalho do aplicativo.

No exemplo a seguir, um aplicativo é hospedado no `SVM1`. O administrador criou um grupo de consistência pai `SVM1_app` , que inclui dois grupos filhos de consistência: `SVM1appDataCG` Para os dados e `SVM1app_logCG` para os logs. Cada grupo de consistência filho tem sua própria política do Snapshot. Cópias snapshot dos volumes `SVM1appDataCG` são realizadas a cada 15 minutos. Os instantâneos de `SVM1app_logCG` são tirados por hora. O grupo de consistência pai `SVM1_app` tem uma política de sincronização ativa do SnapMirror que replica os dados para garantir a continuidade do serviço em caso de desastre.



A partir do ONTAP 9.12,1, os grupos de consistência suportam clonagem e modificam os membros da consistência no adicionar ou remover volumesGerenciador do sistema e na API REST do ONTAP. A partir do ONTAP 9.12,1, a API REST do ONTAP também suporta:

- Criação de grupos de consistência com novos volumes NFS, SMB ou namespaces NVMe.
- Adição de volumes NFS, SMB ou namespaces NVMe novos ou existentes a grupos de consistência existentes.

Para obter mais informações sobre a API REST do ONTAP, "Documentação de referência da API REST do ONTAP" consulte .

Monitorar grupos de consistência

A partir do ONTAP 9.13,1, os grupos de consistência oferecem monitoramento de capacidade e desempenho em tempo real e histórico, oferecendo insights sobre o desempenho de aplicativos e grupos de consistência individuais.

Os dados de monitoramento são atualizados a cada cinco minutos e são mantidos por até um ano. Você pode acompanhar as métricas de:

- Performance: IOPS, latência e taxa de transferência
- Capacidade: Tamanho, lógico usado, disponível

Você pode visualizar os dados de monitoramento na guia **Visão geral** do menu do grupo de consistência no System Manager ou solicitando-os na API REST. A partir do ONTAP 9.14,1, você pode visualizar métricas de grupo de consistência com a CLI usando o `consistency-group metrics show` comando.

No ONTAP 9.13,1, você só pode recuperar métricas históricas usando a API REST. A partir do ONTAP 9.14,1, métricas históricas também estão disponíveis no Gerenciador de sistemas.

Proteja grupos de consistência

Grupos de consistência oferecem proteção consistente com as aplicações, garantindo a consistência dos dados em vários volumes ou LIFs. Ao criar uma cópia Snapshot de um grupo de consistência, uma "vedação" é estabelecida no grupo de consistência. A cerca inicia uma fila para e/S até que a operação Snapshot seja concluída, garantindo consistência pontual dos dados em todas as entidades do grupo de consistência. A vedação pode causar um pico transitório na latência durante as operações de criação do Snapshot, como uma política de snapshot agendada ou criar um snapshot com o System Manager. Para obter mais informações no contexto da API REST e da CLI, consulte a documentação da API REST do ONTAP e a página de manual da CLI.

Os grupos de consistência oferecem proteção através de:

- Políticas do Snapshot
- Sincronização ativa do SnapMirror
- [mcc] (Começando com ONTAP 9.11,1)
- Assíncrono com SnapMirror (Começando com ONTAP 9.13,1)
- "Recuperação de desastres da SVM" (Começando com ONTAP 9.14,1)

Criar um grupo de consistência não ativa automaticamente a proteção. As políticas de proteção locais e remotas podem ser definidas ao criar ou depois de criar um grupo de consistência.

Para configurar a proteção em um grupo de consistência, "Proteja um grupo de consistência"consulte .

Para utilizar a proteção remota, você deve atender aos requisitos Sincronização ativa do SnapMirrordo .

As relações de sincronização ativa do SnapMirror não podem ser estabelecidas em volumes montados para acesso nas.

Suporte à verificação de vários administradores para grupos de consistência

A partir do ONTAP 9.16,1, você pode usar a verificação multi-admin (MAV) com grupos de consistência para garantir que certas operações, como criar, modificar ou excluir grupos de consistência, possam ser executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis nas configurações existentes.

"Saiba mais"

Grupos de consistência nas configurações do MetroCluster

A partir do ONTAP 9.11,1, é possível provisionar grupos de consistência com novos volumes em um cluster em uma configuração do MetroCluster. Esses volumes são provisionados em agregados espelhados.

Depois que eles forem provisionados, você poderá mover volumes associados a grupos de consistência entre agregados espelhados e sem espelhamento. Portanto, os volumes associados a grupos de consistência podem ser localizados em agregados espelhados, agregados sem espelhamento ou ambos. É possível modificar agregados espelhados que contêm volumes associados a grupos de consistência para se tornarem sem espelhamento. Da mesma forma, você pode modificar agregados sem espelhamento contendo volumes associados a grupos de consistência para habilitar o espelhamento.

Os volumes e as cópias Snapshot associadas a grupos de consistência colocados em agregados espelhados são replicados para o local remoto (local B). O conteúdo dos volumes no local B fornece uma garantia de ordem de gravação para o grupo de consistência, permitindo que você se recupere do local B em caso de desastre. Você pode acessar as cópias Snapshot do grupo de consistência usando o grupo de consistência com a API REST e o Gerenciador de sistema em clusters que executam o ONTAP 9.11,1 ou posterior. A partir do ONTAP 9.14,1, você também pode acessar cópias Snapshot com a CLI do ONTAP.

Se alguns ou todos os volumes associados a um grupo de consistência estiverem localizados em agregados sem espelhamento que não estejam atualmente acessíveis, OBTENHA ou EXCLUA operações no grupo de consistência se comportarem como se os volumes locais ou agregados de hospedagem estivessem offline.

Configurações de grupo de consistência para replicação

Se o local B estiver executando o ONTAP 9.10,1 ou anterior, somente os volumes associados aos grupos de consistência localizados em agregados espelhados serão replicados para o local B. as configurações do grupo de consistência serão replicados apenas para o local B, se ambos os sites estiverem executando o ONTAP 9.11,1 ou posterior. Após o upgrade do local B para o ONTAP 9.11,1, os dados para grupos de consistência no local A que tenham todos os volumes associados colocados em agregados espelhados são replicados para o local B.

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

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1 ou posterior, os grupos de consistência criados com o SnapMirror ative Sync (anteriormente conhecido como SnapMirror Business Continuity) no ONTAP 9.8 e 9.9.1 são atualizados automaticamente e podem ser gerenciados em **armazenamento > grupos de consistência** no Gerenciador de sistemas ou na API REST do ONTAP para obter mais informações sobre a atualização do ONTAP 9.8 ou 9,9.1, "Considerações sobre atualização e reversão da sincronização ativa do SnapMirror"consulte .

As cópias Snapshot criadas na API REST podem ser gerenciadas por meio da interface do Grupo de consistência do System Manager e pelos endpoints da API REST do grupo de consistência. A partir do ONTAP 9.14,1, snapshots de grupo de consistência também podem ser gerenciados com a CLI do ONTAP.

> Cópias snapshot criadas com os comandos ONTAPI `cg-start` e `cg-commit` não são reconhecidas como snapshots de grupo de consistência e, portanto, não podem ser gerenciadas por meio da interface de grupo de consistência do Gerenciador do sistema ou dos pontos de extremidade do grupo de consistência na API REST do ONTAP. A partir do ONTAP 9.14,1, essas cópias Snapshot podem ser espelhadas para o volume de destino se você estiver usando uma política assíncrona do SnapMirror. Para obter mais informações, Configurar o SnapMirror assíncronoconsulte .

Recursos suportados pelo lançamento

	ONTAP 9.16,1	ONTAP 9.15,1	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1	ONTAP 9.10,1
Grupos hierárquicos de consistência	✓	✓	✓	✓	✓	✓	✓
Proteção local com cópias Snapshot	✓	✓	✓	✓	✓	✓	✓
Sincronização ativa do SnapMirror	✓	✓	✓	✓	✓	✓	✓
Suporte à MetroCluster	✓	✓	✓	✓	✓	✓	
Commits de duas fases (somente API REST)	✓	✓	✓	✓	✓	✓	
Tags de aplicativos e componentes	✓	✓	✓	✓	✓		
Grupos de consistência de clones	✓	✓	✓	✓	✓		
Adicionar e remover volumes	✓	✓	✓	✓	✓		
Crie CGS com novos volumes nas	✓	✓	✓	✓	Somente API REST		
Crie CGS com novos namespaces NVMe	✓	✓	✓	✓	Somente API REST		
Mover volumes entre grupos de consistência filho	✓	✓	✓	✓			
Modifique a geometria do grupo de consistência	✓	✓	✓	✓			
Monitorização	✓	✓	✓	✓			
Verificação multi-admin	✓						
Assíncrono SnapMirror (somente grupos de consistência únicos)	✓	✓	✓	✓			
Recuperação de desastres da SVM (somente grupos de consistência únicos)	✓	✓	✓				
Suporte CLI	✓	✓	✓				

Saiba mais sobre grupos de consistência

Informações relacionadas

- "Documentação de automação do ONTAP"
- Sincronização ativa do SnapMirror
- Noções básicas de recuperação de desastres assíncrona do SnapMirror
- "Documentação do MetroCluster"
- "Verificação multi-admin"

Limites do grupo de consistência

Ao Planejar e gerenciar seus grupos de consistência, considere os limites de objetos no escopo do cluster e do grupo de consistência pai ou filho.

Limites impostos

A tabela a seguir captura limites para grupos de consistência. Limites separados se aplicam a grupos de consistência usando a sincronização ativa do SnapMirror. Para obter mais informações, "Limites de sincronização ativa do SnapMirror"consulte .

Limite	Âmbito de aplicação	Mínimo	Máximo
Número de grupos de consistência	Cluster	0	Igual à contagem máxima de volume no cluster*
Número de grupos de consistência pai	Cluster	0	Igual à contagem máxima de volume no cluster
Número de grupos de consistência individual e pai	Cluster	0	Igual à contagem máxima de volume no cluster

Número de volumes em um grupo de consistência	Grupo de consistência único	volume 1	80 volumes
Número de volumes em um grupo de consistência com o SnapMirror assíncrono	Grupo de consistência único	volume 1	• Em ONTAP 9.15,1 e posterior: 80 volumes • Em ONTAP 9.13,1 e 9.14.1: 16 volumes
Número de volumes no filho de um grupo de consistência pai	Grupo de consistência pai	volume 1	80 volumes
Número de volumes em um grupo de consistência filho	Grupo de consistência infantil	volume 1	80 volumes
Número de grupos filhos de consistência em um grupo pai de consistência	Grupo de consistência pai	1 grupo de consistência	5 grupos de consistência
Número de relacionamentos de recuperação de desastres do SVM em que existe um grupo de consistência (disponível a partir do ONTAP 9.14,1)	Cluster	0	32

Um máximo de 50 grupos de consistência habilitados com o SnapMirror assíncrono podem ser hospedados em um cluster.

Limites não aplicados

O agendamento mínimo de cópia Snapshot compatível para grupos de consistência é de 30 minutos. Isso é baseado "Teste para FlexGroups"no , que compartilha a mesma infraestrutura Snapshot que os grupos de consistência.

Configurar um único grupo de consistência

Os grupos de consistência podem ser criados com volumes existentes ou novos LUNs ou volumes (dependendo da versão do ONTAP). Um volume ou LUN só pode ser associado a um grupo de consistência de cada vez.

Sobre esta tarefa

- No ONTAP 9.10,1 a 9.11.1, a modificação dos volumes de membros de um grupo de consistência após a criação não é suportada.

  A partir do ONTAP 9.12,1, você pode modificar os volumes de membros de um grupo de consistência. Para obter mais informações sobre este processo, Modifique um grupo de consistênciaconsulte .

Crie um grupo de consistência com novos LUNs ou volumes

No ONTAP 9.10,1 a 9.12.1, você pode criar um grupo de consistência usando novos LUNs. A partir do ONTAP

9.13,1, o System Manager também dá suporte à criação de um grupo de consistência com novos namespaces NVMe ou novos volumes nas. (Isso também é suportado na API REST do ONTAP começando com ONTAP 9.12,1.)

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar * e, em seguida, selecione o protocolo para o seu objeto de armazenamento.

   No ONTAP 9.10,1 até 9.12.1, a única opção para um novo objeto de armazenamento é **usando novos LUNs**. A partir do ONTAP 9.13,1, o System Manager dá suporte à criação de grupos de consistência com novos namespaces NVMe e novos volumes nas.

3. Nomeie o grupo de consistência. Designar o número de volumes ou LUNs e a capacidade por volume ou LUN.
   a. **Tipo de aplicativo**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de aplicativo. Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se você planeja criar um grupo de consistência com uma política de proteção remota, use **Other**.
   b. Para **novos LUNs**: Selecione o sistema operacional host e o formato LUN. Insira as informações do iniciador do host.
   c. Para **novos volumes nas**: Escolha a opção de exportação apropriada (NFS ou SMB/CIFS) com base na configuração nas do SVM.
   d. Para **novos namespaces NVMe**: Selecione o sistema operacional do host e o subsistema NVMe.
4. Para configurar políticas de proteção, adicione um grupo de consistência filho ou permissões de acesso, selecione **mais opções**.
5. Selecione **Guardar**.
6. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparecerá quando o trabalho for concluído. Se você definir uma política de proteção, saberá que ela foi aplicada quando você vir um escudo verde sob olhar sob a política apropriada, remota ou local.

CLI

A partir do ONTAP 9.14,1, é possível criar um novo grupo de consistência com novos volumes usando a CLI do ONTAP. Os parâmetros específicos dependem se os volumes são SAN, NVMe ou NFS.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Criar um grupo de consistência com volumes NFS

1. Crie o grupo de consistência:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

Crie um grupo de consistência com volumes SAN

1. Crie o grupo de consistência:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

Crie um grupo de consistência com namespaces NVMe

1. Crie o grupo de consistência:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

Depois de terminar

1. Confirme que seu grupo de consistência foi criado usando o `consistency-group show` comando.

Crie um grupo de consistência com volumes existentes

Você pode usar volumes existentes para criar um grupo de consistência.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar* e depois **usando volumes existentes**.
3. Nomeie o grupo de consistência e selecione a VM de armazenamento.
   a. **Tipo de aplicativo**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de aplicativo. Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se o grupo consistência tiver uma relação de sincronização ativa do SnapMirror, você deve usar **Other**.

      Em versões do ONTAP anteriores ao ONTAP 9.15,1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror.

4. Selecione os volumes existentes a incluir. Apenas os volumes que ainda não fazem parte de um grupo de consistência estarão disponíveis para seleção.

   Se estiver criando um grupo de consistência com volumes existentes, o grupo de consistência será compatível com volumes FlexVol. Volumes com ou relacionamentos assíncronos SnapMirror ou SnapMirror podem ser adicionados a grupos de consistência, mas eles não têm reconhecimento de grupo de consistência. Os grupos de consistência não são compatíveis com buckets do S3 ou VMs de storage com relacionamentos SVMDR.

5. Selecione **Guardar**.
6. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparece quando a tarefa ONTAP for concluída. Se você escolheu uma política de proteção, confirme que ela foi corretamente definida selecionando seu grupo de consistência no menu. Se você definir uma política de proteção, sabe que ela foi aplicada quando você vê um escudo verde sob olhar sob a política apropriada, remota ou local.

CLI

A partir do ONTAP 9.14,1, é possível criar um grupo de consistência com volumes existentes usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passos

1. Emita o `consistency-group create` comando. O `-volumes` parâmetro aceita uma lista separada por vírgulas de nomes de volume.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

2. Visualize seu grupo de consistência usando o `consistency-group show` comando.

Próximas etapas

- Proteja um grupo de consistência
- Modifique um grupo de consistência
- Clonar um grupo de consistência

Configurar um grupo hierárquico de consistência

Os grupos hierárquicos de consistência permitem gerenciar grandes cargas de trabalho que abrangem vários volumes, criando um grupo de consistência pai que serve como um guarda-chuva para grupos de consistência filhos.

Os grupos hierárquicos de consistência têm um pai que pode incluir até cinco grupos de consistência individuais. Os grupos hierárquicos de consistência podem oferecer suporte a diferentes políticas de Snapshot locais em grupos de consistência ou volumes individuais. Se você usar uma política de proteção remota, isso se aplicará a todo o grupo hierárquico de consistência (pai e filhos).

Começando com ONTAP 9.13,1, você pode modifique a geometria de seus grupos de consistência e mover volumes entre grupos de consistência filho.

Para obter os limites de objetos em grupos de consistência, Limites de objetos para grupos de consistênciaconsulte .

Crie um grupo hierárquico de consistência com novos LUNs ou volumes

Ao criar um grupo de consistência hierárquica, você pode preenchê-lo com novos LUNs. A partir do ONTAP 9.13,1, você também pode usar novos namespaces NVMe e volumes nas.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar * e, em seguida, selecione o protocolo para o seu objeto de armazenamento.

   No ONTAP 9.10,1 até 9.12.1, a única opção para um novo objeto de armazenamento é **usando novos LUNs**. A partir do ONTAP 9.13,1, o System Manager dá suporte à criação de grupos de consistência com novos namespaces NVMe e novos volumes nas.

3. Nomeie o grupo de consistência. Designar o número de volumes ou LUNs e a capacidade por volume ou LUN.
   a. **Tipo de aplicativo**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de aplicativo. Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se você pretende usar uma política de proteção remota, você deve escolher **outro**.
4. Selecione o sistema operacional host e o formato LUN. Insira as informações do iniciador do host.
   a. Para **novos LUNs**: Selecione o sistema operacional host e o formato LUN. Insira as informações do iniciador do host.
   b. Para **novos volumes nas**: Escolha a opção de exportação apropriada (NFS ou SMB/CIFS) com base na configuração nas do SVM.
   c. Para **novos namespaces NVMe**: Selecione o sistema operacional do host e o subsistema NVMe.
5. Para adicionar um grupo de consistência filho, selecione **mais opções** e depois * Adicionar grupo de consistência filho*.
6. Selecione o nível de performance, o número de LUNs ou volumes e a capacidade por LUN ou volume. Designe as configurações de exportação apropriadas ou as informações do sistema operacional com base no protocolo que você está usando.
7. Opcionalmente, selecione uma política de snapshot local e defina as permissões de acesso.
8. Repita para até cinco grupos de consistência infantil.
9. Selecione **Guardar**.
10. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparecerá quando a tarefa ONTAP for concluída. Se você definir uma política de proteção, observe a política apropriada, remota ou local, que deve exibir um escudo verde com uma marca de seleção nela.

CLI

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Ao criar um grupo de consistência hierárquica na CLI com novos volumes, você deve criar cada grupo de consistência filho individualmente.

Passo

1. Crie o novo grupo de consistência usando o `consistency-group create` comando.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
   -count <number_of_volumes> -size <size>
   ```

2. Quando solicitado pela CLI, confirme que você deseja criar o novo grupo de consistência pai. Introduza `y`.
3. Opcionalmente, repita a etapa 1 para criar mais grupos de consistência filho.

Crie um grupo de consistência hierárquica com volumes existentes

Você pode organizar volumes existentes em um grupo hierárquico de consistência.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar* e depois **usando volumes existentes**.
3. Selecione a VM de armazenamento.
4. Selecione os volumes existentes a incluir. Apenas os volumes que ainda não fazem parte de um grupo de consistência estarão disponíveis para seleção.
5. Para adicionar um grupo de consistência filho, selecione * Adicionar grupo de consistência filho*. Crie os grupos de consistência necessários, que serão nomeados automaticamente.
   a. **Tipo de componente**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de componente de "dados", "logs" ou "Other". Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se você pretende usar uma política de proteção remota, você deve usar **outro**.
6. Atribua volumes existentes a cada grupo de consistência.
7. Opcionalmente, selecione uma política de instantâneo local.
8. Repita para até cinco grupos de consistência infantil.
9. Selecione **Guardar**.
10. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparecerá quando a tarefa ONTAP for concluída. Se você escolheu uma política de proteção, confirme que ela foi corretamente definida selecionando seu grupo de consistência no menu; no tipo de política apropriado, você verá um escudo verde com uma marca de seleção dentro dela.

CLI

A partir do ONTAP 9.14,1, você pode criar um grupo hierárquico de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passos

1. Provisione um novo grupo de consistência pai e atribua volumes a um novo grupo de consistência filho:

```
consistency-group create -vserver <svm_name> -consistency-group
<child_consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volumes <volume_names>
```

2. Digite `y` para confirmar que deseja criar um novo grupo de consistência pai e filho.

Próximas etapas

- Modifique a geometria de um grupo de consistência

- Modifique um grupo de consistência
- Proteja um grupo de consistência

Proteja grupos de consistência

Os grupos de consistência oferecem proteção local e remota facilmente gerenciada para aplicações SAN, nas e NVMe que abrangem vários volumes.

Criar um grupo de consistência não ativa automaticamente a proteção. As políticas de proteção podem ser definidas no momento da criação ou após a criação do seu grupo de consistência. Você pode proteger grupos de consistência usando:

- Cópias Snapshot locais
- SnapMirror ative Sync (referido como SnapMirror Business Continuity em versões do ONTAP anteriores a 9.15.1)
- MetroCluster (início de 9.11.1)
- SnapMirror assíncrono (início de 9.13.1)
- Recuperação assíncrona de desastres do SVM (início de 9.14.1)

Se você estiver utilizando grupos de consistência aninhados, poderá definir políticas de proteção diferentes para os grupos de consistência pai e filho.

Começando com ONTAP 9.11,1, grupos de consistência oferecem Criação de Snapshot do grupo de consistência em duas fases. A operação Snapshot de duas fases executa uma pré-verificação, garantindo que a cópia Snapshot seja capturada com êxito.

A recuperação pode ocorrer para um grupo inteiro de consistência, um único grupo de consistência em uma configuração hierárquica ou para volumes individuais dentro do grupo de consistência. A recuperação pode ser obtida selecionando o grupo de consistência do qual você deseja recuperar, selecionando o tipo de cópia Snapshot e identificando a cópia Snapshot para basear a restauração. Para obter mais informações sobre esse processo, "Restaurar um volume a partir de uma cópia Snapshot anterior"consulte .

Configurar uma política de instantâneo local

Definir uma política de proteção de snapshot local permite criar uma política que abrange todos os volumes em um grupo de consistência.

Sobre esta tarefa

O agendamento mínimo de cópia Snapshot compatível para grupos de consistência é de 30 minutos. Isso é baseado "Teste para FlexGroups"no , que compartilha a mesma infraestrutura Snapshot que os grupos de consistência.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que você criou no menu do grupo de consistência.
3. No canto superior direito da página de visão geral do grupo consistência, selecione **Editar**.
4. Marque a caixa ao lado de **Agendar cópias Snapshot (local)**.
5. Selecione uma política de instantâneos. Para configurar uma nova política personalizada, "Crie uma política de proteção de dados personalizada"consulte .
6. Selecione **Guardar**.
7. Regresse ao menu de visão geral do grupo de consistência. Na coluna à esquerda em **cópias Snapshot (local)**, o status dirá protegido ao lado de .

CLI

A partir do ONTAP 9.14,1, você pode modificar a política de proteção de um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passo

1. Execute o seguinte comando para definir ou modificar a política de proteção:

   Se você estiver modificando a política de proteção de uma consistência filho, será necessário identificar o grupo de consistência pai usando o `-parent-consistency-group` *`parent_consistency_group_name`* parâmetro.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Crie uma cópia Snapshot sob demanda

Se você precisar criar uma cópia Snapshot do seu grupo de consistência fora de uma política normalmente agendada, poderá criar uma sob demanda.

System Manager

Passos

1. Navegue até **armazenamento** > **grupos de consistência**.
2. Selecione o grupo de consistência para o qual você deseja criar uma cópia Snapshot sob demanda.
3. Mude para a guia **cópias Snapshot** e selecione * Adicionar*.
4. Forneça um **Nome** e um **Etiqueta SnapMirror**. No menu suspenso para **consistência**, selecione **consistente aplicação** ou **Crash consistente**.
5. Selecione **Guardar**.

CLI

A partir do ONTAP 9.14,1, você pode criar uma cópia Snapshot sob demanda de um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passo

1. Criar a cópia Snapshot:

   Por padrão, o tipo Snapshot é consistente com falhas. Você pode modificar o tipo de instantâneo com o parâmetro opcional `-type`.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Crie instantâneos de grupo de consistência em duas fases

A partir do ONTAP 9.11,1, os grupos de consistência suportam commits de duas fases para a criação de instantâneo do grupo de consistência (CG), que executam uma pré-verificação antes de confirmar a cópia Snapshot. Esse recurso só está disponível com a API REST do ONTAP.

A criação de Snapshot CG em duas fases só está disponível para a criação do Snapshot, não para provisionar grupos de consistência ou restaurar grupos de consistência.

Um CG Snapshot de duas fases divide o processo de criação de Snapshot em duas fases:

1. Na primeira fase, a API executa pré-verificações e aciona a criação do Snapshot. A primeira fase inclui um parâmetro de tempo limite, designando a quantidade de tempo para a cópia Snapshot ser confirmada com êxito.
2. Se a solicitação na primeira fase for concluída com êxito, você poderá invocar a segunda fase dentro do intervalo designado a partir da primeira fase, comprometendo a cópia Snapshot ao endpoint apropriado.

Antes de começar

- Para usar a criação de Snapshot CG em duas fases, todos os nós do cluster devem estar executando o ONTAP 9.11,1 ou posterior.

- Apenas uma invocação ativa de uma operação Snapshot de grupo de consistência é suportada em uma instância de grupo de consistência de cada vez, seja em uma fase ou em duas fases. A tentativa de invocar uma operação Snapshot enquanto outra está em andamento resulta em uma falha.
- Quando você invoca criação do Snapshot, você pode definir um valor de tempo limite opcional entre 5 e 120 segundos. Se nenhum valor de tempo limite for fornecido, o tempo de operação expira no padrão de 7 segundos. Na API, defina o valor de tempo limite com o `action_timeout` parâmetro. Na CLI, use a `-timeout` bandeira.

Passos

Você pode concluir um snapshot de duas fases com a API REST ou, a partir do ONTAP 9.14,1, a CLI do ONTAP. Esta operação não é suportada no System Manager.

Se você invocar a criação do Snapshot com a API, deverá confirmar a cópia Snapshot com a API. Se você invocar a criação do Snapshot com a CLI, deverá confirmar a cópia Snapshot com a CLI. Os métodos de mistura não são suportados.

CLI

A partir do ONTAP 9.14,1, você pode criar uma cópia Snapshot em duas fases usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passos

1. Inicie o instantâneo:

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Verifique se o instantâneo foi obtido:

   ```
   consistency-group snapshot show
   ```

3. Confirme o snapshot:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Invoque a criação do Snapshot. Envie uma SOLICITAÇÃO POST para o endpoint do grupo de consistência usando o `action=start` parâmetro.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. Se a SOLICITAÇÃO POST for bem-sucedida, a saída inclui um uuuid Snapshot. Usando esse uuid, envie uma SOLICITAÇÃO DE PATCH para confirmar a cópia Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Defina a proteção remota para um grupo de consistência

Os grupos de consistência oferecem proteção remota por meio da sincronização ativa do SnapMirror e, a partir do ONTAP 9.13,1, assíncrono do SnapMirror.

Configure a proteção com a sincronização ativa do SnapMirror

Você pode utilizar a sincronização ativa do SnapMirror para garantir que as cópias Snapshot dos grupos de consistência criados no grupo de consistência sejam copiadas para o destino. Para saber mais sobre a sincronização ativa do SnapMirror ou como configurar a sincronização ativa do SnapMirror usando a CLI, Configurar a proteção para a continuidade dos negóciosconsulte .

Antes de começar

- As relações de sincronização ativa do SnapMirror não podem ser estabelecidas em volumes montados para acesso nas.
- Os rótulos de política no cluster de origem e destino devem corresponder.
- O SnapMirror active Sync não replicará cópias Snapshot por padrão, a menos que uma regra com um rótulo SnapMirror seja adicionada à política predefinida `AutomatedFailOver` e as cópias Snapshot sejam criadas com esse rótulo.

  Para saber mais sobre este processo, "Proteja com a sincronização ativa do SnapMirror"consulte .

- Implantações em cascata Não são compatíveis com a sincronização ativa do SnapMirror.
- Começando com ONTAP 9.13,1, você pode sem interrupções adicione volumes a um grupo de consistência com uma relação de sincronização ativa do SnapMirror. Quaisquer outras alterações em um grupo de consistência exigem que você quebre a relação de sincronização ativa do SnapMirror, modifique o grupo de consistência e, em seguida, restabeleça e ressincronize a relação.

Para configurar a sincronização ativa do SnapMirror com a CLI, Proteja com a sincronização ativa do SnapMirrorconsulte .

Etapas para o System Manager

1. Certifique-se de que encontrou o "Pré-requisitos para usar a sincronização ativa do SnapMirror".
2. Selecione **armazenamento > grupos de consistência**.
3. Selecione o grupo de consistência que você criou no menu do grupo de consistência.
4. No canto superior direito da página de visão geral, selecione **mais** e depois **proteger**.

5. O System Manager preenche automaticamente as informações do lado da fonte. Selecione o cluster e a VM de armazenamento apropriados para o destino. Selecione uma política de proteção. Certifique-se de que **Initialize Relationship** está marcado.
6. Selecione **Guardar**.
7. O grupo de consistência precisa inicializar e sincronizar. Confirme se a sincronização foi concluída com êxito retornando ao menu **Grupo de consistência**. O status **SnapMirror (remoto)** é exibido `Protected` ao lado de .

Configurar o SnapMirror assíncrono

A partir do ONTAP 9.13,1, você pode configurar a proteção assíncrona do SnapMirror para um único grupo de consistência. A partir do ONTAP 9.14,1, você pode usar o assíncrono SnapMirror para replicar cópias Snapshot granular de volume para o cluster de destino usando o relacionamento de grupo de consistência.

Sobre esta tarefa

Para replicar cópias Snapshot granular de volume, você precisa executar o ONTAP 9.14,1 ou posterior. Para políticas MirrorAndVault e Vault, o rótulo SnapMirror da política de snapshot granular de volume deve corresponder à regra de política SnapMirror do grupo de consistência. Os snapshots granulares em volume cumprem o valor manter da política SnapMirror do grupo de consistência, que é calculada independentemente dos snapshots do grupo de consistência. Por exemplo, se você tiver uma política para manter duas cópias Snapshot no destino, poderá ter duas cópias Snapshot granular de volume e duas cópias Snapshot de grupo de consistência.

Ao ressincronizar a relação do SnapMirror com cópias Snapshot granular de volume, é possível preservar as cópias Snapshot granular de volume com o `-preserve` sinalizador. Cópias Snapshot granular de volume mais recentes que o grupo de consistência as cópias Snapshot são preservadas. Se não houver uma cópia Snapshot de grupo de consistência, nenhuma cópia Snapshot granular de volume poderá ser transferida para a operação ressincronizada.

Antes de começar

- A proteção assíncrona do SnapMirror está disponível apenas para um único grupo de consistência. Não é suportado para grupos hierárquicos de consistência. Para converter um grupo de consistência hierárquica em um único grupo de consistência, modifique a arquitetura do grupo de consistênciaconsulte .
- Os rótulos de política no cluster de origem e destino devem corresponder.
- Você pode sem interrupções adicione volumes a um grupo de consistência com uma relação assíncrona ativa do SnapMirror. Quaisquer outras alterações em um grupo de consistência exigem que você quebre o relacionamento SnapMirror, modifique o grupo de consistência e, em seguida, restabeleça e ressincronize o relacionamento.
- Os grupos de consistência habilitados para proteção com o SnapMirror Asynchronous têm limites diferentes. Para obter mais informações, Limites do grupo de consistênciaconsulte .
- Se você tiver configurado uma relação de proteção assíncrona do SnapMirror para vários volumes individuais, poderá converter esses volumes em um grupo de consistência e reter as cópias Snapshot existentes. Para converter volumes com sucesso:
  - Deve haver uma cópia Snapshot comum dos volumes.
  - Você deve quebrar a relação existente do SnapMirror eadicione os volumes a um único grupo de consistência, em seguida, ressincronizar a relação usando o seguinte fluxo de trabalho.

Passos

1. No cluster de destino, selecione **armazenamento > grupos de consistência**.

2. Selecione o grupo de consistência que você criou no menu do grupo de consistência.
3. No canto superior direito da página de visão geral, selecione **mais** e depois **proteger**.
4. O System Manager preenche automaticamente as informações do lado da fonte. Selecione o cluster e a VM de armazenamento apropriados para o destino. Selecione uma política de proteção. Certifique-se de que **Initialize Relationship** está marcado.

   Ao selecionar uma política assíncrona, você tem a opção de **Substituir programação de transferência**.

   > O cronograma mínimo com suporte (objetivo do ponto de restauração ou RPO) para grupos de consistência com assíncrono SnapMirror é de 30 minutos.

5. Selecione **Guardar**.
6. O grupo de consistência precisa inicializar e sincronizar. Confirme se a sincronização foi concluída com êxito retornando ao menu **Grupo de consistência**. O status **SnapMirror (remoto)** é exibido `Protected` ao lado de .

Configurar a recuperação de desastres da SVM

A partir do ONTAP 9.14,1, Recuperação de desastres da SVM suporta grupos de consistência, permitindo espelhar informações do grupo de consistência da origem para o cluster de destino.

Se você habilitar a recuperação de desastres do SVM em uma SVM que já contenha um grupo de consistência, siga os workflows de configuração do SVM System Managerpara ou o CLI do ONTAP.

Se você estiver adicionando um grupo de consistência a um SVM que esteja em uma relação de recuperação de desastres ativa e saudável da SVM, você precisará atualizar a relação de recuperação de desastres do SVM no cluster de destino. Para obter mais informações, Atualizar uma relação de replicação manualmenteconsulte . Você deve atualizar o relacionamento sempre que expandir o grupo de consistência.

Limitações

- A recuperação de desastres da SVM não dá suporte a grupos de consistência hierárquicos.
- A recuperação de desastre do SVM não dá suporte a grupos de consistência protegidos com o SnapMirror assíncrono. É necessário interromper a relação do SnapMirror antes de configurar a recuperação de desastres da SVM.
- Ambos os clusters devem estar executando o ONTAP 9.14,1 ou posterior.
- As relações de fan-out não são compatíveis com configurações de recuperação de desastres da SVM que contenham grupos de consistência.
- Para outros limites, limites do grupo de consistênciaconsulte .

Visualize relacionamentos

O System Manager visualiza mapas LUN no menu **proteção > relacionamentos**. Quando você seleciona uma relação de origem, o System Manager exibe uma visualização das relações de origem. Ao selecionar um volume, você pode aprofundar esses relacionamentos para ver uma lista dos LUNs contidos e dos relacionamentos do grupo de iniciadores. Essas informações podem ser baixadas como uma pasta de trabalho do Excel a partir da exibição de volume individual; a operação de download é executada em segundo plano.

Informações relacionadas

- "Clonar um grupo de consistência"

- "Configurar cópias Snapshot"
- "Crie políticas de proteção de dados personalizadas"
- "Recuperar de cópias Snapshot"
- "Restaurar um volume a partir de uma cópia Snapshot anterior"
- "Descrição geral da sincronização ativa do SnapMirror"
- "Documentação de automação do ONTAP"
- Noções básicas de recuperação de desastres assíncrona do SnapMirror

Modificar volumes de membros em um grupo de consistência

A partir do ONTAP 9.12,1, é possível modificar um grupo de consistência removendo volumes ou adicionando volumes (expandindo o grupo de consistência). A partir do ONTAP 9.13,1, é possível mover volumes entre grupos de consistência filho se eles compartilharem um pai comum.

Adicione volumes a um grupo de consistência

A partir do ONTAP 9.12,1, você pode adicionar volumes a um grupo de consistência sem interrupções.

Sobre esta tarefa

- Não é possível adicionar volumes associados a outro grupo de consistência.
- Os grupos de consistência são compatíveis com protocolos nas, SAN e NVMe.
- Você pode adicionar até 16 volumes de cada vez a um grupo de consistência se os ajustes estiverem dentro do limites do grupo de consistência.
- A partir do ONTAP 9.13,1, você pode adicionar volumes a um grupo de consistência sem interrupções com uma política de sincronização ativa do SnapMirror ativa ou assíncrona do SnapMirror.
- Quando você adiciona volumes a um grupo de consistência protegido pela sincronização ativa do SnapMirror, o status da relação de sincronização ativa do SnapMirror muda para "expansão" até que o espelhamento e a proteção estejam configurados para o novo volume. Se ocorrer um desastre no cluster primário antes que esse processo seja concluído, o grupo de consistência voltará à sua composição original como parte da operação de failover.
- No ONTAP 9.12,1 e anteriores, _não é possível adicionar volumes a um grupo de consistência em uma relação de sincronização ativa do SnapMirror. Primeiro, você deve excluir a relação de sincronização ativa do SnapMirror, modificar o grupo de consistência e restaurar a proteção com a sincronização ativa do SnapMirror.
- A partir do ONTAP 9.12,1, a API REST do ONTAP suporta a adição de *new* ou volumes existentes a um grupo de consistência. Para obter mais informações sobre a API REST do ONTAP, "Documentação de referência da API REST do ONTAP"consulte .

  A partir do ONTAP 9.13,1, essa funcionalidade é suportada no Gerenciador de sistemas.

- Ao expandir um grupo de consistência, as cópias Snapshot do grupo de consistência capturado antes da modificação serão consideradas parciais. Qualquer operação de restauração com base nessa cópia Snapshot refletirá o grupo de consistência no momento do snapshot.
- Se você estiver usando ONTAP 9.10,1 até 9.11.1, não poderá modificar um grupo de consistência. Para alterar a configuração de um grupo de consistência no ONTAP 9.10,1 ou 9.11.1, você deve excluir o grupo de consistência e criar um novo grupo de consistência com os volumes que deseja incluir.

- A partir do ONTAP 9.14,1, é possível replicar snapshots granular de volume para o cluster de destino usando o SnapMirror assíncrono. Ao expandir um grupo de consistência usando o SnapMirror assíncrono, os snapshots granulares de volume só são replicados depois de expandir o grupo de consistência quando a política SnapMirror é EspelrorAll ou EspelrorAndVault. Somente snapshots granulares em volume mais recentes que o grupo de consistência de linha de base Snapshot são replicados.
- Se você adicionar volumes a um grupo de consistência em uma relação de recuperação de desastres da SVM (compatível a partir de ONTAP 9.14,1), será necessário atualizar a relação de recuperação de desastres da SVM do cluster de destino após a expansão do grupo de consistência. Para obter mais informações, Atualizar uma relação de replicação manualmenteconsulte .

Exemplo 2. Passos

System Manager

A partir do ONTAP 9.12,1, você pode executar esta operação com o Gerenciador do sistema.

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja modificar.
3. Se você estiver modificando um único grupo de consistência, na parte superior do menu **volumes**, selecione **mais** e, em seguida, **expandir** para adicionar um volume.

   Se você estiver modificando um grupo de consistência filho, identifique o grupo de consistência pai que deseja modificar. Selecione o botão **>** para visualizar os grupos de consistência filho e, em seguida, selecione ⋮ ao lado do nome do grupo de consistência filho que deseja modificar. Nesse menu, selecione **expandir**.
4. Selecione até 16 volumes para adicionar ao grupo de consistência.
5. Selecione **Guardar**. Quando a operação for concluída, exiba os volumes recém-adicionados no menu **volumes** do grupo de consistência.

CLI

A partir do ONTAP 9.14,1, é possível adicionar volumes a um grupo de consistência usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Adicionar volumes existentes

1. Emita o seguinte comando. O `-volumes` parâmetro aceita uma lista de volumes separados por vírgulas.

   ⓘ Inclua o parâmetro somente `-parent-consistency-group` se o grupo de consistência estiver em uma relação hierárquica.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Adicione novos volumes

O procedimento para adicionar novos volumes depende do protocolo que está a utilizar.

ⓘ Inclua o parâmetro somente `-parent-consistency-group` se o grupo de consistência estiver em uma relação hierárquica.

- Para adicionar novos volumes sem exportá-los:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  ```

```
child_consistency_group -parent-consistency-group existingParentCg -volume
volume_name -size size
```

- Para adicionar novos volumes NFS:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- Para adicionar novos volumes SAN:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Para adicionar novos namespaces NVMe:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

Remover volumes de um grupo de consistência

Os volumes removidos de um grupo de consistência não são excluídos. Eles permanecem ativos no cluster.

Sobre esta tarefa

- Não é possível remover volumes de um grupo de consistência em uma relação de recuperação de desastres do SnapMirror active Sync ou SVM. Primeiro, você deve excluir a relação de sincronização ativa do SnapMirror para modificar o grupo de consistência e, em seguida, restabelecer a relação.
- Se um grupo de consistência não tiver volumes após a operação de remoção, o grupo de consistência será excluído.
- Quando um volume é removido de um grupo de consistência, os instantâneos existentes do grupo de consistência permanecem, mas são considerados inválidos. Os instantâneos existentes não podem ser usados para restaurar o conteúdo do grupo de consistência. Snapshots granulares em volume permanecem válidos.
- Se você excluir um volume do cluster, ele será removido automaticamente do grupo de consistência.
- Para alterar a configuração de um grupo de consistência no ONTAP 9.10,1 ou 9.11.1, você deve excluir o grupo de consistência e criar um novo grupo de consistência com os volumes de membros desejados.
- A exclusão de um volume do cluster removerá automaticamente o grupo de consistência.

System Manager

A partir do ONTAP 9.12,1, você pode executar esta operação com o Gerenciador do sistema.

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência único ou filho que deseja modificar.
3. No menu **volumes**, marque as caixas de seleção ao lado dos volumes individuais que deseja remover do grupo consistência.
4. Selecione **Remover volumes do grupo de consistência**.
5. Confirme se você entende que a remoção dos volumes fará com que todas as cópias Snapshot do grupo de consistência se tornem inválidas e selecione **Remover**.

CLI

A partir do ONTAP 9.14,1, você pode remover volumes de um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passo

1. Remova os volumes. O `-volumes` parâmetro aceita uma lista de volumes separados por vírgulas.

   Inclua o parâmetro somente `-parent-consistency-group` se o grupo de consistência estiver em uma relação hierárquica.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Mover volumes entre grupos de consistência

A partir do ONTAP 9.13,1, é possível mover volumes entre grupos de consistência filho que compartilham um pai.

Sobre esta tarefa

- Você só pode mover volumes entre grupos de consistência aninhados no mesmo grupo de consistência pai.
- Os instantâneos de grupos de consistência existentes tornam-se inválidos e não são mais acessíveis como instantâneos de grupos de consistência. Instantâneos de volume individuais permanecem válidos.
- As cópias snapshot do grupo de consistência pai permanecem válidas.
- Se você mover todos os volumes para fora de um grupo de consistência filho, esse grupo de consistência será excluído.
- As modificações a um grupo de consistência devem respeitar limites do grupo de consistênciao .

System Manager

A partir do ONTAP 9.12,1, você pode executar esta operação com o Gerenciador do sistema.

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai que contém os volumes que deseja mover. Encontre o grupo de consistência filho e expanda o menu **volumes**. Selecione os volumes que pretende mover.
3. Selecione **mover**.
4. Escolha se deseja mover os volumes para um novo grupo de consistência ou um grupo existente.
   a. Para mover para um grupo de consistência existente, selecione **grupo de consistência filho existente** e escolha o nome do grupo de consistência no menu suspenso.
   b. Para mover para um novo grupo de consistência, selecione **novo grupo de consistência filho**. Insira um nome para o novo grupo de consistência filho e selecione um tipo de componente.
5. Selecione **mover**.

CLI

A partir do ONTAP 9.14,1, é possível mover volumes entre grupos de consistência usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Mover volumes para um novo grupo de consistência filho

1. O comando a seguir cria um novo grupo de consistência filho que contém os volumes designados.

   Ao criar o novo grupo de consistência, você designará novas políticas de snapshot, QoS e disposição em camadas.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Mover volumes para um grupo de consistência filho existente

1. Reatribuir os volumes. O `-volumes` parâmetro aceita uma lista separada por vírgulas de nomes de volume.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Informações relacionadas

- Limites do grupo de consistência
- Clonar um grupo de consistência

Modifique a geometria do grupo de consistência

A partir do ONTAP 9.13,1, você pode modificar a geometria de um grupo de consistência. Modificar a geometria de um grupo de consistência permite alterar a configuração de grupos de consistência pai ou filho sem interromper as operações de e/S em andamento.

A modificação da geometria do grupo de consistência tem impacto nas cópias Snapshot existentes do grupo de consistência. Para obter detalhes, consulte a modificação específica da geometria que deseja executar.

> Não é possível modificar a geometria de um grupo de consistência configurado com uma política de proteção remota. Você deve primeiro quebrar a relação de proteção, modificar a geometria e restaurar a proteção remota.

Adicione um novo grupo de consistência filho

A partir do ONTAP 9.13,1, você pode adicionar um novo grupo de consistência filho a um grupo de consistência pai existente.

Sobre esta tarefa

- Um grupo de consistência pai pode conter no máximo cinco grupos filhos. limites do grupo de consistênciaConsulte para obter outros limites.
- Não é possível adicionar um grupo de consistência filho a um único grupo de consistência. Você deve primeiro [promover] o grupo de consistência, então você pode adicionar um grupo de consistência filho.
- Cópias Snapshot existentes do grupo de consistência capturado antes da operação de expansão serão consideradas parciais. Qualquer operação de restauração baseada nessa cópia Snapshot refletirá o grupo de consistência no momento da cópia Snapshot.

Exemplo 3. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Adicione um novo grupo de consistência filho

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai ao qual deseja adicionar um grupo de consistência filho.
3. Ao lado do nome do grupo de consistência pai, selecione **More** (mais) e depois **Add new child consistency group (Adicionar novo grupo de consistência filho)**.
4. Introduza um nome para o seu grupo de consistência.
5. Escolha se deseja adicionar volumes novos ou existentes.
   a. Se você estiver adicionando volumes existentes, selecione **volumes existentes** e escolha os volumes no menu suspenso.
   b. Se você estiver adicionando novos volumes, selecione **novos volumes** e designe o número de volumes e seu tamanho.
6. Selecione **Adicionar**.

CLI

A partir do ONTAP 9.14,1, você pode adicionar um grupo de consistência filho usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Adicione um grupo de consistência filho com novos volumes

1. Crie o novo grupo de consistência. Forneça valores para o nome do grupo de consistência, prefixo de volume, número de volumes, tamanho do volume, serviço de storage e nome da política de exportação:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Adicione um grupo de consistência filho com volumes existentes

1. Crie o novo grupo de consistência. O `volumes` parâmetro aceita uma lista separada por vírgulas de nomes de volume.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Separe um grupo de consistência infantil

A partir do ONTAP 9.13,1, você pode remover um grupo de consistência filho de seu pai, convertendo-o em um grupo de consistência individual.

Sobre esta tarefa

- Separar um grupo de consistência filho faz com que as cópias Snapshot do grupo de consistência pai se tornem inválidas e inacessíveis. As cópias Snapshot granular de volume permanecem válidas.
- As cópias Snapshot existentes do grupo de consistência individual permanecem válidas.
- Esta operação falhará se houver um único grupo de consistência existente que tenha o mesmo nome do grupo de consistência filho que você pretende separar. Se você encontrar este cenário, você deve renomear o grupo de consistência quando você o desanexar.

Exemplo 4. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Separe um grupo de consistência infantil

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai que contém o filho que você deseja desanexar.
3. Ao lado do grupo de consistência filho que você deseja desanexar, selecione **More** (mais) e depois **Detach from parent** (Desanexar do pai).
4. Opcionalmente, renomeie o grupo de consistência e selecione um tipo de aplicativo.
5. Selecione **Desanexar**.

CLI

A partir do ONTAP 9.14,1, você pode desanexar um grupo de consistência filho usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Separe um grupo de consistência infantil

1. Separe o grupo de consistência. Opcionalmente, renomeie o grupo de consistência destacada com o `-new-name` parâmetro.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Mover um único grupo de consistência existente em um grupo de consistência pai

A partir do ONTAP 9.13,1, você pode converter um único grupo de consistência existente para um grupo de consistência filho. Você pode mover o grupo de consistência em um grupo de consistência pai existente ou criar um novo grupo de consistência pai durante a operação mover.

Sobre esta tarefa

- O grupo de consistência pai deve ter quatro ou menos filhos. Um grupo de consistência pai pode conter no máximo cinco grupos filhos. limites do grupo de consistênciaConsulte para obter outros limites.
- Cópias Snapshot existentes do grupo de consistência *pai* capturadas antes dessa operação são consideradas parciais. Qualquer operação de restauração baseada em uma dessas cópias Snapshot reflete o grupo de consistência no momento da cópia Snapshot.
- As cópias Snapshot do grupo de consistência único permanecem válidas.

Exemplo 5. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Mover um único grupo de consistência existente em um grupo de consistência pai

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja converter.
3. Selecione **More** (mais) e, em seguida, **mover para o grupo de consistência diferente**.
4. Opcionalmente, insira um novo nome para o grupo de consistência e selecione um tipo de componente. Por padrão, o tipo de componente será outro.
5. Escolha se deseja migrar para um grupo de consistência pai existente ou criar um novo grupo de consistência pai:
   a. Para migrar para um grupo de consistência pai existente, selecione **grupo de consistência existente** e escolha o grupo de consistência no menu suspenso.
   b. Para criar um novo grupo de consistência pai, selecione **novo grupo de consistência** e, em seguida, forneça um nome para o novo grupo de consistência.
6. Selecione **mover**.

CLI

A partir do ONTAP 9.14,1, você pode mover um único grupo de consistência em um grupo de consistência pai usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Mover um grupo de consistência em um novo grupo de consistência pai

1. Crie o novo grupo de consistência pai. O `-consistency-groups` parâmetro migrará qualquer grupo de consistência existente para o novo pai.

   ```
   consistency-group attach -vserver svm_name -consistency-group
   parent_consistency_group -consistency-groups child_consistency_group
   ```

Mover um grupo de consistência em um grupo de consistência existente

1. Mover o grupo de consistência:

   ```
   consistency-group add -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   ```

Promover um grupo de consistência infantil

A partir do ONTAP 9.13,1, você pode promover um único grupo de consistência para um grupo de consistência pai. Quando você promove o grupo de consistência único para um pai, você também cria um novo grupo de consistência filho que herda todos os volumes no grupo de consistência original e único.

Sobre esta tarefa

- Se você quiser converter um grupo de consistência filho para um grupo de consistência pai, primeiro [detach] o grupo de consistência filho, siga este procedimento.
- As cópias Snapshot existentes do grupo de consistência permanecem válidas depois que você promover o grupo de consistência.

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Promover um grupo de consistência infantil

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja promover.
3. Selecione **mais** e depois **promover para o grupo de consistência pai**.
4. Digite um **Nome** e selecione um **tipo de componente** para o grupo de consistência filho.
5. Selecione **promover**.

CLI

A partir do ONTAP 9.14,1, você pode mover um único grupo de consistência em um grupo de consistência pai usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Promover um grupo de consistência infantil

1. Promover o grupo de consistência. Este comando criará um grupo de consistência pai e um filho.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

Demote um pai para um único grupo de consistência

A partir do ONTAP 9.13,1, você pode rebaixar um grupo de consistência pai para um único grupo de consistência. A rebaixamento do pai achata a hierarquia do grupo de consistência, removendo todos os grupos de consistência filho associados. Todos os volumes no grupo consistência permanecerão sob o novo grupo de consistência única.

Sobre esta tarefa

- As cópias Snapshot existentes do grupo de consistência *pai* permanecem válidas depois de rebaixá-lo para uma única consistência. Cópias Snapshot existentes de qualquer um dos grupos de consistência *filho* associados desse pai se tornam inválidas ao serem rebaixadas. As cópias Snapshot de volume individual dentro do grupo de consistência filho continuam acessíveis como cópias Snapshot granular de volume.

Exemplo 6. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Demote um grupo de consistência

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai que deseja rebaixar.
3. Selecione **mais** e depois **demote para um único grupo de consistência**.
4. Um aviso irá informá-lo de que todos os grupos de consistência filho associados serão eliminados e os seus volumes serão movidos para o novo grupo de consistência único. Selecione **demote** para confirmar que compreende o impactos.

CLI

A partir do ONTAP 9.14,1, você pode rebaixar um grupo de consistência usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Demote um grupo de consistência

1. Demote o grupo de consistência. Use o parâmetro opcional `-new-name` para renomear o grupo de consistência.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Modificar tags de aplicativo e componente

A partir do ONTAP 9.12,1, os grupos de consistência suportam a marcação de componentes e aplicativos. Tags de aplicativo e componente são uma ferramenta de gerenciamento, permitindo filtrar e identificar diferentes cargas de trabalho em seus grupos de consistência.

Sobre esta tarefa

Grupos de consistência oferecem dois tipos de tags:

- **Etiquetas de aplicação**: Aplicam-se a grupos de consistência individuais e pai. As tags de aplicação fornecem rotulagem para workloads como MongoDB, Oracle ou SQL Server. A tag padrão do aplicativo para grupos de consistência é outra.
- **Tags de componente**: Crianças em grupos de consistência hierárquica têm tags de componente em vez de tags de aplicativo. As opções para tags de componentes são "dados", "logs" ou "outros". O valor padrão é outro.

Você pode aplicar tags ao criar grupos de consistência ou após os grupos de consistência terem sido criados.

Se o grupo de consistência tiver uma relação de sincronização ativa do SnapMirror, você deve usar **Other** como a tag de aplicativo ou componente.

Passos

A partir do ONTAP 9.12,1, você pode modificar tags de aplicativos e componentes usando o Gerenciador de sistema. A partir do ONTAP 9.14,1, você pode modificar as tags de aplicativo e componente usando a CLI do ONTAP.

System Manager

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência cuja tag você deseja modificar. Selecione o ⋮ ao lado do nome do grupo de consistência e depois **Editar**.
3. No menu suspenso, escolha a aplicação ou a etiqueta de componente apropriada.
4. Selecione **Guardar**.

CLI

A partir do ONTAP 9.14,1, você pode modificar a tag de aplicativo ou componente de um grupo de consistência existente usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Modifique a etiqueta da aplicação

1. As etiquetas de aplicação aceitam um número limitado de strings predefinidas. Para ver a lista aceita de strings, execute o seguinte comando:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Escolha a cadeia de carateres apropriada da saída, o grupo modificar a consistência:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Modifique a etiqueta do componente

1. Modificar o tipo de componente. O tipo de componente pode ser dados, logs ou outro. Se você estiver usando a sincronização ativa do SnapMirror, ela deve ser "outra".
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Clonar um grupo de consistência

A partir do ONTAP 9.12,1, você pode clonar um grupo de consistência para criar uma cópia de um grupo de consistência e seu conteúdo. Clonar um grupo de consistência cria uma cópia da configuração do grupo de consistência, seus metadados, como tipo de aplicação, e todos os volumes e seu conteúdo, como arquivos, diretórios, LUNs ou

namespaces NVMe.

Sobre esta tarefa

Ao clonar um grupo de consistência, é possível cloná-lo com a configuração atual, mas com conteúdo de volume tal como ele está ou baseado em um grupo de consistência Snapshot existente.

Clonar um grupo de consistência é compatível apenas para todo o grupo de consistência. Você não pode clonar um grupo de consistência filho individual em uma relação hierárquica: Somente a configuração completa do grupo de consistência pode ser clonada.

Ao clonar um grupo de consistência, os seguintes componentes não são clonados:

- IGroups
- Mapas LUN
- Subsistemas NVMe
- Mapas de subsistema de namespace NVMe

Antes de começar

- Ao clonar um grupo de consistência, o ONTAP não criará compartilhamentos SMB para os volumes clonados se um nome de compartilhamento não for especificado. * Grupos de consistência clonados não são montados se um caminho de junção não for especificado.
- Se você tentar clonar um grupo de consistência com base em um instantâneo que não reflita os volumes constituintes atuais do grupo de consistência, a operação falhará.
- Depois de clonar um grupo de consistência, você precisa executar a operação de mapeamento apropriada.

  Mapeie grupos para vários LUNsConsulte ou Mapear um namespace NVMe para um subsistema para obter mais informações.

- Clonar um grupo de consistência não é compatível para um grupo de consistência em uma relação de sincronização ativa do SnapMirror ou com quaisquer volumes DP associados.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja clonar no menu **Grupo de consistência**.
3. No canto superior direito da página de visão geral do grupo consistência, selecione **Clone**.
4. Insira um nome para o novo grupo de consistência clonada ou aceite o nome padrão.
   a. Selecione se deseja ativar "**Provisionamento fino**"o .
   b. Escolha **Split Clone** se você quiser dissociar o grupo de consistência de sua origem e alocar espaço em disco adicional para o grupo de consistência clonada.
5. Para clonar o grupo de consistência em seu estado atual, escolha **Adicionar uma nova cópia Snapshot**.

   Para clonar o grupo de consistência com base em um snapshot, escolha **usar uma cópia Snapshot existente**. Selecionar esta opção irá abrir um novo submenu. Escolha o Snapshot que você deseja usar como base para a operação de clone.
6. Selecione **Clone**.
7. Retorne ao menu **Grupo de consistência** para confirmar que seu grupo de consistência foi clonado.

CLI

A partir do ONTAP 9.14,1, você pode clonar um grupo de consistência usando a CLI com credenciais de administrador do cluster.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Clonar um grupo de consistência

1. O `consistency-group clone create` comando clona o grupo de consistência em seu status de ponto no tempo atual. Para basear a operação de clone em um Snapshot, inclua o `-source -snapshot` parâmetro.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

Próximas etapas

- Mapeie grupos para vários LUNs
- Mapear um namespace NVMe para um subsistema

Excluir um grupo de consistência

Se você decidir que não precisa mais de um grupo de consistência, você pode excluí-lo.

Sobre esta tarefa

- A exclusão de um grupo de consistência exclui a instância do grupo de consistência e *não* afeta os volumes constituintes ou LUNs. A exclusão de um grupo de consistência não resulta na exclusão dos instantâneos presentes em cada volume, mas eles não estarão mais acessíveis como instantâneos de grupo de consistência. No entanto, os snapshots podem continuar sendo gerenciados como snapshots granulares de volume comuns.
- O ONTAP exclui automaticamente um grupo de consistência se todos os volumes no grupo de consistência forem excluídos.
- A exclusão de um grupo de consistência pai resulta na exclusão de todos os grupos de consistência filho associados.
- Se você estiver usando uma versão do ONTAP entre 9.10.1 e 9.12.0, os volumes só poderão ser removidos de um grupo de consistência se o volume em si for excluído, caso em que o volume é removido automaticamente do grupo de consistência. A partir do ONTAP 9.12,1, você pode remover volumes de um grupo de consistência sem excluir o grupo de consistência. Para obter mais informações sobre este processo, Modifique um grupo de consistênciaconsulte .

Exemplo 7. Passos

System Manager

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja excluir.
3. Ao lado do nome do grupo consistência, selecione **Excluir**.

CLI

A partir do ONTAP 9.14,1, você pode excluir um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Excluir um grupo de consistência

1. Excluir o grupo de consistência:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

Sincronização ativa do SnapMirror

Introdução

Descrição geral da sincronização ativa do SnapMirror

O SnapMirror ative Sync (também conhecido como SnapMirror Business Continuity *[SM-BC]*) permite que os serviços de negócios continuem operando mesmo com uma falha completa do local, dando suporte ao failover de aplicações de forma transparente

usando uma cópia secundária. Não há necessidade de intervenção manual ou script personalizado para acionar um failover com a sincronização ativa do SnapMirror.

Disponível a partir do ONTAP 9.9,1, a sincronização ativa do SnapMirror é compatível com clusters AFF, clusters All-Flash SAN Array (ASA) e C-Series (AFF ou ASA). Os clusters primário e secundário devem ser do mesmo tipo: ASA ou AFF. A sincronização ativa do SnapMirror protege aplicações com LUNs iSCSI ou FCP.

A partir do ONTAP 9.15,1, o SnapMirror active Sync oferece suporte a um funcionalidade ativo-ativo simétrica, habilitando operações de e/S de leitura e gravação de ambas as cópias de um LUN protegido com replicação síncrona bidirecional, permitindo que ambas as cópias do LUN forneçam operações de e/S localmente. Antes do ONTAP 9.15,1, a sincronização ativa do SnapMirror suporta apenas configurações ativas/ativas assimétricas, nas quais os dados no local secundário são aumentados para um LUN.

A partir de julho de 2024, o conteúdo de relatórios técnicos publicados anteriormente como PDFs foi integrado à documentação do produto ONTAP. A documentação de sincronização ativa do ONTAP SnapMirror agora inclui conteúdo de *TR-4878: SnapMirror active Sync*.

Benefícios

O SnapMirror ative Sync oferece os seguintes benefícios:

- Disponibilidade contínua para aplicações essenciais aos negócios.
- Capacidade de hospedar aplicações críticas alternadamente de locais primários e secundários.
- Gerenciamento simplificado de aplicações usando grupos de consistência para consistência dependente da ordem de gravação.
- Capacidade de testar failover em cada aplicação.
- Criação instantânea de clones espelhados sem afetar a disponibilidade da aplicação.
- Capacidade de implantar workloads protegidos e não protegidos no mesmo cluster do ONTAP.
- A identidade de LUN permanece a mesma, então o aplicativo as vê como um dispositivo virtual compartilhado.
- Capacidade de reutilizar clusters secundários com flexibilidade para criar clones instantâneos para uso da aplicação para fins de desenvolvimento/teste, UAT ou geração de relatórios, sem impactar a performance ou a disponibilidade da aplicação.

O SnapMirror active Sync permite que você proteja LUNs de dados, o que permite o failover de aplicações de forma transparente, para fins de continuidade dos negócios em caso de desastre. Para obter mais informações, "Casos de uso"consulte .

Conceitos-chave

A sincronização ativa do SnapMirror utiliza grupos de consistência e o Mediador ONTAP para garantir que seus dados sejam replicados e atendidos, mesmo em caso de desastre. Ao Planejar sua implantação de sincronização ativa do SnapMirror, é importante entender os conceitos essenciais do SnapMirror ative Sync e sua arquitetura.

Assimetria e simetria

O SnapMirror ative Sync suporta soluções ativas-ativas assimétricas e, a partir do ONTAP 9.15,1, simétricas. Essas opções referem-se a como os hosts acessam caminhos de armazenamento e gravam dados. Em uma configuração assimétrica, os dados no local secundário são aumentados para um LUN. Em uma configuração ativo-ativo simétrica, ambos os locais podem acessar o storage local para e/S ativa

O ativo-ativo simétrico é otimizado para aplicativos em cluster, incluindo VMware vMSC, cluster de failover do Windows com SQL e Oracle RAC.

Para obter mais informações, Arquitetura de sincronização ativa do SnapMirrorconsulte .

Grupo de consistência

A "grupo de consistência" é uma coleção de volumes do FlexVol que garante consistência para o workload da aplicação que precisa ser protegido para manter a continuidade dos negócios.

O objetivo de um grupo de consistência é tirar imagens instantâneas simultâneas de vários volumes, garantindo assim cópias consistentes com falhas de uma coleção de volumes em um momento. Um grupo de consistência garante que todos os volumes de um conjunto de dados sejam silenciados e, em seguida, encaixados exatamente no mesmo ponto no tempo. Isso fornece um ponto de restauração consistente com dados nos volumes que dão suporte ao conjunto de dados. Um grupo de consistência mantém, assim, consistência dependente da ordem de gravação. Se você decidir proteger aplicativos para a continuidade dos negócios, o grupo de volumes correspondentes a esse aplicativo deve ser adicionado a um grupo de consistência para que um relacionamento de proteção de dados seja estabelecido entre uma origem e um grupo de consistência de destino. A consistência de origem e destino deve conter o mesmo número e tipo de volumes.

Constituinte

Um volume individual ou LUN que faz parte do grupo de consistência protegido na relação de sincronização ativa do SnapMirror.

ONTAP Mediador

O "ONTAP Mediador" recebe informações de integridade sobre nós e clusters ONTAP peered, orquestrando entre os dois e determinando se cada nó/cluster está íntegro e em execução. O Mediador ONTAP fornece as informações de saúde sobre:

- Clusters peer ONTAP
- Nós de cluster de peer ONTAP
- Grupos de consistência (que definem as unidades de failover em uma relação de sincronização ativa do SnapMirror); para cada grupo de consistência, as seguintes informações são fornecidas:
  - Estado de replicação: Não inicializado, em Sincronizar ou fora de Sincronizar
  - Qual cluster hospeda a cópia primária
  - Contexto de operação (usado para failover planejado)

Com essas informações de integridade do ONTAP Mediator, os clusters podem diferenciar entre tipos distintos de falhas e determinar se devem executar um failover automatizado. O Mediador ONTAP é uma das três partes no quorum de sincronização ativa do SnapMirror, juntamente com os clusters do ONTAP (primário e secundário). Para chegar a um consenso, pelo menos duas partes no quórum devem concordar com uma determinada operação.

> A partir do ONTAP 9.15,1, o Gerenciador do sistema exibe o status da relação de sincronização ativa do SnapMirror de qualquer cluster. Você também pode monitorar o status do Mediador ONTAP de qualquer cluster no Gerenciador de sistema. Em versões anteriores do ONTAP, o Gerenciador de sistema exibe o status das relações de sincronização ativa do SnapMirror a partir do cluster de origem.

Failover planejado

Uma operação manual para alterar as funções das cópias em uma relação de sincronização ativa do

SnapMirror. Os locais primários se tornam secundários, e o secundário se torna o primário.

Viés primário e primário

A sincronização ativa do SnapMirror usa um princípio primário que dá preferência à cópia primária para servir e/S no caso de uma partição de rede.

Primary-bias é uma implementação de quórum especial que melhora a disponibilidade de um conjunto de dados protegido por sincronização ativa do SnapMirror. Se a cópia primária estiver disponível, o viés primário entrará em vigor quando o Mediador ONTAP não estiver acessível a partir de ambos os clusters.

Primary-first e Primary bias são suportadas na sincronização ativa do SnapMirror a partir do ONTAP 9.15,1. As cópias primárias são designadas no System Manager e são enviadas com a API REST e CLI.

Failover não planejado automático (AUFO)

Uma operação automática para executar um failover para a cópia espelhada. A operação requer a assistência do Mediador ONTAP para detetar que a cópia primária não está disponível.

Fora de sincronização (OOS)

Quando a e/S do aplicativo não estiver replicando para o sistema de storage secundário, ela será reportada como **fora de sincronia**. Um status fora de sincronia significa que os volumes secundários não são sincronizados com o primário (origem) e que a replicação do SnapMirror não está ocorrendo.

Se o estado do espelho for `Snapmirrored`, isso indica uma falha ou falha de transferência devido a uma operação não suportada.

A sincronização ativa do SnapMirror suporta ressincronização automática, permitindo que as cópias voltem a um estado InSync.

A partir do ONTAP 9.15,1, a sincronização ativa do SnapMirror suporta "reconfiguração automática em configurações de fan-out".

Configuração uniforme e não uniforme

- **O acesso uniforme ao host** significa que os hosts de ambos os locais estão conetados a todos os caminhos para os clusters de armazenamento em ambos os locais. Os caminhos entre os locais são estendidos ao longo da distância.
- **Acesso não uniforme ao host** significa que os hosts em cada local são conetados apenas ao cluster no mesmo local. Caminhos entre locais e caminhos esticados não estão conetados.

> O acesso uniforme de host é compatível com qualquer implantação de sincronização ativa do SnapMirror. O acesso de host não uniforme só é compatível com implantações ativas/ativas simétricas.

RPO zero

RPO significa objetivo do ponto de restauração, que é a quantidade de perda de dados considerada aceitável durante um determinado período de tempo. Zero RPO significa que nenhuma perda de dados é aceitável.

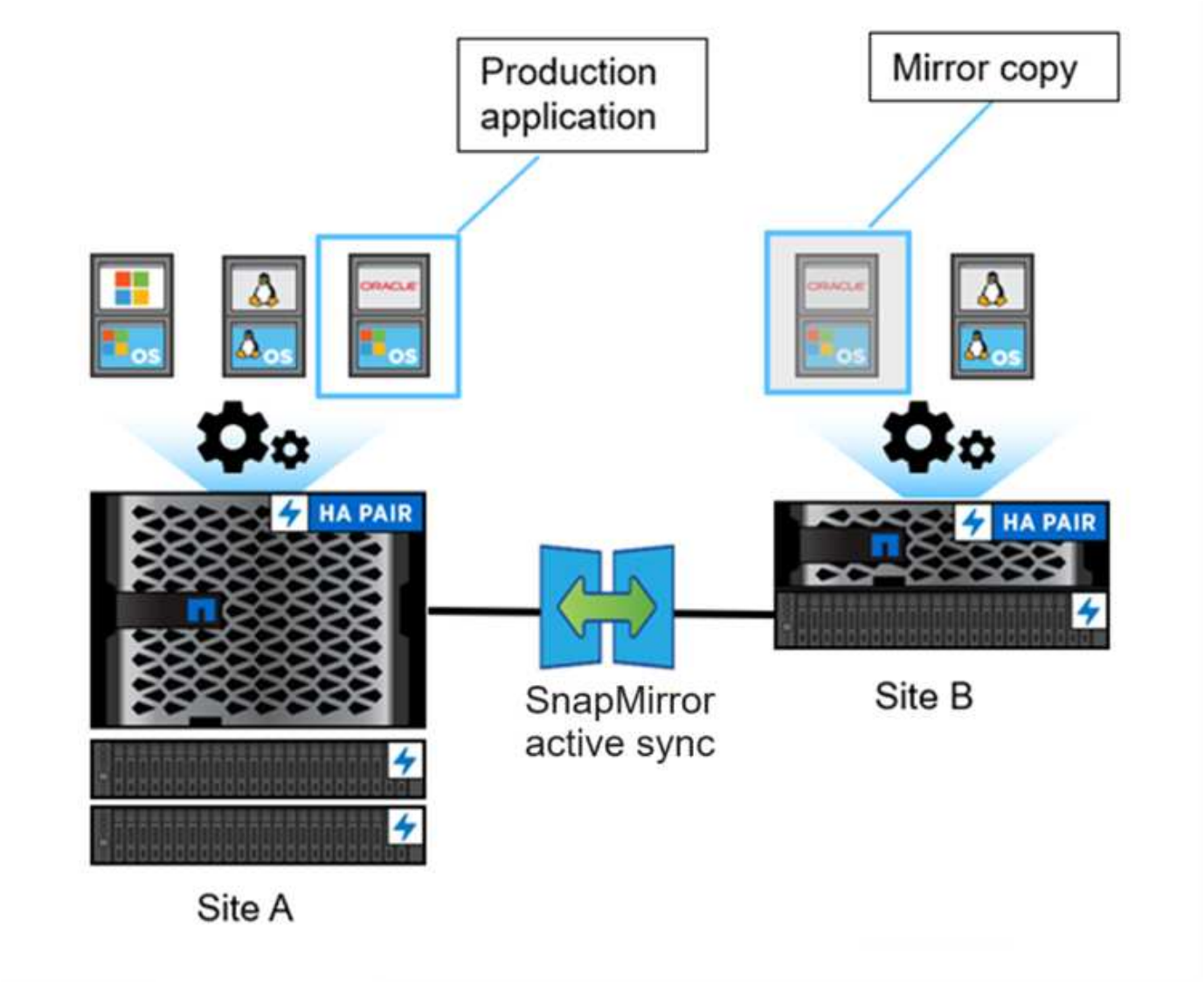
Rto zero

Rto representa o objetivo de tempo de recuperação, que é o tempo que é considerado aceitável para um aplicativo retornar às operações normais sem interrupções, após uma interrupção, falha ou outro evento de perda de dados. Zero rto significa que nenhuma quantidade de tempo de inatividade é aceitável.

Arquitetura de sincronização ativa do SnapMirror

A arquitetura de sincronização ativa do SnapMirror permite workloads ativos nos dois clusters, onde workloads primários podem ser atendidos simultaneamente a partir de ambos os clusters. Os regulamentos para instituições financeiras em alguns países exigem que as empresas sejam periodicamente reparáveis a partir de seus data centers secundários também, chamados de implantações de "Tick-Tock", que o SnapMirror ative Sync permite.

A relação de proteção de dados que protege para manter a continuidade dos negócios é criada entre o sistema de storage de origem e o sistema de storage de destino, adicionando LUNs específicas da aplicação de diferentes volumes em uma máquina virtual de storage (SVM) ao grupo de consistência. Em operações normais, a aplicação empresarial grava no grupo de consistência principal, o que replica de forma síncrona essa e/S para o grupo de consistência espelhada.



Embora existam duas cópias separadas dos dados na relação de proteção de dados, como a sincronização ativa do SnapMirror mantém a mesma identidade de LUN, o host do aplicativo vê isso como um dispositivo virtual compartilhado com vários caminhos, enquanto apenas uma cópia LUN está sendo gravada por vez. Quando uma falha torna o sistema de armazenamento primário offline, o ONTAP deteta essa falha e usa o Mediador para reconfirmação; se nem o ONTAP nem o Mediador forem capazes de fazer ping no local

principal, o ONTAP executará a operação de failover automático. Esse processo resulta em falha apenas de uma aplicação específica sem a necessidade de intervenção manual ou script que anteriormente era necessário para fins de failover.

Outros pontos a considerar:

- São suportados volumes não espelhados que existem fora da proteção para a continuidade dos negócios.
- Somente uma outra relação assíncrona do SnapMirror é suportada para volumes protegidos para continuidade dos negócios.
- Topologias em cascata não são suportadas com proteção para a continuidade dos negócios.

ONTAP Mediador

O ONTAP Mediator é instalado em um terceiro domínio de falha, distinto dos dois clusters ONTAP. Seu papel principal é atuar como uma testemunha passiva das cópias de sincronização ativa do SnapMirror. No caso de uma partição de rede ou indisponibilidade de uma cópia, o SnapMirror SnapMirror ative Sync usa o Mediator para determinar qual cópia continua a servir e/S, enquanto descontinua a e/S na outra cópia. Existem três componentes principais nesta configuração:

- Cluster ONTAP primário que hospeda o CG primário de sincronização ativa do SnapMirror
- Cluster ONTAP secundário que hospeda o CG espelhado
- ONTAP Mediador

O Mediador ONTAP desempenha um papel crucial nas configurações de sincronização ativa do SnapMirror como testemunha de quórum passivo, garantindo a manutenção do quórum e facilitando o acesso aos dados durante falhas. Ele atua como um proxy ping para controladores para determinar a vivacidade dos controladores peer. Embora o Mediator não acione ativamente as operações de comutação, ele fornece uma função vital, permitindo que o nó sobrevivente verifique o status de seu parceiro durante problemas de comunicação de rede. Em seu papel como testemunha de quórum, o Mediador ONTAP fornece um caminho alternativo (servindo efetivamente como proxy) para o cluster de pares.

Além disso, permite que os clusters obtenham essas informações como parte do processo de quórum. Ele utiliza o LIF de gerenciamento de nós e o LIF de gerenciamento de clusters para fins de comunicação. Ele estabelece conexões redundantes através de vários caminhos para diferenciar entre falha do local e falha do InterSwitch Link (ISL). Quando um cluster perde a conexão com o software Mediador ONTAP e todos os seus nós devido a um evento, ele é considerado não alcançável. Isso aciona um alerta e permite o failover automatizado para o Mirror Consistency Group (CG) no local secundário, garantindo e/S ininterrupto para o cliente. O caminho dos dados de replicação depende de um mecanismo de heartbeat, e se uma falha de rede ou evento persistir além de um determinado período, pode resultar em falhas de heartbeat, fazendo com que a relação fique fora de sincronia. No entanto, a presença de caminhos redundantes, como failover de LIF para outra porta, pode sustentar o batimento cardíaco e evitar tais interrupções.

Para resumir, o Mediador ONTAP é usado para os seguintes fins:

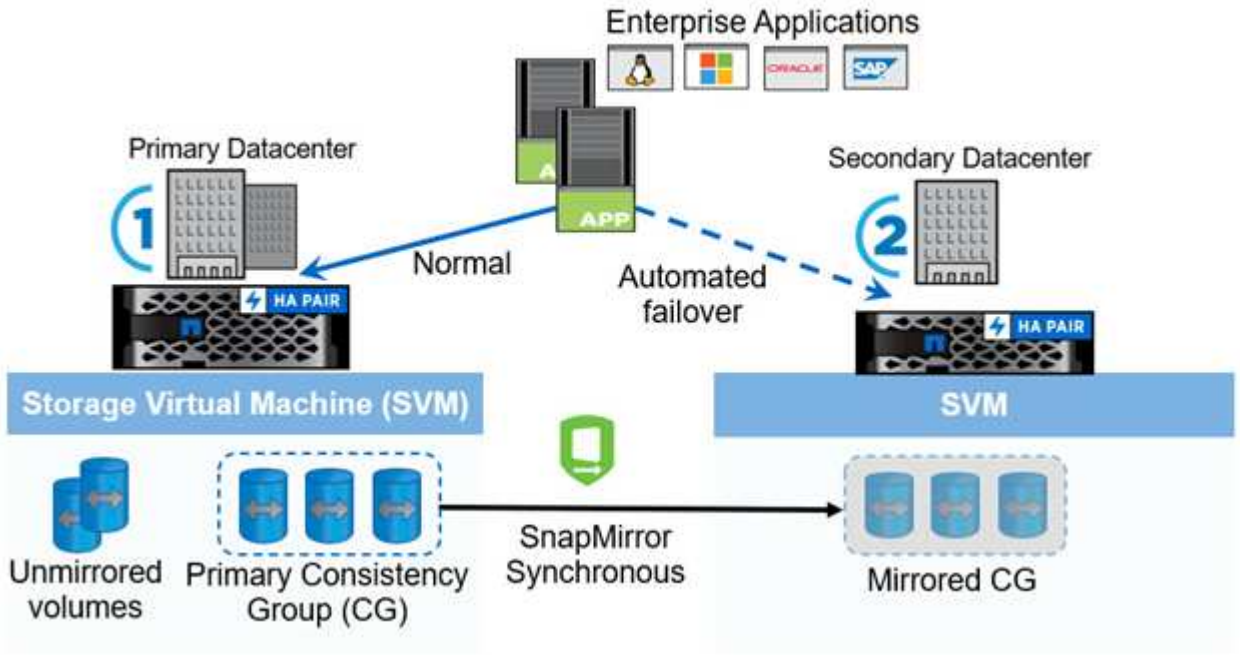
- Estabeleça um quórum
- Disponibilidade contínua por failover automático (AUFO)
- Failovers planejados (PFO)

> O ONTAP Mediator 1,7 pode gerenciar dez pares de cluster com o objetivo de continuidade dos negócios.

Quando o Mediador ONTAP não está disponível, não é possível executar failovers planejados ou automatizados. Os dados da aplicação continuam a replicar de forma síncrona, sem interrupções, para zero perda de dados.

Operações

A figura a seguir ilustra o design da sincronização ativa do SnapMirror em alto nível.



O diagrama mostra uma aplicação empresarial hospedada em uma VM de storage (SVM) no data center primário. O SVM contém cinco volumes, três dos quais fazem parte de um grupo de consistência. Os três volumes no grupo de consistência são espelhados para um data center secundário. Em circunstâncias normais, todas as operações de gravação são executadas no data center principal; na verdade, esse data center serve como fonte para operações de e/S, enquanto o data center secundário serve como destino.

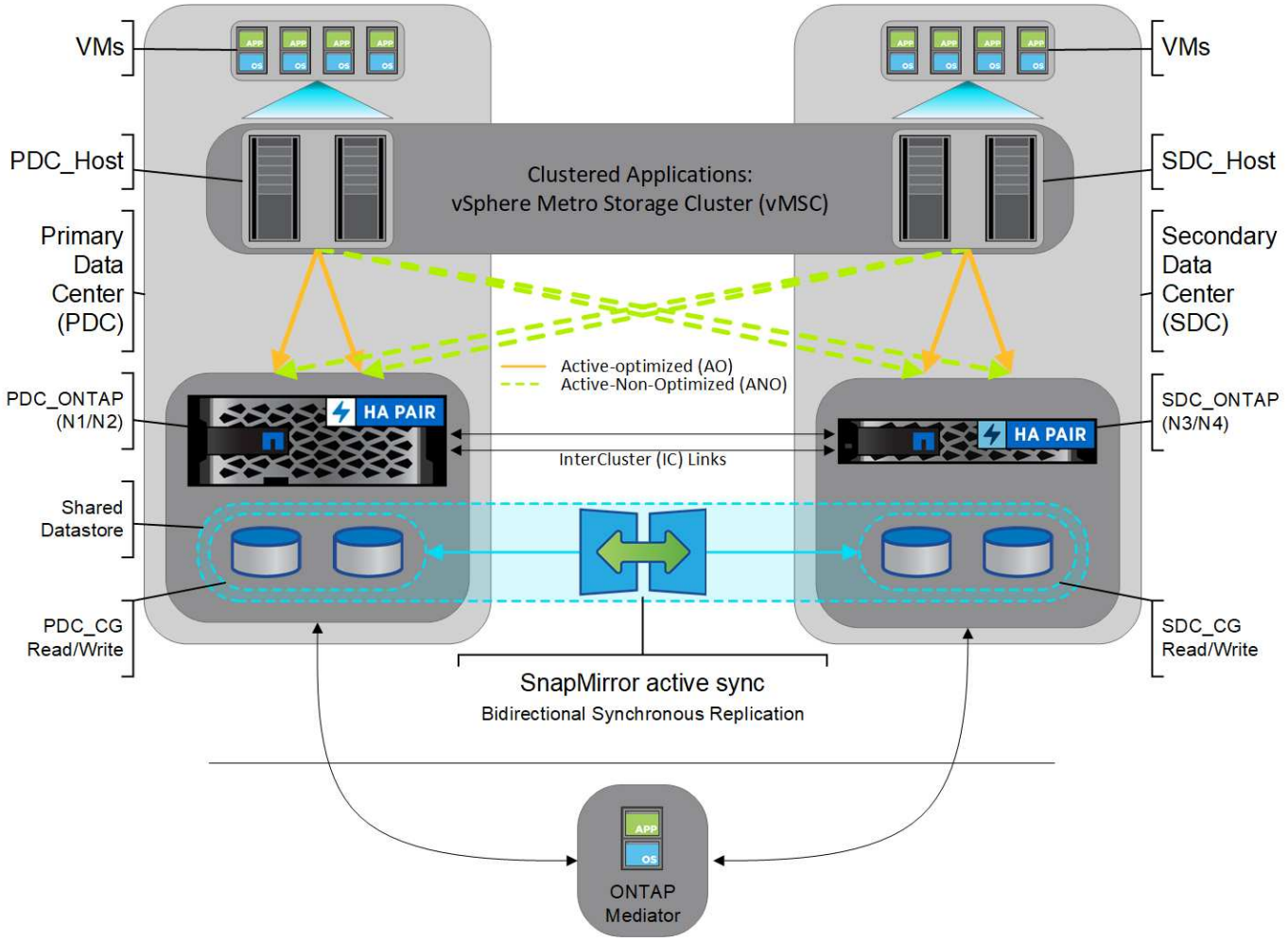
No caso de um cenário de desastre no data center principal, o ONTAP direciona o data center secundário para atuar como o principal, atendendo a todas as operações de e/S. Apenas os volumes que são espelhados no grupo consistência são servidos. Qualquer operação pertencente aos outros dois volumes na SVM será afetada pelo evento de desastre.

Ativo-ativo simétrico

O SnapMirror active Sync oferece soluções assimétricas e simétricas.

Em *configurações assimétricas*, a cópia de armazenamento primário expõe um caminho otimizado para ativos e serve ativamente e/S do cliente O local secundário usa um caminho remoto para e/S Os caminhos de storage do local secundário são considerados ativos-não-otimizados. O acesso ao LUN de gravação é maximizado a partir do site secundário.

Em *configurações ativas/ativas simétricas*, os caminhos otimizados para ativos são expostos em ambos os locais, são específicos do host e são configuráveis, o que significa que os hosts de ambos os lados podem acessar o storage local para e/S ativa



Ativo-ativo simétrico é destinado a aplicativos em cluster, incluindo VMware Metro Storage Cluster, Oracle RAC e Cluster de failover do Windows com SQL.

Casos de uso para sincronização ativa do SnapMirror

As demandas de um ambiente de negócios globalmente conectado exigem recuperação rápida de dados de aplicações essenciais aos negócios, sem perda de dados no caso de uma interrupção, como um ataque cibernético, uma interrupção de energia ou um desastre natural. Essas demandas são intensificadas em áreas como finanças e aquelas que aderiram a mandatos regulatórios, como o Regulamento Geral de proteção de dados (GDPR).

A sincronização ativa do SnapMirror fornece os seguintes casos de uso:

Implantação de aplicativos para objetivo de tempo de recuperação zero (rto)

Em uma implantação de sincronização ativa do SnapMirror, você tem um cluster primário e secundário. Um LUN no cluster primário `1LP`) tem um espelho (`L1s`) no secundário; ambos os LUNs compartilham o mesmo ID de série e são relatados como LUNs de leitura e gravação no host. No entanto, as operações de leitura e gravação só são atendidas no LUN primário `1LP`, . Todas as gravações no espelho `L1S` são servidas por proxy.

Implantação de aplicações para rto zero ou failover transparente de aplicações (TAF)

O TAF é baseado no failover de caminho baseado em software MPIO de host para obter acesso sem

interrupções ao storage. Ambas as cópias LUN - por exemplo, cópia primária (L1P) e cópia espelhada (L1S) - têm a mesma identidade (número de série) e são reportadas como graváveis para leitura para o host. No entanto, as leituras e gravações são atendidas apenas pelo volume primário. I/os emitidos para a cópia espelhada são proxied para a cópia primária. O caminho preferido do host para L1 é VS1:N1 com base no estado de acesso otimizado ativo (A/o) de acesso por unidade lógica assimétrica (ALUA). O Mediador ONTAP é necessário como parte da implantação, principalmente para executar failover (planejado ou não planejado) em caso de uma interrupção de storage no primário.

O SnapMirror ative Sync usa o ALUA, um mecanismo que permite que um software de multipathing host de aplicativos com caminhos anunciados com prioridades e disponibilidade de acesso para a comunicação do host de aplicativos com o storage array. O ALUA marca caminhos otimizados ativos para os controladores que possuem o LUN e outros como caminhos não otimizados ativos, usados somente se o caminho primário falhar.

Aplicações em cluster

Os aplicativos em cluster, incluindo VMware Metro Storage Cluster, Oracle RAC e Windows failover Clustering com SQL, exigem acesso simultâneo para que as VMs possam ser reexecutadas em outro local sem qualquer sobrecarga de desempenho. O SnapMirror ativo-ativo simétrico do SYNC ativo serve a e/S localmente com replicação bidirecional para atender aos requisitos de aplicações em cluster.

Cenário de desastre

Replique sincronamente vários volumes para uma aplicação entre locais em locais geograficamente dispersos. Você pode fazer o failover automaticamente para a cópia secundária em caso de interrupção do primário, permitindo a continuidade dos negócios das aplicações de camada um. Quando o site que hospeda o cluster primário sofre um desastre, o software de multipathing do host marca todos os caminhos pelo cluster como inativos e usa caminhos do cluster secundário. O resultado é um failover sem interrupções habilitado pelo ONTAP Mediator para a cópia espelhada.

Failover do Windows

O SnapMirror active Sync oferece flexibilidade com granularidade fácil de usar no nível da aplicação e failover automático. O SnapMirror active Sync usa replicação síncrona comprovada da SnapMirror em rede IP para replicar dados em alta velocidade via LAN ou WAN, para obter alta disponibilidade de dados e rápida replicação de dados para seus aplicativos essenciais aos negócios, como Oracle, Microsoft SQL Server e assim por diante, em ambientes virtuais e físicos.

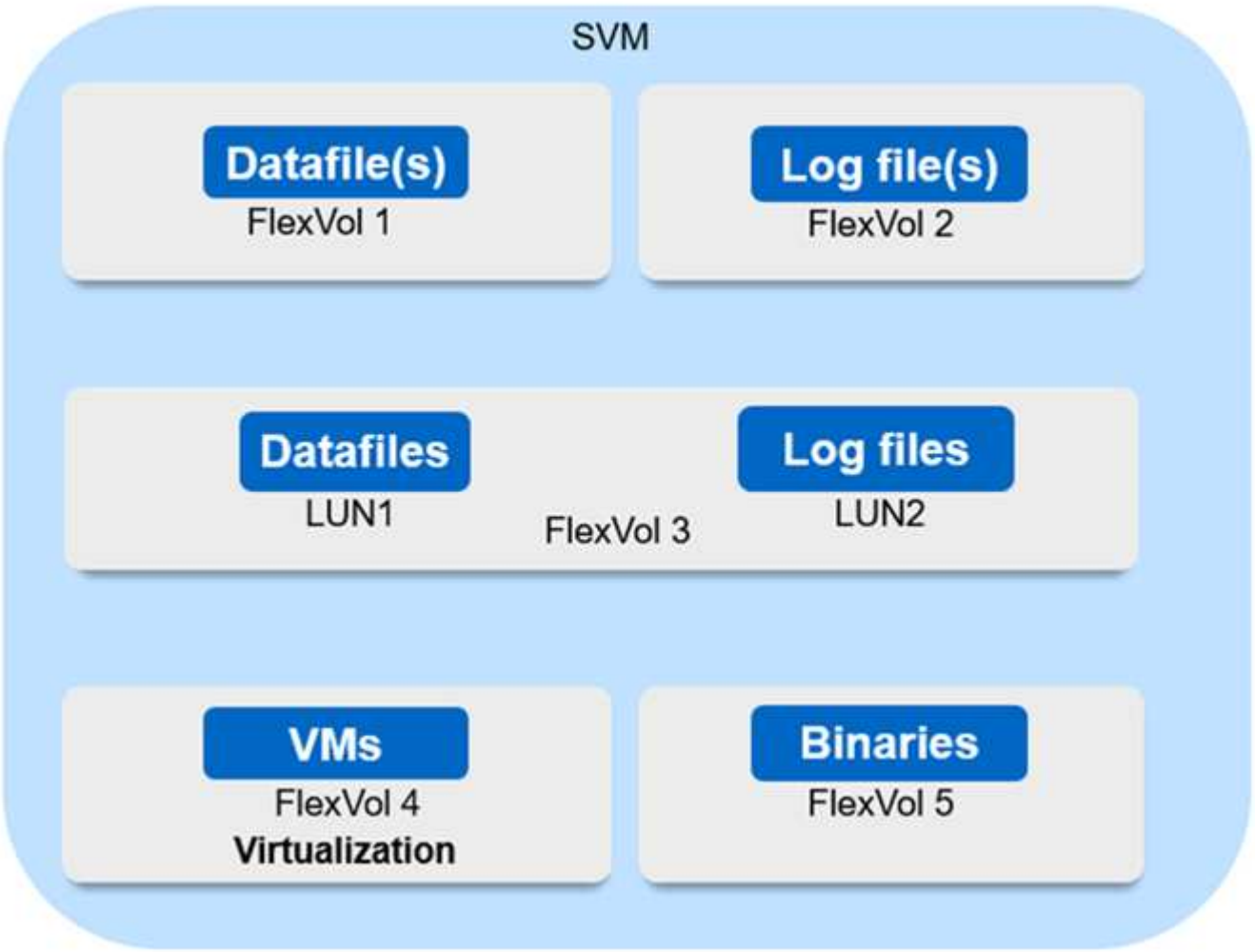
O SnapMirror ative Sync permite que os serviços de negócios essenciais continuem operando mesmo com uma falha completa do local, com o TAF para a cópia secundária. Nenhuma intervenção manual ou nenhum script adicional é necessário para acionar esse failover.

Estratégia de implantação e práticas recomendadas para a sincronização ativa do SnapMirror

É importante que sua estratégia de proteção de dados identifique claramente as ameaças aos workloads que precisam ser protegidas para manter a continuidade dos negócios. A etapa mais importante na estratégia de proteção de dados é ter clareza no layout de dados de aplicações empresariais para que você possa decidir como distribuir os volumes e proteger a continuidade dos negócios. Como o failover ocorre no nível do grupo de consistência por aplicação, adicione os volumes de dados necessários ao grupo de consistência.

Configuração SVM

O diagrama captura uma configuração recomendada de VM de storage (SVM) para sincronização ativa do SnapMirror.



- Para volumes de dados:
  - Cargas de trabalho de leitura aleatória são isoladas de gravações sequenciais; portanto, dependendo do tamanho do banco de dados, os dados e arquivos de log são normalmente colocados em volumes separados.
    - Para grandes bancos de dados críticos, o único arquivo de dados está no FlexVol 1 e seu arquivo de log correspondente está no FlexVol 2.
    - Para uma melhor consolidação, bancos de dados não críticos de tamanho pequeno a médio são agrupados de modo que todos os arquivos de dados estejam no FlexVol 1 e seus arquivos de log correspondentes estejam no FlexVol 2. No entanto, você perderá a granularidade no nível do aplicativo por meio desse agrupamento.
  - Outra variante é ter todos os arquivos dentro do mesmo FlexVol 3, com arquivos de dados em LUN1 e seus arquivos de log em LUN 2.
- Se o seu ambiente for virtualizado, você terá todas as VMs para vários aplicativos empresariais compartilhados em um datastore. Normalmente, as VMs e os binários da aplicação são replicados assincronamente usando o SnapMirror.

Plano

Pré-requisitos

Ao Planejar sua implantação de sincronização ativa do SnapMirror, verifique se você atendeu aos vários requisitos de hardware, software e configuração do sistema.

Hardware

- Somente clusters de HA de dois nós são compatíveis.
- Ambos os clusters precisam ser AFF (A-Series e C-Series) ou ASA (A-Series e C-Series). A mistura entre AFF e ASA não é suportada. A replicação é suportada entre o AFF A-Series e o C-Series.

Software

- ONTAP 9.9,1 ou posterior
- ONTAP Mediador 1,2 ou posterior
- Um servidor Linux ou máquina virtual para o Mediador ONTAP executando um dos seguintes:

ONTAP versão mediadora	Versões Linux suportadas
1,9	• Red Hat Enterprise Linux ◦ Compatível: 8,4, 8,5, 8,6, 8,7, 8,9, 9,1 e 9,3 1 ◦ Recomendado: 8,8, 8,10, 9,0, 9,2, 9,4 e 9,5 • Rocky Linux 8 e 9
1,8	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4 • Rocky Linux 8 e 9
1,7	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Rocky Linux 8 e 9
1,6	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2 • Rocky Linux 8 e 9
1,5	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,4	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,3	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3 • CentOS: 7,6, 7,7, 7,8, 7,9
1,2	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1 • CentOS: 7,6, 7,7, 7,8, 7,9

1. Compatível significa que o RHEL não suporta mais esta versão, mas o ONTAP Mediator ainda pode ser instalado.

Licenciamento

- A licença síncrona do SnapMirror deve ser aplicada em ambos os clusters.
- A licença do SnapMirror deve ser aplicada em ambos os clusters.

> Se os sistemas de storage da ONTAP tiverem sido adquiridos antes de junho de 2019, consulte "Chaves de licença principal do NetApp ONTAP" para obter a licença síncrona SnapMirror necessária.

Ambiente de rede

- O tempo de ida e volta (RTT) de latência entre clusters deve ser inferior a 10 milissegundos.
- A partir do ONTAP 9.14,1, "Reservas persistentes SCSI-3" são suportados com a sincronização ativa do SnapMirror.

Protocolos compatíveis

- Somente protocolos SAN são compatíveis (não NFS/SMB).
- Apenas são suportados protocolos Fibre Channel e iSCSI.
- O espaço IPspace padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos de pares de cluster. IPspace personalizado não é suportado.

Estilo de segurança NTFS

O estilo de segurança NTFS é **não** suportado em volumes de sincronização ativos do SnapMirror.

ONTAP Mediador

- O Mediador ONTAP deve ser provisionado externamente e anexado ao ONTAP para failover transparente de aplicativos.
- Para estar totalmente funcional e habilitar o failover automático não planejado, o mediador externo do ONTAP deve ser provisionado e configurado com clusters do ONTAP.
- O Mediador ONTAP deve ser instalado em um terceiro domínio de falha, separado dos dois clusters ONTAP.
- Ao instalar o Mediador ONTAP, você deve substituir o certificado autoassinado por um certificado válido assinado por uma CA confiável convencional.
- Para obter mais informações sobre o Mediador ONTAP, "Prepare-se para instalar o serviço Mediador ONTAP"consulte .

Outros pré-requisitos

- As relações de sincronização ativa do SnapMirror não são compatíveis com volumes de destino de leitura e gravação. Antes de usar um volume de leitura e gravação, você deve convertê-lo em um volume DP criando uma relação de SnapMirror em nível de volume e excluindo a relação. Para obter detalhes, "Converta relações SnapMirror existentes para a sincronização ativa do SnapMirror"consulte .
- As VMs de armazenamento que usam a sincronização ativa do SnapMirror não podem ser Unidas ao ative Directory como um cliente computado.

Mais informações

- "Hardware Universe"
- "Visão geral do Mediador ONTAP"

Interoperabilidade de sincronização ativa do SnapMirror

O SnapMirror ative Sync é compatível com vários sistemas operacionais, hosts de aplicativos e outros recursos do ONTAP.

Para obter detalhes específicos de capacidade de suporte e interoperabilidade não abordados aqui, consulte a ferramenta de Matriz de interoperabilidade ("IMT").

Hosts de aplicativos

Os hosts de aplicativos de suporte a sincronização ativa do SnapMirror incluem Hyper-V, Red Hat Enterprise Linux (RHEL), VMware, VMware vSphere Metro Storage Cluster (vMSC), Windows Server e, a partir do ONTAP 9.14,1, cluster de failover de servidor do Windows.

Sistemas operacionais

O SnapMirror ative Sync é compatível com vários sistemas operacionais, incluindo:

- AIX via PVR (Início ONTAP 9.11,1)
- HP-UX (Início do ONTAP 9.10,1)
- Solaris 11,4 (Início do ONTAP 9.10,1)

AIX

A partir do ONTAP 9.11,1, o AIX é suportado com a sincronização ativa do SnapMirror via PVR.

O SnapMirror active Sync pode fornecer proteção de dados RPO zero, mas o processo de failover com AIX requer etapas adicionais para reconhecer a alteração de caminho. Os LUNs que não fazem parte de um grupo de volume raiz terão uma pausa de e/S até que um `cfgmgr` comando seja executado. Isso pode ser automatizado, e a maioria dos aplicativos retomará as operações sem interrupções adicionais.

Os LUNs que fazem parte de um grupo de volumes raiz geralmente não devem ser protegidos com a sincronização ativa do SnapMirror. Não é possível executar o `cfgmgr` comando após um failover, o que significa que uma reinicialização é necessária para reconhecer as alterações nos caminhos SAN. Você ainda pode alcançar a proteção de dados RPO zero do grupo de volume raiz, mas o failover causará interrupções.

Consulte sua equipe de conta do NetApp para obter mais informações sobre a sincronização ativa do SnapMirror com o AIX.

HP-UX

A partir do ONTAP 9.10,1, é suportada a sincronização ativa do SnapMirror para HP-UX.

Failover automático não planejado com HP-UX

Um evento de failover não planejado automático (AUFO) no cluster mestre isolado pode ser causado por falha de evento duplo quando a conexão entre o cluster primário e o cluster secundário é perdida e a conexão entre o cluster primário e o mediador também é perdida. Este é considerado um evento raro, ao contrário de outros eventos AUFO.

- Nesse cenário, pode levar mais de 120 segundos para que a I/o seja retomada no host HP-UX. Dependendo dos aplicativos que estão sendo executados, isso pode não levar a interrupções de e/S ou mensagens de erro.
- Para remediar, é necessário reiniciar os aplicativos no host HP-UX que tenham uma tolerância de interrupção inferior a 120 segundos.

Solaris

A partir do ONTAP 9.10,1, o SnapMirror ative Sync suporta o Solaris 11,4.

Para garantir que os aplicativos clientes Solaris não sejam disruptivos quando ocorrer um switchover não planejado de failover de local em um ambiente de sincronização ativa do SnapMirror, modifique as configurações padrão do Solaris os. Para configurar o Solaris com as configurações recomendadas, consulte o artigo da base de dados de Conhecimento "Configurações recomendadas no SnapMirror ative Sync".

Interoperabilidade do ONTAP

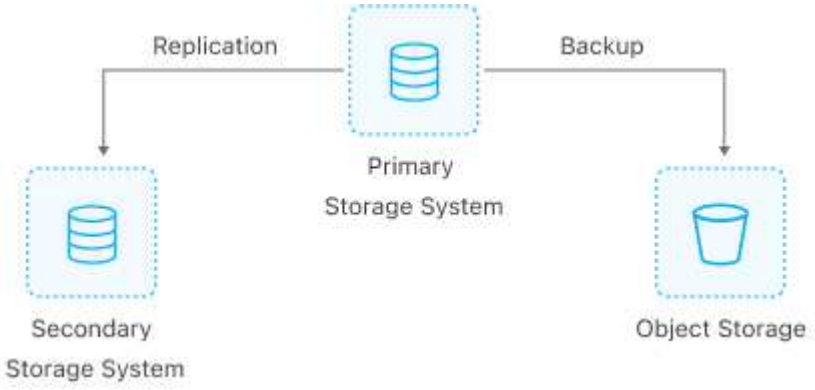
O SnapMirror active Sync integra-se a componentes do ONTAP para estender seus recursos de proteção de dados.

FabricPool

O SnapMirror active Sync é compatível com volumes de origem e destino em agregados FabricPool com políticas de disposição em camadas Nenhuma, Snapshot ou automática. O SnapMirror active Sync não é compatível com agregados FabricPool usando uma política de disposição em camadas.

Configurações de fan-out

No configurações de fan-out, o volume de origem pode ser espelhado em um ponto de extremidade de destino de sincronização ativa do SnapMirror e em um ou mais relacionamentos assíncronos do SnapMirror.



A sincronização ativa do SnapMirror é compatível configurações de fan-out com a `MirrorAllSnapshots` política e, a partir do ONTAP 9.11,1, a `MirrorAndVault` política. As configurações de fan-out não são suportadas na sincronização ativa do SnapMirror com a `XDPDefault` política.

A partir do ONTAP 9.15,1, o SnapMirror ative Sync suporta reconfiguração automática na etapa fan-out após um evento de failover. Se o failover do local primário para o local secundário tiver sido bem-sucedido, o local terciário será reconfigurado automaticamente para tratar o local secundário como a origem. A reconfiguração é acionada por um failover planejado ou não planejado. A reconfiguração também ocorre após o failback para o site primário.

Para obter informações sobre como gerenciar sua configuração de fan-out em versões anteriores do ONTAP,

retomar a proteção na configuração de fan-outconsulte .

Restauração NDMP

A partir do ONTAP 9.13,1, você pode usar NDMP para copiar e restaurar dados com a sincronização ativa do SnapMirror. O uso do NDMP permite que você mova dados para a fonte de sincronização ativa do SnapMirror para concluir uma restauração sem pausar a proteção. Isso é particularmente útil em configurações de fan-out.

SnapCenter

A sincronização ativa do SnapMirror é suportada com o SnapCenter a partir "SnapCenter 5,0"do . O SnapCenter permite a criação de snapshots que podem ser usados para proteger e recuperar aplicativos e máquinas virtuais, permitindo soluções de armazenamento sempre disponíveis com granularidade no nível do aplicativo.

SnapRestore

O SnapMirror ative Sync é compatível com SnapRestore de arquivo único e parcial.

SnapRestore de um único arquivo

A partir do ONTAP 9.11,1, Single-file SnapRestore é compatível com volumes de sincronização ativos do SnapMirror. É possível restaurar um único arquivo de uma cópia Snapshot replicada da fonte de sincronização ativa do SnapMirror para o destino. Como os volumes podem conter um ou mais LUNs, esse recurso ajuda a implementar uma operação de restauração menos disruptiva, restaurando de maneira granular um único LUN sem interromper os outros LUNs. O Single File SnapRestore tem duas opções: In-place e out-of-place.

SnapRestore de arquivo parcial

A partir do ONTAP 9.12,1, "Restauração parcial de LUN" é compatível com volumes de sincronização ativos do SnapMirror. É possível restaurar os dados de cópias Snapshot criadas por aplicações que foram replicadas entre a fonte (volume) de sincronização ativa do SnapMirror e os volumes de destino (cópia Snapshot). LUN parcial ou restauração de arquivos pode ser necessária se você precisar restaurar um banco de dados em um host que armazena vários bancos de dados no mesmo LUN. O uso desta funcionalidade requer que você saiba o deslocamento de byte inicial da contagem de dados e bytes.

LUNs grandes e grandes volumes

O suporte para LUNs grandes e volumes grandes (maiores de 100 TB) depende da versão do ONTAP que você está usando e da sua plataforma.

ONTAP 9.12.1P2 e posterior

- Para o ONTAP 9.12,1 P2 e posterior, o SnapMirror ative Sync suporta LUNs grandes e volumes grandes superiores a 100 TB no ASA e no AFF (Série A e Série C). Os clusters primário e secundário devem ser do mesmo tipo: ASA ou AFF. É suportada a replicação do AFF A-Series para o AFF C-Series e vice-versa.

> Nas versões 9.12.1P2 e posteriores do ONTAP, você precisa garantir que os clusters primário e secundário sejam all-flash SAN Arrays (ASA) ou all-flash array (AFF) e que ambos tenham ONTAP 9.12,1 P2 ou posterior instalado. Se o cluster secundário estiver executando uma versão anterior ao ONTAP 9.12.1P2 ou se o tipo de array não for o mesmo que o cluster primário, a relação síncrona poderá ficar fora de sincronia se o volume primário aumentar acima de 100 TB.

ONTAP 9.9,1 - 9.12.1P1

- Para versões do ONTAP entre o ONTAP 9.9,1 e o 9.12.1 P1 (inclusive), LUNs grandes e volumes maiores que 100TB TB são compatíveis apenas com arrays all-flash SAN. É suportada a replicação do AFF A-Series para o AFF C-Series e vice-versa.

> Para versões do ONTAP entre o ONTAP 9.9,1 e o 9.12.1 P2, você deve garantir que os clusters primário e secundário sejam all-flash SAN arrays e que ambos tenham o ONTAP 9.9,1 ou posterior instalado. Se o cluster secundário estiver executando uma versão anterior ao ONTAP 9.9,1 ou se não for um array SAN all-flash, a relação síncrona poderá ficar fora de sincronia se o volume primário aumentar acima de 100 TB.

Mais informações

- "Como configurar um host AIX para sincronização ativa do SnapMirror"

Limites de objetos para sincronização ativa do SnapMirror

Ao se preparar para usar a sincronização ativa do SnapMirror, esteja ciente dos seguintes limites de objeto.

Grupos de consistência em um cluster

Os limites de grupo de consistência para um cluster com sincronização ativa do SnapMirror são calculados com base nas relações e dependem da versão do ONTAP usada. Os limites são independentes da plataforma.

Versão de ONTAP	Número máximo de relacionamentos
ONTAP 9.11,1 e posterior	50
ONTAP 9.10,1	20
ONTAP 9.9,1	5

Volumes por grupo de consistência

O número máximo de volumes por grupo de consistência com a sincronização ativa do SnapMirror é independente da plataforma.

Versão de ONTAP	Número máximo de volumes suportados em uma relação de grupo de consistência
ONTAP 9.15,1 e posterior	80
ONTAP 9.10,1-9.14.1	16
ONTAP 9.9,1	12

Volumes

Os limites de volume na sincronização ativa do SnapMirror são calculados com base no número de endpoints, e não no número de relacionamentos. Um grupo de consistência com 12 volumes contribui com 12 pontos de extremidade no cluster primário e secundário. As relações de sincronização ativa do SnapMirror e sincronização SnapMirror contribuem para o número total de endpoints.

Os pontos finais máximos por plataforma estão incluídos na tabela a seguir.

S. não	Plataforma	Pontos de extremidade por HA para sincronização ativa do SnapMirror			Pontos de extremidade de sincronização total e de sincronização ativa do SnapMirror por HA		
		ONTAP 9.11,1 e posterior	ONTAP 9.10,1	ONTAP 9.9,1	ONTAP 9.11,1 e posterior	ONTAP 9.10,1	ONTAP 9.9,1
1	AFF	400	200	60	400	200	80
2	ASA	400	200	60	400	200	80

Limites de objetos SAN

Os limites de objetos SAN estão incluídos na tabela a seguir. Os limites se aplicam independentemente da plataforma.

Objeto em uma relação de sincronização ativa do SnapMirror	Contar
LUNs por volume	256
Mapas LUN por nó	• 4096 (ONTAP 9.10 e posterior) • 2048 (ONTAP 9.9,1 e anteriores)
Mapas LUN por cluster	• 8192 (ONTAP 9.10 e posterior) • 4096 (ONTAP 9.9,1 e anteriores)
LIFs por SVM (com pelo menos um volume em uma relação de sincronização ativa do SnapMirror)	256
LIFs entre clusters por nó	4
LIFs inter-cluster por cluster	8

Informações relacionadas

- "Hardware Universe"
- "Limites do grupo de consistência"

Configurar

Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror utiliza clusters com permissões para garantir que seus dados estejam disponíveis no caso de um cenário de failover. O Mediador ONTAP é um recurso chave que garante a continuidade dos negócios, monitorando a integridade de cada cluster. Para configurar a sincronização ativa do SnapMirror, primeiro instale o Mediador do ONTAP e verifique se os clusters primário e secundário estão configurados corretamente.

Depois de instalar o Mediador do ONTAP e configurar os clusters, você deve [initialize-the-ontap-mediator]usar o Mediador do ONTAP para usar com a sincronização ativa do SnapMirror. Você deve então Crie, inicialize e mapeie o grupo de consistência para a sincronização ativa do SnapMirror.

ONTAP Mediador

O Mediador do ONTAP fornece um armazenamento persistente e vedado para metadados de alta disponibilidade (HA) usados pelos clusters do ONTAP em uma relação de sincronização ativa do SnapMirror. Além disso, o ONTAP Mediator fornece uma funcionalidade de consulta de integridade de nó síncrono para auxiliar na determinação de quórum e serve como proxy de ping para deteção de vivacidade do controlador.

Pré-requisitos para o Mediador ONTAP

- O Mediador ONTAP inclui seu próprio conjunto de pré-requisitos. Você deve atender a esses pré-requisitos antes de instalar o mediador.

  Para obter mais informações, "Prepare-se para instalar o serviço Mediador ONTAP"consulte .

- Por padrão, o Mediador ONTAP fornece serviço através da porta TCP 31784. Você deve garantir que a porta 31784 esteja aberta e disponível entre os clusters do ONTAP e o mediador.

Instale o Mediador ONTAP e confirme a configuração do cluster

Prossiga por cada uma das etapas a seguir. Para cada etapa, você deve confirmar se a configuração específica foi executada. Use o link incluído após cada etapa para obter mais informações, conforme necessário.

Passos

1. Instale o serviço do Mediador ONTAP antes de garantir que os clusters de origem e destino estejam configurados corretamente.

   Prepare-se para instalar ou atualizar o serviço do Mediador ONTAP

2. Confirme se existe uma relação de peering de cluster entre os clusters.

   > O espaço IPspace padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos de pares de cluster. Um espaço IPspace personalizado não é suportado.

   Configurar relações entre pares

3. Confirme se as VMs de armazenamento são criadas em cada cluster.

   Criação de um SVM

4. Confirme se existe uma relação de pares entre as VMs de armazenamento em cada cluster.

   Criando uma relação de peering SVM

5. Confirme se os volumes existem para os LUNs.

   Criando um volume

6. Confirme se pelo menos um SAN LIF é criado em cada nó no cluster.

   "Considerações para LIFs em um ambiente de SAN de cluster"

   "Criando um LIF"

7. Confirme se os LUNs necessários são criados e mapeados para um grupo, que é usado para mapear LUNs para o iniciador no host do aplicativo.

   Crie LUNs e mapeie grupos

8. Pode novamente o anfitrião de aplicações para descobrir quaisquer novos LUNs.

Inicialize o Mediador ONTAP para sincronização ativa do SnapMirror usando certificados autoassinados

Depois de instalar o Mediador ONTAP e confirmar a configuração do cluster, você deve inicializar o Mediador ONTAP para monitoramento de cluster. Você pode inicializar o Mediador ONTAP usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

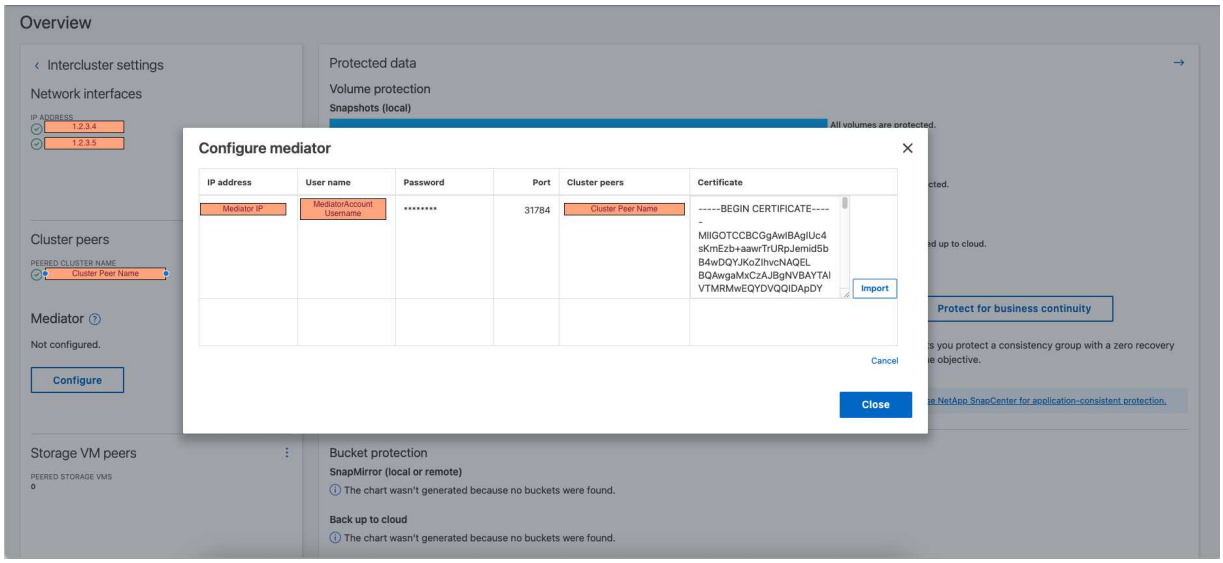
Com o Gerenciador de sistema, você pode configurar o servidor do ONTAP Mediator para failover automatizado. Você também pode substituir o SSL e a CA autoassinados pelo certificado SSL validado de terceiros e pela CA se ainda não o tiver feito.

> Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

ONTAP Mediador 1,9 e posterior

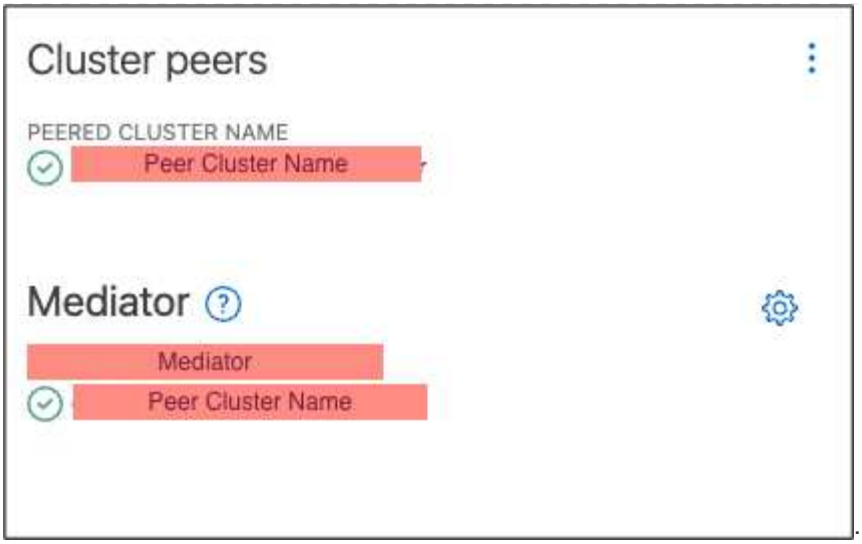
1. Navegue até **proteção > Visão geral > Mediador > Configurar**.
2. Selecione **Adicionar** e insira as seguintes informações do servidor do ONTAP Mediator:
   - Endereço IPv4
   - Nome de utilizador
   - Palavra-passe
   - Certificado
3. Você pode fornecer a entrada do certificado de duas maneiras:
   - **Opção (a)**: Selecione **Importar** para navegar para o `intermediate.crt` arquivo e importá-lo.
   - **Opção (b)**: Copie o conteúdo do `intermediate.crt` arquivo e cole-o no campo **certificado**.

   Quando todos os detalhes são inseridos corretamente, o certificado fornecido é instalado em todos os clusters de pares.



Quando a adição de certificado estiver concluída, o Mediador ONTAP é adicionado ao cluster ONTAP.

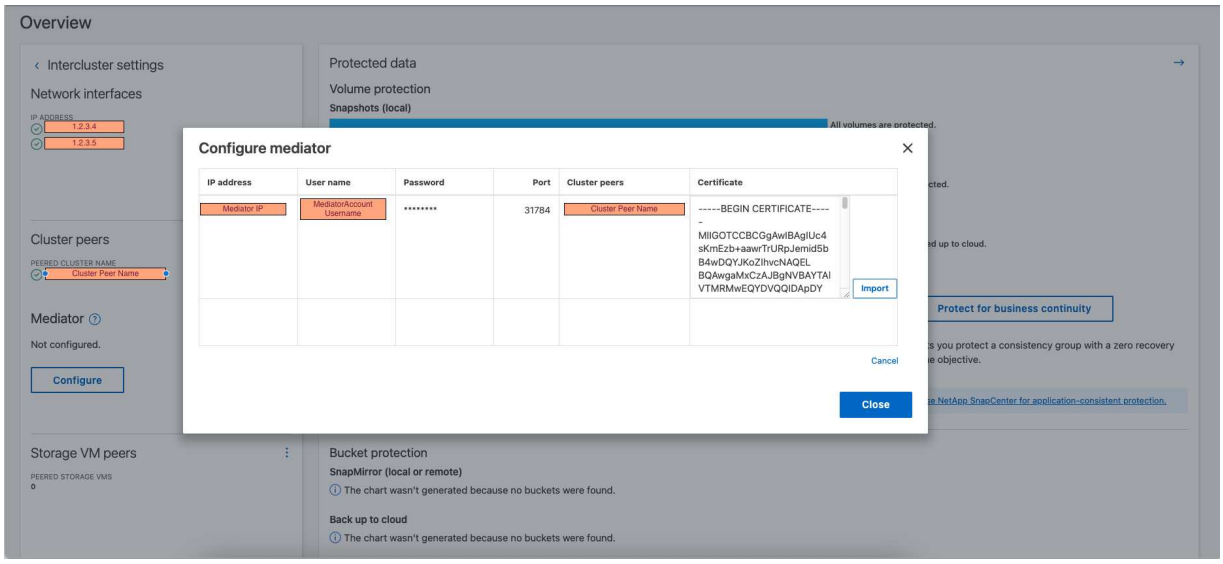
A imagem a seguir demonstra uma configuração bem-sucedida do ONTAP Mediator:



ONTAP Mediador 1,8 e anterior

1. Navegue até **proteção > Visão geral > Mediador > Configurar**.
2. Selecione **Adicionar** e insira as seguintes informações do servidor do ONTAP Mediator:
   - Endereço IPv4
   - Nome de utilizador
   - Palavra-passe
   - Certificado
3. Você pode fornecer a entrada do certificado de duas maneiras:
   - **Opção (a)**: Selecione **Importar** para navegar para o `ca.crt` arquivo e importá-lo.
   - **Opção (b)**: Copie o conteúdo do `ca.crt` arquivo e cole-o no campo **certificado**.

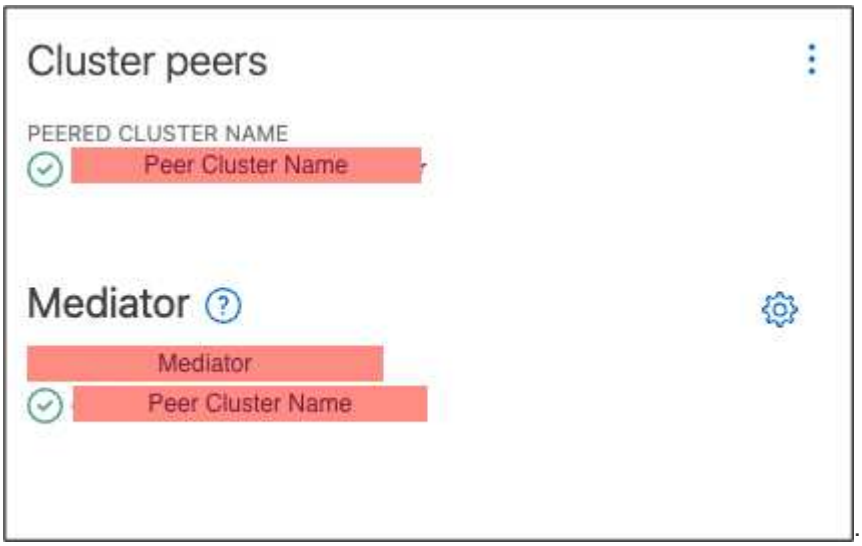
     Quando todos os detalhes são inseridos corretamente, o certificado fornecido é instalado em todos os clusters de pares.



Quando a adição de certificado estiver concluída, o Mediador ONTAP é adicionado ao cluster

ONTAP.

A imagem a seguir demonstra uma configuração bem-sucedida do ONTAP Mediator:



CLI

Você pode inicializar o Mediador ONTAP a partir do cluster primário ou secundário usando a CLI do ONTAP. Quando você emite o `mediator add` comando em um cluster, o Mediador ONTAP é adicionado automaticamente ao outro cluster.

Ao usar o Mediador para monitorar um relacionamento de sincronização ativa do SnapMirror, o Mediador não pode ser inicializado no ONTAP sem um certificado de autoridade de certificação (CA) ou autoassinado válido. Você adiciona um certificado válido ao armazenamento de certificados para clusters com permissões. Ao usar o Mediator para monitorar sistemas IP MetroCluster, o HTTPS não é usado após a configuração inicial; portanto, os certificados não são necessários.

ONTAP Mediador 1,9 e posterior

1. Localize o certificado da CA do Mediador ONTAP no local de instalação do software de host/VM do ONTAP Mediator Linux `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Adicione uma autoridade de certificação válida ao armazenamento de certificados no cluster de permissões.

   Exemplo

   ```
   [root@ontap-mediator server_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
   BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
   …
   p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
   -----END CERTIFICATE-----
   ```

3. Adicione o certificado da CA do Mediador do ONTAP a um cluster do ONTAP. Quando solicitado, insira o certificado de CA obtido no Mediador ONTAP. Repita as etapas em todos os clusters de pares:

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   Exemplo

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator server_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
   BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
   …
   p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. Exiba o certificado de CA autoassinado instalado usando o nome gerado do certificado:

   ```
   security certificate show -common-name <common_name>
   ```

   Exemplo

   ```
   C1_test_cluster::*> security certificate show -common-name
   ONTAPMediatorCA
   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- ------------------------------------
   ------------
   C1_test_cluster
              6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                              ONTAPMediatorCA
   server-ca
       Certificate Authority: ONTAP Mediator CA
             Expiration Date: Thu Feb 15 14:35:25 2029
   ```

5. Inicialize o Mediador ONTAP em um dos clusters. O Mediador ONTAP é adicionado automaticamente para o outro cluster:

   ```
   snapmirror mediator add -mediator-address <ip_address> -peer-cluster
   ```

`<peer_cluster_name> -username user_name`

Exemplo

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Verifique o status da configuração do Mediador ONTAP:

`snapmirror mediator show`

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` Indica se as relações de grupo de consistência do SnapMirror estão sincronizadas com o Mediador ONTAP; um status de `true` indica sincronização bem-sucedida.

ONTAP Mediador 1,8 e anterior

1. Localize o certificado da CA do Mediador ONTAP no local de instalação do software de host/VM do ONTAP Mediator Linux `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Adicione uma autoridade de certificação válida ao armazenamento de certificados no cluster de permissões.

Exemplo

```
[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

3. Adicione o certificado da CA do Mediador do ONTAP a um cluster do ONTAP. Quando solicitado, insira o certificado de CA obtido no Mediador ONTAP. Repita as etapas em todos os clusters de pares:

`security certificate install -type server-ca -vserver <vserver_name>`

Exemplo

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. Exiba o certificado de CA autoassinado instalado usando o nome gerado do certificado:

   `security certificate show -common-name <common_name>`

   Exemplo

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- -------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                          ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. Inicialize o Mediador ONTAP em um dos clusters. O Mediador ONTAP é adicionado automaticamente para o outro cluster:

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Exemplo

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Verifique o status da configuração do Mediador ONTAP:

   `snapmirror mediator show`

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

   `Quorum Status` Indica se as relações de grupo de consistência do SnapMirror estão sincronizadas com o Mediador ONTAP; um status de `true` indica sincronização bem-sucedida.

Reinicie o ONTAP Mediator com certificados de terceiros

Talvez seja necessário reinicializar o serviço ONTAP Mediator. Pode haver situações que exigem a reinicialização do serviço do Mediador ONTAP, como uma alteração no endereço IP do Mediador ONTAP, expiração do certificado e muito mais.

O procedimento a seguir ilustra a reinicialização do Mediador ONTAP para um caso específico quando um certificado autoassinado precisa ser substituído por um certificado de terceiros.

Sobre esta tarefa

Você precisa substituir os certificados autoassinados do cluster SM-BC por certificados de terceiros, remover a configuração do Mediador ONTAP do ONTAP e, em seguida, adicionar o Mediador ONTAP.

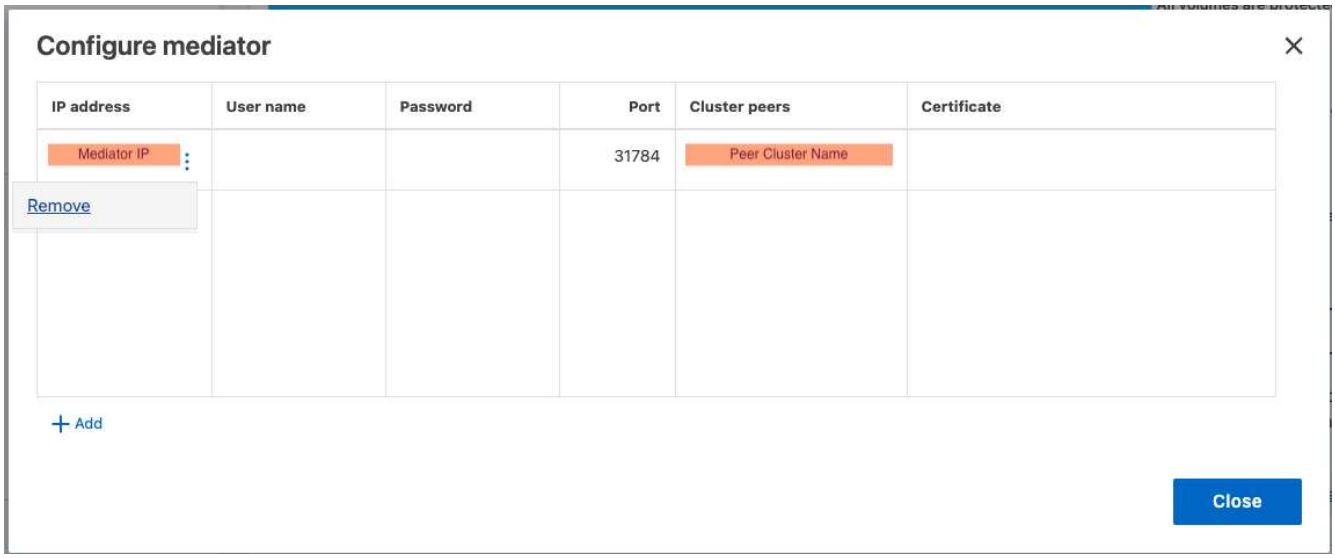
System Manager

Com o Gerenciador de sistema, você precisa remover o Mediador ONTAP configurado com o certificado autoassinado antigo do cluster ONTAP e reconfigurar o cluster ONTAP com o novo certificado de terceiros.

Passos

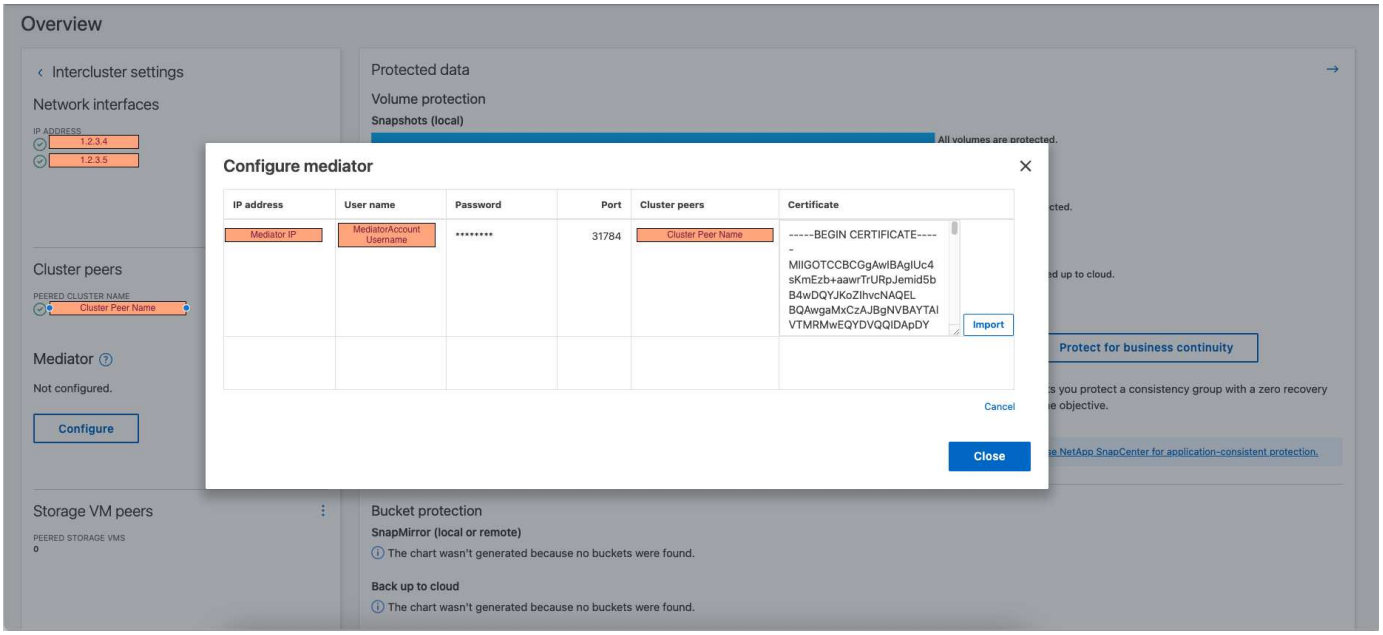
1. Selecione o ícone de opções de menu e selecione **Remover** para remover o Mediador ONTAP.

   Esta etapa não remove o servidor-CA autoassinado do cluster ONTAP. A NetApp recomenda navegar até a guia **certificado** e removê-lo manualmente antes de executar a próxima etapa abaixo para adicionar um certificado de terceiros:



2. Adicione o Mediador ONTAP novamente com o certificado correto.

O Mediador ONTAP está agora configurado com o novo certificado auto-assinado de terceiros.



CLI

Você pode reinicializar o Mediador do ONTAP a partir do cluster primário ou secundário usando a CLI do ONTAP para substituir o certificado autoassinado pelo certificado de terceiros.

ONTAP Mediador 1,9 e posterior

1. Remova o autoassinado instalado `intermediate.crt` anteriormente quando você usou certificados autoassinados para todos os clusters. No exemplo abaixo, há dois clusters:

   Exemplo

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. Remova o Mediador ONTAP configurado anteriormente do cluster SM-BC usando `-force true`:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Consulte as etapas descritas em "Substitua certificados autoassinados por certificados de terceiros confiáveis" para obter instruções sobre como obter certificados de uma CA subordinada, chamada de `intermediate.crt`. Substitua certificados autoassinados por certificados de terceiros confiáveis

O `intermediate.crt` tem certas propriedades que deriva da solicitação que precisam ser enviadas à autoridade PKI, definida no arquivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Adicione o novo certificado de CA do Mediador ONTAP de terceiros `intermediate.crt` a partir do local de instalação do software de VM/host do ONTAP Mediator:

   Exemplo

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator server_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

5. Adicione o `intermediate.crt` arquivo ao cluster de Contatos. Repita esta etapa para todos os clusters de pares:

   Exemplo

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Remova o Mediador ONTAP configurado anteriormente do cluster de sincronização ativa do SnapMirror:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Adicione o Mediador ONTAP novamente:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

`Quorum Status` Indica se as relações do grupo de consistência do SnapMirror estão sincronizadas com o mediador; um status de `true` indica a sincronização bem-sucedida.

ONTAP Mediador 1,8 e anterior

1. Remova o autoassinado instalado `ca.crt` anteriormente quando você usou certificados autoassinados para todos os clusters. No exemplo abaixo, há dois clusters:

   Exemplo

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. Remova o Mediador ONTAP configurado anteriormente do cluster SM-BC usando `-force true`:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Consulte as etapas descritas em "Substitua certificados autoassinados por certificados de terceiros confiáveis" para obter instruções sobre como obter certificados de uma CA subordinada, chamada de `ca.crt`. Substitua certificados autoassinados por certificados de terceiros confiáveis

> O `ca.crt` tem certas propriedades que deriva da solicitação que precisam ser enviadas à autoridade PKI, definida no arquivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Adicione o novo certificado de CA do Mediador ONTAP de terceiros `ca.crt` a partir do local de instalação do software de VM/host do ONTAP Mediator:

Exemplo

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

5. Adicione o `intermediate.crt` arquivo ao cluster de Contatos. Repita esta etapa para todos os clusters de pares:

   Exemplo

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Remova o Mediador ONTAP configurado anteriormente do cluster de sincronização ativa do SnapMirror:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Adicione o Mediador ONTAP novamente:

Exemplo

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

`Quorum Status` Indica se as relações do grupo de consistência do SnapMirror estão sincronizadas com o mediador; um status de `true` indica a sincronização bem-sucedida.

Proteja com a sincronização ativa do SnapMirror

O SnapMirror ative Sync oferece proteção assimétrica e, a partir do ONTAP 9.15,1, proteção ativa/ativa simétrica.

Configurar a proteção assimétrica

A configuração de proteção assimétrica usando a sincronização ativa do SnapMirror envolve a seleção de LUNs no cluster de origem do ONTAP e a adição a um grupo de consistência.

Antes de começar

- Você precisa ter uma licença síncrona do SnapMirror.
- Você deve ser um administrador de cluster ou VM de storage.
- Todos os volumes constituintes de um grupo de consistência precisam estar em uma única VM de storage (SVM).
  - Os LUNs podem residir em volumes diferentes.
- O cluster de origem e destino não pode ser o mesmo.
- Não é possível estabelecer relações de grupo de consistência de sincronização ativa do SnapMirror entre clusters do ASA e clusters que não sejam do ASA.
- O espaço IPspace padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos de pares de cluster. IPspace personalizado não é suportado.
- O nome do grupo de consistência deve ser único.
- Os volumes no cluster secundário (destino) devem ser do tipo DP.
- Os SVMs primário e secundário devem estar em uma relação de Contato.

Passos

Você pode configurar um grupo de consistência usando a CLI do ONTAP ou o Gerenciador do sistema.

A partir do ONTAP 9.10,1, o ONTAP oferece um endpoint de grupo de consistência e um menu no Gerenciador de sistemas, oferecendo utilitários de gerenciamento adicionais. Se estiver a utilizar o ONTAP 9.10,1 ou posterior, consulte "Configurar um grupo de consistência" "configurar a proteção"para criar uma relação de sincronização ativa do SnapMirror.

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

System Manager

1. No cluster principal, navegue até **proteção > Visão geral > proteger para continuidade de negócios > proteger LUNs**.
2. Selecione os LUNs que pretende proteger e adicione-os a um grupo de proteçãoão.
3. Selecione o cluster de destino e o SVM.
4. **Initialize Relationship** é selecionado por padrão. Clique em **Save** para iniciar a proteção.
5. Vá para **Dashboard > Performance** para verificar a atividade de IOPS dos LUNs.
6. No cluster de destino, use o System Manager para verificar se a proteção para o relacionamento de continuidade de negócios está em sincronia: **Proteção > relacionamentos**.

CLI

1. Crie uma relação de grupo de consistência a partir do cluster de destino.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   Você pode mapear até 12 volumes constituintes usando o `cg-item-mappings` parâmetro no `snapmirror create` comando.

   O exemplo a seguir cria dois grupos de consistência: `cg_src_ on the source with `vol1` E `vol2` um grupo de consistência de destino espelhado `cg_dst`, .

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. No cluster de destino, inicialize o grupo de consistência.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. Confirme se a operação de inicialização foi concluída com êxito. O estado deve ser `InSync`.

   ```
   snapmirror show
   ```

4. Em cada cluster, crie um grupo para que você possa mapear LUNs para o iniciador no host do aplicativo.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*
5. Em cada cluster, mapeie LUNs para o grupo:

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. Verifique se o mapeamento LUN foi concluído com êxito com o `lun map` comando. Depois, você pode descobrir os novos LUNs no host de aplicativos.

Configurar a proteção ativo-ativo simétrica

Você pode estabelecer proteção simétrica usando o Gerenciador do sistema ou a CLI do ONTAP. Em ambas

as interfaces, existem diferentes etapas para configurações uniformes e não uniformes.

Antes de começar

- Ambos os clusters devem estar executando o ONTAP 9.15,1 ou posterior.
- Configurações ativo-ativo simétricas exigem a `AutomatedFailoverDuplex` política de proteção. Como alternativa, você pode Crie uma política de SnapMirror personalizada fornecer o `-type` is `automated-failover-duplex`.

Exemplo 8. Passos

System Manager

Passos para uma configuração uniforme

1. No local principal, "Crie um grupo de consistência usando novos LUNs."
   a. Ao criar o grupo de consistência, especifique iniciadores de host para criar grupos.
   b. Marque a caixa de seleção para **Ativar SnapMirror** e escolha a `AutomatedFailoverDuplex` política.
   c. Na caixa de diálogo exibida, marque a caixa de seleção **Replique grupos de iniciadores** para replicar grupos de iniciadores. Em **Editar configurações proximais**, defina SVMs proximais para seus hosts.
   d. Selecione **Guardar**.

Passos para uma configuração não uniforme

1. No local principal, "Crie um grupo de consistência usando novos LUNs."
   a. Ao criar o grupo de consistência, especifique iniciadores de host para criar grupos.
   b. Marque a caixa de seleção para **Ativar SnapMirror** e escolha a `AutomatedFailoverDuplex` política.
   c. Selecione **Salvar** para criar os LUNs, o grupo de consistência, o grupo igrop, a relação SnapMirror e o mapeamento do grupo igrop.
2. No site secundário, crie um igrop e mapeie os LUNs.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione **Adicionar** para criar um novo grupo.
   c. Forneça um **Nome**, selecione **sistema operacional anfitrião** e, em seguida, escolha **Membros do Grupo Iniciador**.
   d. Selecione **Guardar**.
3. Mapeie o novo grupo para os LUNs de destino.
   a. Navegue até **armazenamento** > **LUNs**.
   b. Selecione todos os LUNs para mapear para o grupo.
   c. Selecione **More** (mais) e depois **Map to Initiator Groups (mapa para grupos de iniciadores)**.

CLI

Passos para uma configuração uniforme

1. Crie uma nova relação do SnapMirror agrupando todos os volumes na aplicação. Certifique-se de designar a `AutomatedFailOverDuplex` política para estabelecer replicação de sincronização bidirecional.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

2. Inicialize a relação SnapMirror:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. Confirme se a operação foi bem-sucedida, aguardando que o `Mirrored State` mostre como

`SnapMirrored` e `Relationship Status` as `Insync`.

```
snapmirror show -destination-path <destination_path>
```

4. No seu host, configure a conectividade de host com acesso a cada cluster de acordo com suas necessidades.
5. Estabeleça a configuração do grupo. Defina os caminhos preferidos para iniciadores no cluster local. Especifique a opção para replicar a configuração para a afinidade inversa do cluster de pares.

```
SiteA::> igroup create -vserver <svm_name> -os-type <os_type> -igroup
<igroup_name> -replication-peer <peer_svm_name> -initiator <host>

SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host>
```

6. A partir do host, descubra os caminhos e verifique se os hosts têm um caminho ativo/otimizado para o LUN de storage a partir do cluster preferido.
7. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters para alcançar o balanceamento de carga necessário.

Passos para uma configuração não uniforme

1. Crie uma nova relação do SnapMirror agrupando todos os volumes na aplicação. Certifique-se de designar a política "AutomatedFailOverDuplex" para estabelecer replicação de sincronização bidirecional.

```
snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source_volume:@destination_volume>
-policy AutomatedFailOverDuplex
```

2. Inicialize a relação SnapMirror:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. Confirme se a operação foi bem-sucedida, aguardando que o `Mirrored State` mostre como `SnapMirrored` e `Relationship Status` as `Insync`.

```
snapmirror show -destination-path <destination_path>
```

4. No seu host, configure a conectividade de host com acesso a cada cluster de acordo com suas necessidades.
5. Estabeleça as configurações do igrupo nos clusters de origem e destino.

```
# primary site
SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
<host_1_name_>

# secondary site
SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
<host_2_name>
```

6. A partir do host, descubra os caminhos e verifique se os hosts têm um caminho ativo/otimizado para o LUN de storage a partir do cluster preferido.
7. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters para alcançar o

balanceamento de carga necessário.

Converta uma relação existente do SnapMirror para uma relação de sincronização ativa do SnapMirror

Se tiver configurado a proteção SnapMirror, poderá converter a relação para a sincronização ativa do SnapMirror. A partir do ONTAP 9.15,1, você pode converter a relação para usar proteção ativa/ativa simétrica.

Converta uma relação SnapMirror existente em uma relação de sincronização ativa assimétrica do SnapMirror

Se você tiver uma relação síncrona SnapMirror existente entre um cluster de origem e destino, poderá convertê-la em uma relação de sincronização ativa assimétrica do SnapMirror. Isso permite associar os volumes espelhados a um grupo de consistência, garantindo RPO zero em um workload de vários volumes. Além disso, você pode reter snapshots existentes do SnapMirror se precisar reverter para um ponto no tempo antes de estabelecer a relação de sincronização ativa do SnapMirror.

Sobre esta tarefa

- Você precisa ser um administrador de cluster e SVM nos clusters primário e secundário.
- Você não pode converter RPO zero para sincronização rto zero alterando a política de SnapMirror.
- Você deve garantir que os LUNs não estejam mapeados antes de emitir o `snapmirror create` comando.

  Se os LUNs existentes no volume secundário forem mapeados e a `AutomatedFailover` política estiver configurada, o `snapmirror create` comando acionará um erro.

Antes de começar

- Uma relação de sincronização com SnapMirror RPO zero deve existir entre o cluster primário e o secundário.
- Todos os LUNs no volume de destino devem ser não mapeados antes que a relação zero rto SnapMirror possa ser criada.
- O SnapMirror active Sync só é compatível com protocolos SAN (não NFS/CIFS). Certifique-se de que nenhum componente do grupo de consistência está montado para acesso nas.

Passos

1. A partir do cluster secundário, execute uma atualização do SnapMirror sobre a relação existente:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verifique se a atualização do SnapMirror foi concluída com êxito:

   ```
   SiteB::>snapmirror show
   ```

3. Pausar cada um dos relacionamentos síncronos com RPO zero:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Exclua cada uma das relações síncronas com RPO zero:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Libere a relação de origem do SnapMirror, mas mantenha as cópias Snapshot comuns:

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Crie uma relação síncrona de rto SnapMirror zero:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. Ressincronize o grupo de consistência:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

Converta um relacionamento SnapMirror existente em ativo-ativo simétrico

A partir do ONTAP 9.15,1, você pode converter uma relação existente do SnapMirror para uma relação ativa/ativa simétrica de sincronização ativa do SnapMirror.

Antes de começar

- Você deve estar executando o ONTAP 9.15,1 ou posterior.
- Uma relação de sincronização com SnapMirror RPO zero deve existir entre o cluster primário e o secundário.
- Todos os LUNs no volume de destino devem ser não mapeados antes que a relação zero rto SnapMirror possa ser criada.
- O SnapMirror active Sync só é compatível com protocolos SAN (não NFS/CIFS). Certifique-se de que nenhum componente do grupo de consistência está montado para acesso nas.

Passos

1. A partir do cluster secundário, execute uma atualização do SnapMirror sobre a relação existente:

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. Verifique se a atualização do SnapMirror foi concluída com êxito:

```
SiteB::>snapmirror show
```

3. Pausar cada um dos relacionamentos síncronos com RPO zero:

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Exclua cada uma das relações síncronas com RPO zero:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Libere a relação de origem do SnapMirror, mas mantenha as cópias Snapshot comuns:

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Crie uma relação síncrona de rto SnapMirror zero com a política AutomatedFailoverDuplex:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. Se os hosts existentes forem locais, o cluster primário, adicione o host ao cluster secundário e estabeleça conetividade com o respetivo acesso a cada cluster.
8. No site secundário, exclua os mapas LUN nos grupos associados aos hosts remotos.

   Certifique-se de que o grupo não contenha mapas para LUNs não replicados.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. No local principal, modifique a configuração do iniciador para os hosts existentes para definir o caminho proximal para os iniciadores no cluster local.

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. Adicione um novo grupo e iniciador para os novos hosts e defina a proximidade do host para a afinidade do host para seu site local. Replicação do igroup para replicar a configuração e inverter a localidade do host no cluster remoto.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. Descubra os caminhos nos hosts e verifique se os hosts têm um caminho Ativo/otimizado para o LUN de armazenamento a partir do cluster preferido
12. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters.
13. Ressincronize o grupo de consistência:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

Converter tipo de relação de sincronização ativa do SnapMirror

A partir do ONTAP 9.15,1, você pode converter entre os tipos de proteção de sincronização ativa SnapMirror: De assimétrica a simétrica ativa ativa/ativa e vice-versa.

Converter em um relacionamento ativo-ativo simétrico

Você pode converter uma relação de sincronização ativa do SnapMirror com proteção assíncrona para usar ativo-ativo simétrico.

Antes de começar

- Ambos os clusters devem estar executando o ONTAP 9.15,1 ou posterior.
- Configurações ativo-ativo simétricas exigem a `AutomatedFailoverDuplex` política de proteção. Como alternativa, você pode Crie uma política de SnapMirror personalizada fornecer o `-type` is `automated-failover-duplex`.

System Manager

Passos para uma configuração uniforme

1. Remova o igrop de destino:
   a. No cluster de destino, navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo com o relacionamento SnapMirror e, em seguida, **Excluir**.
   c. Na caixa de diálogo, selecione a caixa **Unmap the Associated LUNs** (Anular mapeamento dos LUNs associados) e **Delete** (Excluir).
2. Edite a relação de sincronização ativa do SnapMirror.
   a. Navegue até **proteção** > **relacionamentos**.
   b. Selecione o menu kabob ao lado do relacionamento que você deseja modificar e, em seguida, **Editar**.
   c. Modifique a **Política de proteção** para AutomatedFailoverDuplex.
   d. A seleção `AutoMatedFailoverDuplex` de solicita uma caixa de diálogo para modificar as configurações de proximidade do host. Para os iniciadores, selecione a opção apropriada para **Iniciador proximal a** e, em seguida, **Guardar**.
   e. Selecione **Guardar**.
3. No menu **proteção**, confirme a operação bem-sucedida quando a relação for exibida como `InSync`.

Passos para uma configuração não uniforme

1. Remova o igrop de destino:
   a. No local secundário, navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo com o relacionamento SnapMirror e, em seguida, **Excluir**.
   c. Na caixa de diálogo, selecione a caixa **Unmap the Associated LUNs** (Anular mapeamento dos LUNs associados) e **Delete** (Excluir).
2. Crie um novo grupo:
   a. No menu **SAN Initiator Groups** no local de destino, selecione **Add**.
   b. Forneça um **Nome**, selecione **sistema operacional anfitrião** e, em seguida, escolha **Membros do Grupo Iniciador**.
   c. Selecione **Guardar**.
3. Mapeie o novo grupo para os LUNs de destino.
   a. Navegue até **armazenamento** > **LUNs**.
   b. Selecione todos os LUNs para mapear para o grupo.
   c. Selecione **More** (mais) e depois **Map to Initiator Groups (mapa para grupos de iniciadores)**.
4. Edite a relação de sincronização ativa do SnapMirror.
   a. Navegue até **proteção** > **relacionamentos**.
   b. Selecione o menu kabob ao lado do relacionamento que você deseja modificar e, em seguida, **Editar**.
   c. Modifique a **Política de proteção** para AutomatedFailoverDuplex.
   d. Selecionar AutoMatedFailoverDuplex inicia a opção para modificar as configurações de proximidade do host. Para os iniciadores, selecione a opção apropriada para **Iniciador proximal**

a e, em seguida, **Guardar**.

e. Selecione **Guardar**.

5. No menu **proteção**, confirme a operação bem-sucedida quando a relação for exibida como `InSync`.

CLI

Passos para uma configuração uniforme

1. Modifique a política SnapMirror de `AutomatedFailover` para `AutomatedFailoverDuplex`:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. A modificação da política aciona uma ressincronização. Aguarde até que a ressincronização seja concluída e confirme que a relação é `Insync`:

```
snapmirror show -destination-path <destination_path>
```

3. Se os hosts existentes forem locais, o cluster primário, adicione o host ao segundo cluster e estabeleça conetividade com o respetivo acesso a cada cluster.
4. No site secundário, exclua os mapas LUN nos grupos associados aos hosts remotos.

Certifique-se de que o grupo não contenha mapas para LUNs não replicados.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. No local principal, modifique a configuração do iniciador para os hosts existentes para definir o caminho proximal para os iniciadores no cluster local.

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name>
-initiator <host> -proximal-vserver <server>
```

6. Adicione um novo grupo e iniciador para os novos hosts e defina a proximidade do host para a afinidade do host para seu site local. Replicação do igroup para replicar a configuração e inverter a localidade do host no cluster remoto.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
host2 -proximal-vserver vsB
```

7. Descubra os caminhos nos hosts e verifique se os hosts têm um caminho Ativo/otimizado para o LUN de armazenamento a partir do cluster preferido
8. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters.

Passos para uma configuração não uniforme

1. Modifique a política SnapMirror de `AutomatedFailover` para `AutomatedFailoverDuplex`:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. A modificação da política aciona uma ressincronização. Aguarde até que a ressincronização seja concluída e confirme que a relação é `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. Se os hosts existentes forem locais para o cluster primário, adicione o host ao segundo cluster e estabeleça conetividade com o respetivo acesso a cada cluster.
4. No site secundário, exclua os mapas LUN nos grupos associados aos hosts remotos.

   Certifique-se de que o grupo não contenha mapas para LUNs não replicados.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

5. No local principal, modifique a configuração do iniciador para os hosts existentes para definir o caminho proximal para os iniciadores no cluster local.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name>
   -initiator <host> -proximal-vserver <server>
   ```

6. No site secundário, adicione um novo grupo e iniciador para os novos hosts e defina a proximidade do host para a afinidade do host para seu site local. Mapeie os LUNs para o grupo.

   ```
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
   SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
   <host_name>
   SiteB::> lun mapping create -igroup <igroup> -path <path_name>
   ```

7. Descubra os caminhos nos hosts e verifique se os hosts têm um caminho Ativo/otimizado para o LUN de armazenamento a partir do cluster preferido
8. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters.

Converter de ativo-ativo simétrico para uma relação assimétrica

Se você configurou a proteção ativa/ativa simétrica, você pode converter a relação para proteção assimétrica usando a CLI do ONTAP.

Passos

1. Mova todos os workloads de VM para o host local para o cluster de origem.
2. Remova a configuração do grupo para os hosts que não gerenciam as instâncias da VM, em seguida, modifique a configuração do grupo para encerrar a replicação do grupo.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. No local secundário, desmapeie os LUNs.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. No site secundário, exclua a relação ativo-ativo simétrica.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. No local principal, libere o relacionamento ativo-ativo simétrico.
```
SiteA::> snapmirror release -destination-path <destination_path> -relationship
-info-only true
```

6. A partir do site secundário, crie uma relação com o mesmo conjunto de volumes com a `AutomatedFailover` política para ressincronizar a relação.

```
SiteB::> snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source:@destination> -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
<policy_type>
```

> O grupo de consistência no site secundário precisa "a eliminar" antes de recriar a relação. Os volumes de "Tem de ser convertido para o tipo DP"destino . Para converter os volumes para DP, execute o `snapmirror resync` comando com uma não-`AutomatedFailover` política: `MirrorAndVault` `MirrorAllSnapshots` , Ou `Sync`.

7. Confirme se o estado do espelho de relacionamento é `Snapmirrored` o Status do relacionamento é `Insync`.

```
snapmirror show -destination-path destination_path
```

8. Redescubra os caminhos do anfitrião.

Gerencie a sincronização ativa do SnapMirror e proteja os dados

Crie uma cópia Snapshot comum

Além das operações de cópia Snapshot programadas regularmente, você pode criar manualmente um comum "Cópia Snapshot" entre os volumes no grupo de consistência do SnapMirror primário e os volumes no grupo de consistência do SnapMirror secundário.

Sobre esta tarefa

O intervalo de criação de Snapshot programado é de 12 horas.

Antes de começar

- A relação de grupo SnapMirror deve estar sincronizada.

Passos

1. Criar uma cópia Snapshot comum:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Monitorize o progresso da atualização:

```
destination::>snapmirror show -fields -newest-snapshot
```

Executar um failover planejado de clusters em uma relação de sincronização ativa do SnapMirror

Em um failover planejado de clusters do ONTAP em uma relação de sincronização ativa do SnapMirror, você alterna as funções dos clusters primário e secundário para que o cluster secundário assuma o controle do cluster primário. Durante um failover, o que normalmente é o cluster secundário processa as solicitações de entrada e saída localmente sem interromper as operações do cliente.

Você pode querer executar um failover planejado para testar a integridade da configuração de recuperação de desastres ou para executar a manutenção no cluster primário.

Sobre esta tarefa

Um failover planejado é iniciado pelo administrador do cluster secundário. A operação requer a comutação das funções primária e secundária para que o cluster secundário assuma o controle do primário. O novo cluster primário pode então começar a processar solicitações de entrada e saída localmente sem interromper as operações do cliente.

Antes de começar

- A relação de sincronização ativa do SnapMirror deve estar sincronizada.
- Não é possível iniciar um failover planejado quando uma operação sem interrupções está em processo. As operações ininterruptas incluem movimentação de volume, realocação de agregados e failovers de storage.
- O Mediador ONTAP deve ser configurado, conetado e no quórum.

Passos

Você pode executar um failover planejado usando a CLI do ONTAP ou o Gerenciador de sistema.

System Manager

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

1. No System Manager, selecione **proteção > Visão geral > relacionamentos**.
2. Identifique a relação de sincronização ativa do SnapMirror que você deseja fazer failover. Ao lado de seu nome, selecione o … próximo ao nome do relacionamento e, em seguida, selecione **failover**.
3. Para monitorar o status do failover, use o `snapmirror failover show` na CLI do ONTAP.

CLI

1. A partir do cluster de destino, inicie a operação de failover:

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Monitore o progresso do failover:

   ```
   destination::>snapmirror failover show
   ```

3. Quando a operação de failover estiver concluída, você poderá monitorar o status do relacionamento de proteção síncrona SnapMirror a partir do destino:

   ```
   destination::>snapmirror show
   ```

Recuperar de operações automáticas de failover não planejadas

Uma operação automática de failover não planejado (AUFO) ocorre quando o cluster primário está inativo ou isolado. O Mediador ONTAP deteta quando ocorre um failover e executa um failover automático não planejado para o cluster secundário. O cluster secundário é convertido para o primário e começa a servir os clientes. Esta operação é realizada apenas com a ajuda do Mediador ONTAP.

Após o failover automático não planejado, é importante reexaminar os caminhos de e/S LUN do host para que não haja perda de caminhos de e/S.

Restabeleça o relacionamento de proteção após um failover não planejado

É possível restabelecer a relação de proteção usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

Passos

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

1. Navegue até **proteção > relacionamentos** e aguarde que o estado da relação mostre "InSync".
2. Para retomar as operações no cluster de origem original, clique ⋮ e selecione **failover**.

CLI

Você pode monitorar o status do failover automático não planejado usando o `snapmirror failover show` comando.

Por exemplo:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte "Referência da EMS"para obter informações sobre mensagens de eventos e sobre ações corretivas.

Retomar a proteção em uma configuração de fan-out após o failover

A partir do ONTAP 9.15,1, o SnapMirror ative Sync suporta reconfiguração automática na etapa fan-out após um evento de failover. Para obter mais informações, "configurações de fan-out"consulte .

Se você estiver usando o ONTAP 9.14,1 ou anterior e tiver um failover no cluster secundário na relação de sincronização ativa do SnapMirror, o destino assíncrono do SnapMirror não será saudável. Você deve restaurar manualmente a proteção excluindo e recriando a relação com o endpoint assíncrono do SnapMirror.

Passos

1. Verifique se o failover foi concluído com êxito:
   `snapmirror failover show`
2. No endpoint assíncrono do SnapMirror, exclua o endpoint de fan-out:
   `snapmirror delete -destination-path` *`destination_path`*
3. No terceiro site, crie relações assíncronas do SnapMirror entre o novo volume primário de sincronização ativa do SnapMirror e o volume de destino de saída de ventoinha assíncrona:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`*

`-policy MirrorAllSnapshots -schedule schedule`

4. Ressincronizar a relação:
`snapmirror resync -destination-path destination_path`
5. Verifique o status e a saúde da relação:
`snapmirror show`

Monitorar operações de sincronização ativa do SnapMirror

Você pode monitorar as seguintes operações de sincronização ativa do SnapMirror para garantir a integridade da configuração de sincronização ativa do SnapMirror:

- ONTAP Mediador
- Operações de failover planejadas
- Operações automáticas de failover não planejadas
- Disponibilidade de sincronização ativa do SnapMirror

> A partir do ONTAP 9.15,1, o Gerenciador do sistema exibe o status da relação de sincronização ativa do SnapMirror de qualquer cluster. Você também pode monitorar o status do Mediador ONTAP de qualquer cluster no Gerenciador de sistema.

ONTAP Mediador

Durante as operações normais, o estado do Mediador ONTAP deve ser conetado. Se estiver em qualquer outro estado, isso pode indicar uma condição de erro. Pode rever o "Mensagens do sistema de Gestão de Eventos (EMS)" para determinar o erro e as ações corretivas adequadas.

Operações de failover planejadas

Você pode monitorar o status e o progresso de uma operação de failover planejada usando o `snapmirror failover show` comando. Por exemplo:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Depois que a operação de failover estiver concluída, você poderá monitorar o status de proteção SnapMirror a partir do novo cluster de destino. Por exemplo:

```
ClusterA::> snapmirror show
```

Consulte "Referência da EMS"para obter informações sobre mensagens de eventos e ações corretivas.

Operações automáticas de failover não planejadas

Durante um failover automático não planejado, você pode monitorar o status da operação usando o `snapmirror failover show` comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte "Referência da EMS"para obter informações sobre mensagens de eventos e sobre ações corretivas.

Disponibilidade de sincronização ativa do SnapMirror

Você pode verificar a disponibilidade da relação de sincronização ativa do SnapMirror usando uma série de comandos, no cluster primário, no cluster secundário ou em ambos.

Os comandos usados incluem o `snapmirror mediator show` comando no cluster primário e secundário para verificar o status da conexão e do quórum, o `snapmirror show` comando e o `volume show` comando. Por exemplo:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

Adicione ou remova volumes a um grupo de consistência

À medida que os requisitos de workload do aplicativo mudam, você pode precisar adicionar ou remover volumes de um grupo de consistência para garantir a continuidade dos negócios. O processo de adição e remoção de volumes em uma relação de sincronização ativa do SnapMirror depende da versão do ONTAP que você está usando.

Na maioria dos casos, este é um processo disruptivo que exige que você exclua a relação SnapMirror, modifique o grupo de consistência e, em seguida, retome a proteção. A partir do ONTAP 9.13,1, adicionar volumes a um grupo de consistência com uma relação SnapMirror ativa é uma operação sem interrupções.

Sobre esta tarefa

- No ONTAP 9.9,1, você pode adicionar ou remover volumes a um grupo de consistência usando a CLI do ONTAP.
- A partir do ONTAP 9.10,1, é recomendável que você gerencie "grupos de consistência" por meio do Gerenciador de sistema ou com a API REST do ONTAP.

  Se você quiser alterar a composição do grupo de consistência adicionando ou removendo um volume, primeiro exclua a relação original e, em seguida, crie o grupo de consistência novamente com a nova composição.

- A partir do ONTAP 9.13,1, você pode adicionar volumes a um grupo de consistência sem interrupções com uma relação do SnapMirror ativa da origem ou destino.

  Remover volumes é uma operação disruptiva. Você deve excluir a relação do SnapMirror antes de remover volumes.

ONTAP 9.9,1-9.13.0

Antes de começar

- Você não pode começar a modificar o grupo de consistência enquanto ele estiver no `InSync` estado.
- O volume de destino deve ser do tipo DP.
- O novo volume adicionado para expandir o grupo de consistência precisa ter um par de cópias Snapshot comuns entre os volumes de origem e destino.

Passos

Os exemplos mostrados em dois mapeamentos de volume: `vol_src1 vol_dst1 vol_src2 vol_dst2` Em uma relação de grupo de consistência entre os pontos finais `vs1_src:/cg/cg_src` e `vs1_dst:/cg/cg_dst`.

1. Nos clusters de origem e destino, verifique se há um Snapshot comum entre os clusters de origem e destino com o comando `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. Se não existir uma cópia Snapshot comum, crie e inicialize uma relação FlexVol SnapMirror:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Excluir a relação do grupo de consistência:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
   ```

4. Solte a relação de origem do SnapMirror e mantenha as cópias Snapshot comuns:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Desmapeie os LUNs e exclua a relação de grupo de consistência existente:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > Os LUNs de destino não são mapeados, enquanto os LUNs na cópia primária continuam a servir a e/S do host

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **Se você estiver usando ONTAP 9.10,1 até 9.13.0,** delete e recrie e o grupo consistência na fonte

com a composição correta. Siga os passos em Excluir um grupo de consistência e, Configurar um único grupo de consistênciaem seguida, . No ONTAP 9.10,1 e posterior, você deve executar as operações de exclusão e criação no Gerenciador de sistema ou com a API REST do ONTAP; não há procedimento de CLI.

Se você estiver usando o ONTAP 9.9,1, vá para a próxima etapa.

7. Crie o novo grupo de consistência no destino com a nova composição:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Ressincronize a relação do grupo de consistência rto zero para garantir que ela esteja sincronizada:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Remapear os LUNs não mapeados na Etapa 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

ONTAP 9.13,1 e posterior

A partir do ONTAP 9.13,1, você pode adicionar volumes a um grupo de consistência sem interrupções com uma relação de sincronização ativa do SnapMirror. O SnapMirror ative Sync suporta a adição de volumes da origem ou do destino.

> Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

Para obter detalhes sobre como adicionar volumes do grupo de consistência de origem, Modifique um grupo de consistênciaconsulte .

Adicione um volume do cluster de destino

1. No cluster de destino, selecione **proteção** > **relacionamentos**.
2. Encontre a configuração do SnapMirror à qual deseja adicionar volumes. Selecione ⋮ e, em seguida, **expandir**.
3. Selecione as relações de volume cujos volumes devem ser adicionados ao grupo de consistência
4. Selecione **expandir**.

Atualize e reverta o ONTAP com a sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror é suportada a partir do ONTAP 9.9,1. A atualização e reversão do cluster do ONTAP tem implicações nas relações de sincronização ativa do SnapMirror, dependendo da versão do ONTAP para a qual você está atualizando ou revertendo.

Atualize o ONTAP com a sincronização ativa do SnapMirror

Para usar a sincronização ativa do SnapMirror, todos os nós nos clusters de origem e destino devem estar executando o ONTAP 9.9,1 ou posterior.

Ao atualizar o ONTAP com relações de sincronização ativas do SnapMirror, você deve usar Atualização automatizada sem interrupções (ANDU)o . O uso DO ANDU garante que suas relações de sincronização ativa do SnapMirror estejam sincronizadas e íntegras durante o processo de atualização.

Não há etapas de configuração para preparar implantações de sincronização ativa do SnapMirror para atualizações do ONTAP. No entanto, é recomendável que antes e depois da atualização, você verifique se:

- As relações de sincronização ativa do SnapMirror estão sincronizadas.
- Não existem erros relacionados ao SnapMirror no registo de eventos.
- O Mediator está on-line e saudável de ambos os clusters.
- Todos os hosts podem ver todos os caminhos corretamente para proteger LUNs.

> Quando você atualiza clusters do ONTAP 9.9,1 ou 9.9.1 para o ONTAP 9.10,1 e posterior, o ONTAP cria novos grupos de consistênciaclusters de origem e destino para as relações de sincronização ativa do SnapMirror que podem ser configuradas usando o Gerenciador do sistema.

> `snapmirror quiesce`Os comandos e `snampirror resume` não são suportados com a sincronização ativa do SnapMirror.

Reverter para ONTAP 9.9,1 a partir de ONTAP 9.10,1

Para reverter relacionamentos de 9.10.1 para 9,9.1, as relações de sincronização ativa do SnapMirror devem ser excluídas, seguidas pela instância do grupo de consistência do 9.10.1. Os grupos de consistência com uma relação de sincronização ativa do SnapMirror não podem ser excluídos. Todos os volumes do FlexVol que foram atualizados para o 9.10.1 anteriormente associados a outro contêiner inteligente ou aplicativo empresarial em 9.9.1 ou anterior não serão mais associados ao Revert. A exclusão de grupos de consistência não exclui os volumes constituintes ou instantâneos granulares de volume. "Excluir um grupo de consistência"Consulte para obter mais informações sobre esta tarefa no ONTAP 9.10,1 e posterior.

Reverter de ONTAP 9.9,1

> A sincronização ativa do SnapMirror não é compatível com clusters ONTAP mistos do que incluir versões anteriores ao ONTAP 9.9,1.

Ao reverter do ONTAP 9.9,1 para uma versão anterior do ONTAP, você deve estar ciente do seguinte:

- Se o cluster hospedar um destino de sincronização ativa do SnapMirror, reverter para o ONTAP 9.8 ou anterior não será permitido até que o relacionamento seja quebrado e excluído.
- Se o cluster hospedar uma fonte de sincronização ativa do SnapMirror, reverter para o ONTAP 9.8 ou anterior não será permitido até que a relação seja liberada.
- Todas as políticas de sincronização ativa do SnapMirror personalizadas criadas pelo usuário devem ser excluídas antes de reverter para o ONTAP 9.8 ou anterior.

Para atender a esses requisitos, "Remova uma configuração de sincronização ativa do SnapMirror"consulte .

Passos

1. Confirme sua prontidão para reverter, inserindo o seguinte comando de um dos clusters na relação de sincronização ativa do SnapMirror:

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   A saída de amostra a seguir mostra um cluster que não está pronto para reverter com instruções para limpeza.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
      abort
       Command to see if the Relationship Status of a SnapMirror
   relationship
      is Quiesced: snapmirror show
       Command to break off a data-protection volume: snapmirror break
       Command to break off a data-protection volume which is the
   destination
      of a SnapMirror relationship with a policy of type "vault":
   snapmirror
      break -delete-snapshots
   ```

```
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. Depois de atender aos requisitos da verificação Reverter, "Reverter ONTAP"consulte .

Remova uma configuração de sincronização ativa do SnapMirror

Se você não precisar mais de proteção síncrona de rto SnapMirror zero, poderá excluir sua relação de sincronização ativa do SnapMirror.

Remova uma configuração assimétrica

- Antes de excluir a relação de sincronização ativa do SnapMirror, todos os LUNs no cluster de destino devem ser não mapeados.
- Depois que os LUNs não são mapeados e o host é reconfigurado, o destino SCSI notifica os hosts de que o inventário LUN foi alterado. Os LUNs existentes nos volumes secundários de rto zero mudam para refletir uma nova identidade depois que a relação rto zero é excluída. Os hosts descobrem os LUNs de volume secundário como novos LUNs que não têm relação com os LUNs de volume de origem.
- Os volumes secundários permanecem volumes DP depois que a relação é excluída. Você pode emitir o `snapmirror break` comando para convertê-los para ler/escrever.
- A exclusão do relacionamento não é permitida no estado de failover quando o relacionamento não é revertido.

Passos

1. No cluster secundário, remova a relação do grupo de consistência de sincronização ativa do SnapMirror entre o ponto final de origem e o ponto de extremidade de destino:

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. No cluster primário, solte a relação de grupo de consistência e as cópias Snapshot criadas para a relação:

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Execute uma nova verificação do host para atualizar o inventário LUN.
4. A partir do ONTAP 9.10,1, a exclusão da relação SnapMirror não exclui o grupo de consistência. Se você quiser excluir o grupo de consistência, use o Gerenciador do sistema ou a API REST do ONTAP. Consulte Excluir um grupo de consistência para obter mais informações.

Remover uma configuração ativo-ativo simétrica

Você pode remover uma configuração simétrica usando o Gerenciador do sistema ou a CLI do ONTAP. Em ambas as interfaces, existem diferentes etapas para configurações uniformes e não uniformes.

System Manager

Passos para uma configuração uniforme

1. No site principal, remova os hosts remotos do igrop e encerre a replicação.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo que você deseja modificar e, em seguida, **Editar**.
   c. Remova o iniciador remoto e encerre a replicação do igroup. Selecione **Guardar**.
2. No site secundário, exclua a relação replicada desmapeando os LUNs.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo com o relacionamento SnapMirror e, em seguida, **Excluir**.
   c. Na caixa de diálogo, selecione a caixa **Unmap the Associated LUNs** (Anular mapeamento dos LUNs associados) e **Delete** (Excluir).
   d. Navegue até **proteção** > **relacionamentos**.
   e. Selecione a relação de sincronização ativa do SnapMirror e, em seguida, **Liberação** para excluir as relações.

Passos para uma configuração não uniforme

1. No site principal, remova os hosts remotos do igrop e encerre a replicação.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo que você deseja modificar e, em seguida, **Editar**.
   c. Remova o iniciador remoto e encerre a replicação do igroup. Selecione **Guardar**.
2. No local secundário, remova a relação de sincronização ativa do SnapMirror.
   a. Navegue até **proteção** > **relacionamentos**.
   b. Selecione a relação de sincronização ativa do SnapMirror e, em seguida, **Liberação** para excluir as relações.

CLI

Passos para uma configuração uniforme

1. Mova todos os workloads de VM para o host local para o cluster de origem da sincronização ativa do SnapMirror.
2. No cluster de origem, remova os iniciadores do iggroup e modifique a configuração do iggroup para encerrar a replicação do iggroup.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. No site secundário, exclua o mapeamento de LUN e remova a configuração do igroup:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. No site secundário, exclua a relação de sincronização ativa do SnapMirror.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. No local principal, libere a relação de sincronização ativa do SnapMirror do local principal.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Redescubra os caminhos para verificar se apenas o caminho local está disponível para o host.

Passos para uma configuração não uniforme

1. Mova todos os workloads de VM para o host local para o cluster de origem da sincronização ativa do SnapMirror.
2. No cluster de origem, remova os iniciadores do igrop.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. No site secundário, exclua o mapeamento de LUN e remova a configuração do igroup:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. No site secundário, exclua a relação de sincronização ativa do SnapMirror.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. No local principal, libere a relação de sincronização ativa do SnapMirror do local principal.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Redescubra os caminhos para verificar se apenas o caminho local está disponível para o host.

Remova o Mediador ONTAP

Se você quiser remover uma configuração existente do ONTAP Mediator dos clusters do ONTAP, use o `snapmirror mediator remove` comando.

Passos

1. Remover o Mediador ONTAP:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
cluster_xyz
```

Solucionar problemas

A operação de exclusão do SnapMirror falha no estado takover

Problema:

Quando o ONTAP 9.9,1 é instalado em um cluster, a execução do `snapmirror delete` comando falha quando uma relação de grupo de consistência de sincronização

ativa do SnapMirror está no estado de aquisição.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solução

Quando os nós de uma relação de sincronização ativa do SnapMirror estiverem no estado de aquisição, execute a operação de exclusão e liberação do SnapMirror com a opção "-force" definida como verdadeiro.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Falha ao criar uma relação SnapMirror e inicializar um grupo de consistência

Problema:

Falha na criação da relação e inicialização do grupo de consistência do SnapMirror.

Solução:

Certifique-se de que não excedeu o limite de grupos de consistência por cluster. Os limites do grupo de consistência na sincronização ativa do SnapMirror são independentes da plataforma e diferem com base na versão do ONTAP. Consulte "Limites de objetos" para obter orientações específicas para a sua versão do ONTAP.

Erro:

Se o grupo de consistência estiver bloqueado na inicialização, verifique o status das inicializações do grupo de consistência com a API REST do ONTAP, o Gerenciador de sistema ou o comando `sn show -expand`.

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

Solução:

Se os grupos de consistência não iniciarem, remova a relação de sincronização ativa do SnapMirror, exclua o grupo de consistência e, em seguida, recrie a relação e inicialize-a. Este fluxo de trabalho difere dependendo da versão do ONTAP que você está usando.

Se estiver a utilizar o ONTAP 9.9,1	Se estiver a utilizar o ONTAP 9.10,1 ou posterior

1. "Remova a configuração de sincronização ativa do SnapMirror" 2. "Crie uma relação de grupo de consistência e, em seguida, inicialize a relação de grupo de consistência"	1. Em **proteção > relacionamentos**, encontre a relação de sincronização ativa do SnapMirror no grupo consistência. Selecione e, em seguida, **Excluir** para remover a relação de sincronização ativa do SnapMirror. 2. "Exclua o grupo de consistência" 3. "Configure o grupo de consistência"

Failover planejado sem êxito

Problema:

Depois de executar o `snapmirror failover start` comando, a saída para o `snapmirror failover show` comando exibe uma mensagem indica que uma operação sem interrupções está em andamento.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                              08:35:04
08:35:04
```

Causa:

Um failover planejado não pode começar quando uma operação sem interrupções estiver em andamento, incluindo movimentação de volume, realocação de agregado e failover de storage.

Solução:

Aguarde até que a operação sem interrupções seja concluída e tente a operação de failover novamente.

O status do quórum do mediador ONTAP não é alcançável ou falso

Problema:

Depois de executar o `snapmirror failover start` comando, a saída para `snapmirror failover show` o comando exibe uma mensagem indicando que o Mediador ONTAP não está configurado.

"Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Causa:

O mediador não está configurado ou há problemas de conetividade de rede.

Solução:

Se o Mediador do ONTAP não estiver configurado, você deverá configurar o Mediador do ONTAP antes de estabelecer uma relação de sincronização ativa do SnapMirror. Corrija quaisquer problemas de conetividade de rede. Certifique-se de que o Mediador esteja conetado e o status do quórum seja verdadeiro no local de origem e destino usando o comando SnapMirror Mediator show. Para obter mais informações, "Configure o Mediador ONTAP"consulte .

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Failover não planejado automático não acionado no local B.

Problema:

Uma falha no local A não aciona um failover não planejado no local B..

Causa possível n.o 1:

O Mediador ONTAP não está configurado. Para determinar se esta é a causa, emita o `snapmirror mediator show` comando no cluster do local B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Este exemplo indica que o Mediador ONTAP não está configurado no local B.

Solução:

Certifique-se de que o ONTAP Mediator esteja configurado em ambos os clusters, de que o status esteja conetado e de que o quórum esteja definido como verdadeiro.

Causa possível n.o 2:

O grupo de consistência do SnapMirror está fora de sincronia. Para determinar se essa é a causa, exiba o log de eventos para ver se o grupo de consistência estava em sincronia durante o momento em que ocorreu a

falha do Site A.

```
cluster::*> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solução:

Conclua as etapas a seguir para executar um failover forçado no local B.

1. Desmapear todos os LUNs pertencentes ao grupo de consistência do Site B..
2. Exclua a relação do grupo de consistência do SnapMirror usando a `force` opção.
3. Digite o `snapmirror break` comando nos volumes constituintes do grupo de consistência para converter volumes de DP para R/W, para habilitar e/S do local B.
4. Inicialize os nós do local A para criar uma relação rto zero do local B para o local A..
5. Libere o grupo de consistência com `relationship-info-only` o no local A para reter a cópia Snapshot comum e desmapear os LUNs pertencentes ao grupo de consistência.
6. Converta volumes no local A de R/W para DP configurando uma relação de nível de volume usando a política de sincronização ou a política de sincronização.
7. Emita o `snapmirror resync` para sincronizar as relações.
8. Exclua os relacionamentos do SnapMirror com a política de sincronização no local A..
9. Liberar as relações SnapMirror com a política de sincronização usando `relationship-info-only true` no local B..
10. Crie uma relação de grupo de consistência do local B para o local A..
11. Execute uma ressincronização do grupo de consistência no Site A e verifique se o grupo de consistência está em sincronia.
12. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

Link entre o Site B e o Mediator Down e o Site A Down

Para verificar a conexão do Mediador ONTAP, use o `snapmirror mediator show` comando. Se o status da conexão for inalcançável e o local B não conseguir alcançar o local A, você terá uma saída semelhante à abaixo. Siga as etapas da solução para restaurar a conexão

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solução

Forçar um failover para habilitar a e/S do local B e, em seguida, estabelecer uma relação rto zero do local B para o local A. conclua as etapas a seguir para executar um failover forçado no local B.

1. Desmapear todos os LUNs pertencentes ao grupo de consistência do Site B..
2. Exclua a relação do grupo de consistência do SnapMirror usando a opção forçar.
3. Digite o comando SnapMirror Break (`snapmirror break -destination_path` *svm*`:_volume_`) nos volumes constituintes do grupo de consistência para converter volumes de DP para RW, para ativar e/S do local B.

   Você deve emitir o comando SnapMirror Break para cada relacionamento no grupo consistência. Por exemplo, se houver três volumes no grupo consistência, você emitirá o comando para cada volume.

4. Inicialize os nós do local A para criar uma relação rto zero do local B para o local A..

5. Libere o grupo de consistência com somente informações de relacionamento no Site A para reter a cópia Snapshot comum e desmapear os LUNs pertencentes ao grupo de consistência.
6. Converta volumes no local A de RW para DP configurando uma relação de nível de volume usando a política de sincronização ou a política de sincronização.
7. Emita o `snapmirror resync` comando para sincronizar as relações.
8. Excluir as relações SnapMirror com a política de sincronização no local A..
9. Libere as relações do SnapMirror com a política de sincronização usando somente relacionamento verdadeiro no local B..
10. Crie uma relação de grupo de consistência entre o local B e o local A..
11. No cluster de origem, ressincronize o grupo de consistência. Verifique se o estado do grupo de consistência está em sincronia.
12. Reescaneie os caminhos de e/S LUN do host para restaurar todos os caminhos para os LUNs.

Ligação entre o Site A e o Mediator Down e o Site B Down

Ao usar a sincronização ativa do SnapMirror, você pode perder a conetividade entre o Mediador do ONTAP ou seus clusters com peering. É possível diagnosticar o problema verificando o status de conexão, disponibilidade e consenso das diferentes partes da relação de sincronização ativa do SnapMirror e, em seguida, retomando a conexão com força.

O que verificar	Comando CLI	Indicador
Mediador do Site A	`snapmirror mediator show`	O estado da ligação é apresentado como `unreachable`
Conetividade do local B.	`cluster peer show`	A disponibilidade é apresentada como `unavailable`
Status de consenso do volume de sincronização ativa do SnapMirror	`volume show` *`volume_name`* `-fields smbc-consensus`	O `sm-bc consensus` campo é exibido `Awaiting-consensus`

Para obter informações adicionais sobre como diagnosticar e resolver este problema, consulte o artigo da base de dados de Conhecimento "Ligação entre o local A e o Mediador para baixo e o local B para baixo ao utilizar a sincronização ativa do SnapMirror".

A operação de exclusão do SnapMirror falha quando a vedação está definida no volume de destino

Problema:

A operação de exclusão do SnapMirror falha quando qualquer um dos volumes de destino tiver uma vedação de redirecionamento definida.

Solução

Executar as seguintes operações para tentar novamente o redirecionamento e remover a cerca do volume de destino.

- Ressincronização do SnapMirror
- Atualização do SnapMirror

Operação de movimentação de volume emperrada quando o primário está para baixo

Problema:

Uma operação de movimentação de volume fica presa indefinidamente no estado de transição adiada quando o local principal está inativo em uma relação de sincronização ativa do SnapMirror. Quando o local principal está inativo, o local secundário executa um failover não planejado automático (AUFO). Quando uma operação de movimentação de volume está em andamento quando o AUFO é acionado, o movimento de volume fica preso.

Solução:

Abortar a instância de movimentação de volume que está emperrada e reiniciar a operação de movimentação de volume.

A versão do SnapMirror falha quando não é possível excluir a cópia Snapshot

Problema:

A operação de lançamento do SnapMirror falha quando a cópia Snapshot não pode ser excluída.

Solução:

A cópia Snapshot contém uma tag transitória. Use o `snapshot delete` comando com a `-ignore-owners` opção para remover a cópia Snapshot transitória.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Tente novamente o `snapmirror release` comando.

Referência de movimentação de volume a cópia Snapshot é exibida como a mais recente

Problema:

Depois de executar uma operação de movimentação de volume em um volume de grupo de consistência, a cópia Snapshot de referência de movimentação de volume pode ser exibida incorretamente como a mais recente para a relação SnapMirror.

Você pode exibir a cópia Snapshot mais recente com o seguinte comando:

```
snapmirror show -fields newest-snapshot status -expand
```

Solução:

Execute manualmente uma `snapmirror resync` operação de ressincronização automática seguinte após a conclusão da operação de movimentação de volume.

Serviço de mediador para sincronização ativa do MetroCluster e do SnapMirror

Visão geral do Mediador ONTAP

O Mediador ONTAP fornece várias funções para os recursos do ONTAP:

- Fornece um armazenamento persistente e vedado para metadados de HA.
- Serve como um proxy ping para vivacidade do controlador.
- Fornece funcionalidade de consulta de integridade do nó síncrono para auxiliar na determinação do quórum.

O Mediador ONTAP fornece dois serviços adicionais de systemctl:

- **`ontap_mediator.service`**

  Mantém o servidor REST APIs para gerenciar as relações ONAP.

- **`mediator-scst.service`**

  Controla o arranque e o encerramento do módulo iSCSI (SCST).

Ferramentas fornecidas para o administrador do sistema

Ferramentas fornecidas para o administrador do sistema:

- **`/usr/local/bin/mediator_change_password`**

  Define uma nova senha da API quando o nome de usuário e a senha atuais da API são fornecidos.

- **`/usr/local/bin/mediator_change_user`**

  Define um novo nome de usuário da API quando o nome de usuário e a senha atuais da API são fornecidos.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Gera um arquivo tgz local contendo todas as informações úteis de suporte necessárias para a comunicação com o suporte ao cliente NetApp. Isso inclui configuração de aplicativos, logs e algumas informações do sistema. Os pacotes são gerados no disco local e podem ser transferidos manualmente, conforme necessário. Local de armazenamento: /Opt/NetApp/data/support_bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Remove o pacote do Mediador ONTAP e o módulo do kernel SCST. Isso inclui todas as configurações, Registros e dados de caixa de correio.

- **`/usr/local/bin/mediator_unlock_user`**

  Libera um bloqueio na conta de usuário da API se o limite de tentativas de autenticação foi atingido. Este recurso é usado para evitar a derivação de senha de força bruta. Ele solicita ao usuário o nome de usuário e a senha corretos.

- **`/usr/local/bin/mediator_add_user`**

  (Suporte somente) usado para adicionar o usuário da API após a instalação.

Notas especiais

O Mediador ONTAP depende do SCST para fornecer iSCSI (http://scst.sourceforge.net/index.htmlconsulte). Este pacote é um módulo do kernel que é compilado durante a instalação especificamente para o kernel. Qualquer atualização do kernel pode exigir que o SCST seja reinstalado. Alternativamente, desinstale e reinstale o Mediador ONTAP e, em seguida, reconfigure a relação ONTAP.

Todas as atualizações do kernel do sistema operacional do servidor devem ser coordenadas com uma janela de manutenção no ONTAP.

O que há de novo com o Mediador ONTAP

Novas melhorias para o Mediador ONTAP são fornecidas com cada versão. Eis as novidades.

Melhorias

Para obter informações sobre a versão do SCST, consulte Matriz de suporte SCST.

ONTAP versão mediadora	Melhorias
1,9	• Suporte para RHEL: ◦ Compatível: 8,4, 8,5, 8,6, 8,7, 8,9, 9,1 e 9,3. ◦ Recomendado: 8,8, 8,10, 9,0, 9,2, 9,4 e 9,5. • Suporte para Rocky Linux 8 e 9. • Suporte FIPS para RHEL e Rocky Linux. • Melhorias de desempenho adicionadas para maior escalabilidade. • Nomes de arquivo aprimorados para simplificar a configuração de certificados assinados pela PKI.
1,8	• Suporte para RHEL 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4. • Suporte para Rocky Linux 8 e 9.
1,7	• Suporte para RHEL 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3. • Suporte para Rocky Linux 8 e 9. • Suporte para dados SAN (Nome alternativo do assunto) em certificados autoassinados e certificados assinados por terceiros.
1,6	• Atualizações do Python 3,9. • Suporte para RHEL 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1 e 9,2. • Suporte para Rocky Linux 8 e 9. • Suporte descontinuado para RHEL 7.x / CentOS todas as versões.

1,5	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9. • Inclui avisos de depreciação para RHEL 7.x / CentOS 7.x. • Otimiza a velocidade para sistemas de sincronização ativos SnapMirror de maior escala. • Assinatura de código criptográfico adicionada ao instalador.
1,4	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9. • Adicionado suporte para o Secure Boot (SB) de firmware baseado em UFEI.
1,3	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9.
1,2	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9. • Suporte para caixas de correio HTTPS. • Para uso com ONTAP 9.8z AUSO MCC-IP e SnapMirror ative Sync Zrto.
1,1	• Suporte para RHEL 7,6 e 8,0. • Suporte para CentOS 7,6. • Elimina dependências Perl.
1,0	• Suporte para caixas de correio iSCSI. • Para uso com AUSO de MCC-IP ONTAP 9.7. • Suporte para RHEL/CentOS 7,6.

Matriz de suporte de SO

SO para Mediador ONTAP	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
7,6	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Sim	Sim (apenas RHEL)
7,7	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Não	Não
7,8	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Não	Não

7,9	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Compatível	Não	Não
RHEL 8,0	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Sim	Não
RHEL 8,1	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Não	Não
RHEL 8,2	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Não	Não	Não
RHEL 8,3	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Não	Não	Não
RHEL 8,4	Compatível	Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Não
RHEL 8,5	Compatível	Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Não
RHEL 8,6	Compatível	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 8,7	Compatível	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 8,8	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 8,9	Compatível	Sim	Sim	Não	Não	Não	Não	Não	Não	Não
RHEL 8,10	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
RHEL 9,0	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 9,1	Compatível	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 9,2	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 9,3	Compatível	Sim	Sim	Não	Não	Não	Não	Não	Não	Não

RHEL 9,4	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
RHEL 9,5	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não
CentOS 8 e stream	Não	Não	Não	Não	Não	Não	Não	N/A.	N/A.	N/A.
Rocky Linux 8	Sim	Sim	Sim	Sim	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.
Rocky Linux 9	Sim	Sim	Sim	Sim	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.

- OS refere-se a versões RedHat e CentOS, a menos que especificado de outra forma.
- "Sim" significa que o SO é recomendado para a instalação do Mediador ONTAP e é totalmente compatível e suportado.
- "Não" significa que o SO e o Mediador ONTAP não são compatíveis.
- "Compatível" significa que o RHEL não suporta mais esta versão, mas o Mediador ONTAP ainda pode ser instalado.
- O CentOS 8 foi removido para todas as versões devido à sua ramificação. O CentOS Stream foi considerado como um sistema operacional de destino de produção adequado. Nenhum suporte está planejado.
- O ONTAP Mediator 1,5 foi a última versão suportada para sistemas operacionais de ramificação RHEL 7.x.
- O ONTAP Mediator 1,6 adiciona suporte para Linux 8 e 9.

Matriz de suporte SCST

A tabela a seguir mostra a versão SCST suportada para cada versão do ONTAP Mediator.

ONTAP versão mediadora	Versão SCST suportada
ONTAP Mediador 1,9	scst-3,8.0.tar.bz2
ONTAP Mediador 1,8	scst-3,8.0.tar.bz2
ONTAP Mediador 1,7	scst-3,7.0.tar.bz2
ONTAP Mediador 1,6	scst-3,7.0.tar.bz2
ONTAP Mediador 1,5	scst-3,6.0.tar.bz2
ONTAP Mediador 1,4	scst-3,6.0.tar.bz2
ONTAP Mediador 1,3	scst-3,5.0.tar.bz2
ONTAP Mediador 1,2	scst-3,4.0.tar.bz2
ONTAP Mediador 1,1	scst-3,4.0.tar.bz2

ONTAP versão mediadora	Versão SCST suportada
ONTAP Mediador 1,0	scst-3,3.0.tar.bz2

Instalar ou atualizar

Prepare-se para instalar ou atualizar o serviço do Mediador ONTAP

Para instalar o serviço ONTAP Mediator, você deve garantir que todos os pré-requisitos sejam atendidos, buscar o pacote de instalação e executar o instalador no host. Este procedimento é utilizado para uma instalação ou atualização de uma instalação existente.

- A partir do ONTAP 9.7, você pode usar qualquer versão do Mediador ONTAP para monitorar uma configuração IP do MetroCluster.
- A partir do ONTAP 9.8, você pode usar qualquer versão do ONTAP Mediator para monitorar uma relação de sincronização ativa do SnapMirror.

Considerações sobre instalação e atualização

Reveja as seguintes considerações antes de atualizar ou instalar o Mediador ONTAP.

> O ONTAP Mediator 1,8 e versões anteriores não é compatível com o modo FIPS e impedirá que ele seja instalado com sucesso. Você pode verificar se o modo FIPS está ativado usando o `fips-mode-setup --check` comando. Você pode desativar o modo FIPS usando o `fips-modesetup --disable` comando. Reinicie após desativar o modo FIPS para instalar com êxito o ONTAP Mediator 1,8 ou anterior.

- Você deve atualizar o Mediador ONTAP para a versão mais recente disponível. As versões anteriores do ONTAP Mediator permanecem retrocompatíveis com todas as versões do ONTAP, mas as versões recentes incluem patches de segurança para todos os elementos de terceiros.
- Quando você atualiza para uma nova versão do ONTAP Mediator, o instalador atualiza automaticamente para a versão SCST recomendada, a menos que uma versão superior esteja disponível. Para obter instruções sobre como instalar manualmente uma versão SCST mais alta, "Gerencie o serviço Mediator"consulte . Para versões suportadas, consulte "Matriz de suporte SCST".

> Se ocorrer uma falha de instalação, talvez seja necessário atualizar para uma versão posterior do ONTAP Mediator.

- Se você instalar o `yum-utils` pacote, você pode usar o `needs-restarting` comando.

Requisitos da OS

Seu sistema operacional deve atender aos seguintes requisitos:

- instalação física de 64 bits ou máquina virtual
- 8 GB DE RAM
- 1 GB de espaço em disco (usado para instalação de aplicativos, logs de servidor e banco de dados)
- Usuário: Acesso root

A tabela a seguir mostra os sistemas operacionais suportados para cada versão do ONTAP Mediator.

ONTAP versão mediadora	Versões Linux suportadas
1,9	• Red Hat Enterprise Linux ◦ Compatível: 8,4, 8,5, 8,6, 8,7, 8,9, 9,1 e 9,3 1 ◦ Recomendado: 8,8, 8,10, 9,0, 9,2, 9,4 e 9,5 • Rocky Linux 8 e 9
1,8	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4 • Rocky Linux 8 e 9
1,7	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Rocky Linux 8 e 9
1,6	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2 • Rocky Linux 8 e 9
1,5	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,4	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,3	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3 • CentOS: 7,6, 7,7, 7,8, 7,9
1,2	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1 • CentOS: 7,6, 7,7, 7,8, 7,9

1. Compatível significa que o RHEL não suporta mais esta versão, mas o ONTAP Mediator ainda pode ser instalado.

Considerações de atualização DO SO e compatibilidade do kernel

- Todos os pacotes de biblioteca, exceto o kernel, podem ser atualizados com segurança, mas podem exigir uma reinicialização para aplicar as alterações no aplicativo do Mediador ONTAP. Uma janela de serviço é recomendada quando uma reinicialização é necessária.
- Você deve manter o kernel do sistema operacional atualizado. O núcleo do kernel pode ser atualizado para uma versão listada como suportada no "Matriz de versão do Mediador ONTAP". Uma reinicialização é obrigatória, então você deve Planejar uma janela de manutenção para a interrupção.
  - Você deve desinstalar o módulo do kernel SCST antes de reiniciar e depois reinstalá-lo depois.
  - Você deve ter uma versão suportada do SCST pronta para reinstalar antes de iniciar a atualização do sistema operacional do kernel.

- A versão do kernel deve corresponder à versão do sistema operacional.
- A atualização para um kernel além da versão de SO suportada para a versão específica do Mediador ONTAP não é suportada. (Isso provavelmente indica que o módulo SCST testado não irá compilar).

Registre uma chave de segurança quando o UEFI Secure Boot estiver ativado

Para instalar o Mediador ONTAP com inicialização segura UEFI ativada, você deve Registrar uma chave de segurança antes que o serviço possa ser iniciado. A chave é gerada durante a etapa de compilação da instalação do SCST e salva como um par de chaves público-privado em sua máquina. Use o `mokutil` utilitário para adicionar a chave pública como uma chave de proprietário de máquina (MOK) ao firmware UEFI, permitindo que o sistema confie e carregue o módulo assinado. Salve a `mokutil` senha em um local seguro, pois isso é necessário ao reiniciar seu sistema para ativar o MOK.

Para determinar se o sistema está habilitado para UEFI e o Secure Boot está ativado, execute as seguintes etapas:

Passos

1. Se `mokutil` não estiver instalado, execute o seguinte comando:

   ```
   yum install mokutil
   ```

2. Verifique se o UEFI Secure Boot está ativado no seu sistema:

   ```
   mokutil --sb-state
   ```

   Os resultados indicam se o UEFI Secure Boot está ativado neste sistema.

   - Você é solicitado a criar uma senha que você deve armazenar em um local seguro. Você precisará dessa senha para ativar a chave no Gerenciador de Inicialização UEFI.
   - O ONTAP Mediator 1.2.0 e versões anteriores não suportam este modo.

3. Adicione a chave pública à lista MOK:

   ```
   mokutil --import
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
   r
   ```

   Você pode deixar a chave privada em seu local padrão ou movê-la para um local seguro. No entanto, a chave pública deve ser mantida em seu local existente para uso pelo Gerenciador de Inicialização. Para obter mais informações, consulte o seguinte arquivo de assinatura README.module:

   ```
   [root@hostname ~]# ls
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
   README.module-signing scst_module_key.der scst_module_key.priv
   ```

4. Reinicie o host e use o Gerenciador de Inicialização UEFI do dispositivo para aprovar o novo MOK. Você precisará da senha fornecida para o `mokutil` passo 2.

Desative o arranque seguro UEFI

Você também pode optar por desativar a Inicialização segura UEFI antes de instalar o ONTAP Mediator.

Passos

1. Nas configurações do BIOS da máquina física, desative a opção "UEFI Secure Boot".
2. Nas configurações da VMware para a VM, desative a opção "Início seguro" para o vSphere 6.x ou a opção "Inicialização segura" para o vSphere 7.x.

Atualize o sistema operacional host e, em seguida, o Mediador ONTAP

Para atualizar o sistema operacional do host para o ONTAP Mediator para uma versão posterior, você deve primeiro desinstalar o ONTAP Mediator.

Antes de começar

As melhores práticas para instalar o Red Hat Enterprise Linux ou Rocky Linux e os repositórios associados em seu sistema estão listados abaixo. Os sistemas instalados ou configurados de forma diferente podem exigir etapas adicionais.

- Você deve instalar o Red Hat Enterprise Linux ou Rocky Linux de acordo com as melhores práticas da Red Hat. Devido ao suporte de fim de vida para versões CentOS 8.x, não são recomendadas versões compatíveis do CentOS 8.x.
- Durante a instalação do serviço ONTAP Mediator no Red Hat Enterprise Linux ou Rocky Linux, o sistema deve ter acesso ao repositório apropriado para que o programa de instalação possa acessar e instalar todas as dependências de software necessárias.
- Para que o instalador do yum encontre software dependente nos repositórios Red Hat Enterprise Linux, você deve ter registrado o sistema durante a instalação do Red Hat Enterprise Linux ou depois usando uma assinatura válida do Red Hat.

  Consulte a documentação da Red Hat para obter informações sobre o Red Hat Subscription Manager.

- As seguintes portas devem ser não utilizadas e disponíveis para o Mediador:
  - 31784
  - 3260
- Se estiver a utilizar uma firewall de terceiros: Consulte "Requisitos de firewall para o ONTAP Mediator"
- Se o host Linux estiver em um local sem acesso à internet, você deve garantir que os pacotes necessários estejam disponíveis em um repositório local.

  Se você estiver usando o Link Aggregation Control Protocol (LACP) em um ambiente Linux, você deve configurar corretamente o kernel e certificar-se de que o `sysctl net.ipv4.conf.all.arp_ignore` está definido como "2".

O que você vai precisar

Os seguintes pacotes são exigidos pelo serviço Mediador ONTAP:

Todas as versões RHEL/CentOS	Pacotes adicionais para RHEL 8.x / Rocky Linux 8	Pacotes adicionais para RHEL 9.x / Rocky Linux 9

• openssl • openssl-devel • kernel-devel (uname -r) • gcc • marca • libselinux-utils • patch • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeMaker • efibootmgr • mokutil	• python3 pip • elfutils-libelf-devel • policycoreutils-python-utils • redhat-lsb-core • python39 • python39-nível	• python3 pip • elfutils-libelf-devel • policycoreutils-python-utils • python3 • python3-nível

O pacote de instalação Mediator é um arquivo tar compactado auto-extraível que inclui:

- Um arquivo RPM contendo todas as dependências que não podem ser obtidas do repositório da versão suportada.
- Um script de instalação.

Recomenda-se uma certificação SSL válida.

Sobre esta tarefa

Quando você atualiza o sistema operacional do host para o ONTAP Mediator para uma versão maior posterior (por exemplo, de 7.x para 8.x) usando a ferramenta leapp-upgrade, você deve desinstalar o ONTAP Mediator porque a ferramenta tenta detetar novas versões de quaisquer RPMs instalados nos repositórios que estão registrados no sistema.

Como um arquivo .rpm foi instalado como parte do instalador do ONTAP Mediator, ele está incluído nessa pesquisa. No entanto, como o arquivo .rpm foi descompactado como parte do instalador e não baixado de um repositório registrado, não é possível encontrar uma atualização. Neste caso, a ferramenta leapp-upgrade desinstala o pacote.

Para preservar os arquivos de log, que serão usados para triagem de casos de suporte, você deve fazer backup dos arquivos antes de fazer uma atualização do sistema operacional e restaurá-los após uma reinstalação do pacote do ONTAP Mediator. Como o Mediador ONTAP está sendo reinstalado, todos os clusters ONTAP que estão conetados a ele precisarão ser reconetados após a nova instalação.

As etapas a seguir devem ser executadas em ordem. Imediatamente após reinstalar o ONTAP Mediator, você deve parar o serviço ONTAP_Mediator, substituir os arquivos de log e reiniciar o serviço. Isso garantirá que os logs não sejam perdidos.

Passos

1. Faça uma cópia de segurança dos ficheiros de registo.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Execute a atualização com a ferramenta leapp-upgrade.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Reinstale o Mediador ONTAP.

> Execute o resto das etapas imediatamente após reinstalar o ONTAP Mediator para evitar a perda de arquivos de log.

```
[rootmediator-host ~]# ontap-mediator-1.9.0/ontap-mediator-1.9.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Pare o serviço ONTAP_Mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Substitua os arquivos de log.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Inicie o serviço ONTAP_Mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Reconecte todos os clusters do ONTAP ao mediador do ONTAP atualizado

Procedimento para MetroCluster sobre IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

Procedimento para sincronização ativa do SnapMirror

Para a sincronização ativa do SnapMirror, se você instalou o certificado TLS fora do diretório /opt/NetApp, então você não precisará reinstalá-lo. Se você estava usando o certificado autoassinado gerado padrão ou colocou seu certificado personalizado no diretório /opt/NetApp, então você deve fazer o backup e restaurá-lo.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA                        server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
```

```
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

Ativar o acesso aos repositórios

Você deve habilitar o acesso aos repositórios para que o ONTAP Mediator possa acessar os pacotes necessários durante o processo de instalação

Passos

1. Determine quais repositórios devem ser acessados, como mostrado na tabela a seguir:

Se o seu sistema operativo for…	Você deve fornecer acesso a esses repositórios…
RHEL 7.x	• rhel-7-server-optional-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
CentOS 7.x	• C7,6.1810 - repositório base
Rocky Linux 8	• appstream • base
Rocky Linux 9	• appstream • base

2. Use um dos procedimentos a seguir para habilitar o acesso aos repositórios listados acima para que o ONTAP Mediator possa acessar os pacotes necessários durante o processo de instalação.

Se o Mediador ONTAP tiver dependências nos módulos Python presentes nos repositórios "extras" e "opcionais", talvez seja necessário acessar os `rhel-X-for-x86_64-extras-rpms` arquivos e. `rhel-X-for-x86_64-optional-rpms`

Procedimento para o sistema operacional RHEL 7.x.

Use este procedimento se seu sistema operacional for **RHEL 7.x** para habilitar o acesso aos repositórios:

Passos

1. Assine o repositório necessário:

   ```
   subscription-manager repos --enable rhel-7-server-optional-rpms
   ```

   O exemplo a seguir mostra a execução deste comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-7-
   server-optional-rpms
   Repository 'rhel-7-server-optional-rpms' is enabled for this system.
   ```

2. Executar o `yum repolist` comando.

   O exemplo a seguir mostra a execução desse comando. O repositório "rhel-7-server-optional-rpms" deve aparecer na lista.

   ```
   [root@localhost ~]# yum repolist
   Loaded plugins: product-id, search-disabled-repos, subscription-
   manager
   rhel-7-server-optional-rpms | 3.2 kB  00:00:00
   rhel-7-server-rpms | 3.5 kB  00:00:00
   (1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
   |  26 kB  00:00:00
   (2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
   | 2.5 MB  00:00:00
   (3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
   | 8.3 MB  00:00:01
   repo id                                    repo name
   status
   rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
   Linux 7 Server - Optional (RPMs)   19,447
   rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
   Linux 7 Server (RPMs)              26,758
   repolist: 46,205
   [root@localhost ~]#
   ```

Procedimento para o sistema operacional RHEL 8.x.

Use este procedimento se seu sistema operacional for **RHEL 8.x** para habilitar o acesso aos repositórios:

Passos

1. Assine o repositório necessário:

   ```
   subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms

   subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
   ```

   O exemplo a seguir mostra a execução deste comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-baseos-rpms
   Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-appstream-rpms
   Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Executar o `yum repolist` comando.

   Os repositórios recém-inscritos devem aparecer na lista.

Procedimento para o sistema operacional RHEL 9.x.

Use este procedimento se seu sistema operacional for **RHEL 9.x** para habilitar o acesso aos repositórios:

Passos

1. Assine o repositório necessário:

   ```
   subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms

   subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
   ```

   O exemplo a seguir mostra a execução deste comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-baseos-rpms
   Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-appstream-rpms
   Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Executar o `yum repolist` comando.

   Os repositórios recém-inscritos devem aparecer na lista.

Procedimento para o sistema operacional CentOS 7.x.

Use este procedimento se o sistema operacional for **CentOS 7.x** para habilitar o acesso aos repositórios:

> Os exemplos a seguir mostram um repositório para o CentOS 7,6 e podem não funcionar para outras versões do CentOS. Use o repositório base para sua versão do CentOS.

Passos

1. Adicione o repositório C7,6.1810 - base. O repositório do C7,6.1810 - base Vault contém o pacote "kernel-devel" necessário para o ONTAP Mediator.
2. Adicione as seguintes linhas ao /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Executar o `yum repolist` comando.

   O exemplo a seguir mostra a execução desse comando. O repositório CentOS-7.6.1810 - base deve aparecer na lista.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Procedimento para sistemas operacionais Rocky Linux 8 ou 9

Use este procedimento se seu sistema operacional for **Rocky Linux 8** ou **Rocky Linux 9** para habilitar o acesso aos repositórios:

Passos

1. Assine os repositórios necessários:

   ```
   dnf config-manager --set-enabled baseos

   dnf config-manager --set-enabled appstream
   ```

2. Execute uma `clean` operação:

   ```
   dnf clean all
   ```

3. Verifique a lista de repositórios:

   ```
   dnf repolist
   ```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

Baixe o pacote de instalação do Mediator

Faça o download do pacote de instalação do Mediator como parte do processo de instalação.

Passos

1. Faça o download do pacote de instalação do Mediador na página do Mediador do ONTAP.

"Página de download do ONTAP Mediator"

2. Confirme se o pacote de instalação do Mediator está no diretório de trabalho atual:

```
[root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.9.0.tgz
```

```
ontap-mediator-1.9.0.tgz
```

> Para o ONTAP Mediator versões 1,4 e anteriores, o instalador é `ontap-mediator` chamado .

Se você estiver em um local sem acesso à internet, você deve garantir que o instalador tenha acesso aos pacotes necessários.

3. Se necessário, mova o pacote de instalação do Mediator do diretório de download para o diretório de instalação no host do Linux Mediator.
4. Descompacte o pacote de instalação:

`tar xvfz ontap-mediator-1.9.0.tgz`

```
ontap-mediator-1.9.0/
ontap-mediator-1.9.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/ONTAP-Mediator-production.pub
ontap-mediator-1.9.0/ontap-mediator-1.9.0
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig
```

Verifique a assinatura do código do ONTAP Mediator

Você deve verificar a assinatura do código do ONTAP Mediator antes de instalar o pacote de instalação do ONTAP Mediator.

Antes de começar

Antes de verificar a assinatura do código do ONTAP Mediator, o sistema deve atender aos seguintes requisitos.

- openssl versões 1.0.2 a 3,0 para verificação básica
- openssl versão 1.1.0 ou posterior para operações de Time Stamping Authority (TSA)
- Acesso público à Internet para verificação OCSP

Os seguintes arquivos estão incluídos no pacote de download:

Ficheiro	Descrição
`ONTAP-Mediator-production.pub`	A chave pública usada para verificar a assinatura
`csc-prod-chain-ONTAP-Mediator.pem`	A cadeia de confiança da CA de certificação pública
`csc-prod-ONTAP-Mediator.pem`	O certificado usado para gerar a chave
`ontap-mediator-1.9.0`	O executável de instalação do produto para a versão 1.9.0
`ontap-mediator-1.9.0.sig`	O hash SHA-256 e depois o RSA-assinado usando a chave csc-prod, assinatura para o instalador
`ontap-mediator-1.9.0.sig.tsr`	A solicitação de revogação para uso pelo OCSCP para a assinatura do instalador
`ontap-mediator-1.9.0.tsr`	O arquivo de solicitação de assinatura de carimbo de data/hora
`tsa-prod-ONTAP-Mediator.pem`	O certificado público para o TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	O certificado público CA Chain para o TSR

Passos

1. Efetue a verificação de revogação `csc-prod-ONTAP-Mediator.pem` utilizando o OCSP (Online Certificate Status Protocol).
   a. Localize o URL OCSP usado para Registrar o certificado porque os certificados de desenvolvedor podem não fornecer um uri.

      ```
      openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
      ```

   b. Gerar uma solicitação OCSP para o certificado.

      ```
      openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
      prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
      -reqout req.der
      ```

   c. Conete-se ao Gerenciador OCSP para enviar a solicitação OCSP:

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
chain-ONTAP-Mediator.pem
```

2. Verifique a cadeia de confiança do CSC e as datas de expiração em relação ao host local:

   `openssl verify`

   A `openssl` versão DO CAMINHO deve ter um válido `cert.pem` (não autoassinado).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Verifique os `ontap-mediator-1.9.0.sig.tsr` arquivos e `ontap-mediator-1.9.0.tsr` usando os certificados associados:

   `openssl ts -verify`

   `.tsr` os ficheiros contêm a resposta de carimbo de hora associada ao instalador e à assinatura de código. O processamento confirma que o carimbo de data/hora tem uma assinatura válida da TSA e que o seu ficheiro de entrada não foi alterado. A verificação é efetuada localmente na sua máquina. Independentemente, não há necessidade de acessar servidores TSA.

```
openssl ts -verify -data ontap-mediator-1.9.0.sig -in ontap-mediator-
1.9.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.9.0 -in ontap-mediator-
1.9.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
ONTAP-Mediator.pem
```

4. Verifique assinaturas contra a chave:

   `openssl -dgst -verify`

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.9.0.sig ontap-mediator-1.9.0
```

Exemplo de verificação da assinatura do código do ONTAP Mediator (saída do console)

```
[root@scspa2695423001 ontap-mediator-1.9.0]# pwd
/root/ontap-mediator-1.9.0
[root@scspa2695423001 ontap-mediator-1.9.0]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.9.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.9.0.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.9.0.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.9.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.9.0]#
[root@scspa2695423001 ontap-mediator-1.9.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.9.0.sig -in ontap-mediator-
1.9.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.9.0 -in ontap-mediator-
1.9.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.9.0.sig ontap-mediator-1.9.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.9.0]#
```

Instale o pacote de instalação do Mediador ONTAP

Para instalar o serviço Mediador ONTAP, você deve obter o pacote de instalação e executar o instalador no host.

Passos

1. Execute o instalador e responda aos prompts conforme necessário:

   ```
   ./ontap-mediator-1.9.0/ontap-mediator-1.9.0 -y
   ```

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.9.0/ontap-mediator-1.9.0 -y
   ```

   O processo de instalação prossegue para criar as contas necessárias e instalar os pacotes necessários. Se você tiver uma versão anterior do Mediator instalada no host, você será solicitado a confirmar que deseja atualizar.

2. A partir do ONTAP Mediator 1,4, o mecanismo de Inicialização segura é ativado em sistemas UEFI. Quando o Secure Boot estiver ativado, você deve seguir etapas adicionais para Registrar a chave de segurança após a instalação:

   - Siga as instruções no arquivo README para assinar o módulo do kernel SCST.:

     ```
     /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
     signing
     ```

- Localize as teclas necessárias:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> Após a instalação, os arquivos README e a localização da chave também são fornecidos na saída do sistema.

Exemplo de instalação do Mediador ONTAP (saída do console)

```
[root@mediator_host ~]# cat /etc/os-release
NAME="Red Hat Enterprise Linux"
VERSION="9.4 (Plow)"
ID="rhel"
ID_LIKE="fedora"
VERSION_ID="9.4"
PLATFORM_ID="platform:el9"
PRETTY_NAME="Red Hat Enterprise Linux 9.4 (Plow)"
ANSI_COLOR="0;31"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:redhat:enterprise_linux:9::baseos"
HOME_URL="https://www.redhat.com/"
DOCUMENTATION_URL="https://access.redhat.com/documentation/en-
us/red_hat_enterprise_linux/9"
BUG_REPORT_URL="https://bugzilla.redhat.com/"

REDHAT_BUGZILLA_PRODUCT="Red Hat Enterprise Linux 9"
REDHAT_BUGZILLA_PRODUCT_VERSION=9.4
REDHAT_SUPPORT_PRODUCT="Red Hat Enterprise Linux"
REDHAT_SUPPORT_PRODUCT_VERSION="9.4"
[root@mediator_host ~]#

[root@mediator_host ~]# tar -zxvf ontap-mediator-1.9.0.tgz
ontap-mediator-1.9.0/
ontap-mediator-1.9.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/ONTAP-Mediator-production.pub
ontap-mediator-1.9.0/ontap-mediator-1.9.0
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig
[root@mediator_host ~]# ontap-mediator-1.9.0/ontap-mediator-1.9.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
```

```
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? y(es)/N(o): yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin



Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode


+ Checking for default Linux firewall


################################################################
Preparing for installation of ONTAP Mediator packages.


+ Installing required packages.


Last metadata expiration check: 0:15:55 ago on Thu 17 Oct 2024 09:06:29
AM EDT.
Package openssl-1:3.0.7-27.el9.x86_64 is already installed.
Package openssl-devel-1:3.0.7-27.el9.x86_64 is already installed.
Package kernel-devel-5.14.0-427.22.1.el9_4.x86_64 is already installed.
Package gcc-11.4.1-3.el9.x86_64 is already installed.
Package make-1:4.3-8.el9.x86_64 is already installed.
Package libselinux-utils-3.6-1.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package bzip2-1.0.8-8.el9.x86_64 is already installed.
Package elfutils-libelf-devel-0.190-2.el9.x86_64 is already installed.
Package policycoreutils-python-utils-3.6-2.1.el9.noarch is already
```

```
installed.
Package python3-3.9.18-3.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
===========
 Package
Architecture                              Version
Repository                                                                  Size
================================================================================
================================================================================
================================================================================
===========
Installing:
 efibootmgr                                                                 x86_64
16-12.el9                                       rhel-9-for-x86_64-
baseos-rpms                                      48 k
 mokutil                                                                    x86_64
2:0.6.0-4.el9                                   rhel-9-for-x86_64-
baseos-rpms                                      50 k
 patch                                                                      x86_64
2.7.6-16.el9                                    rhel-9-for-x86_64-
appstream-rpms                                  130 k
 perl-ExtUtils-MakeMaker                                                    noarch
2:7.60-3.el9                                    rhel-9-for-x86_64-
appstream-rpms                                  304 k
 python3-devel                                                              x86_64
3.9.18-3.el9_4.5                                rhel-9-for-x86_64-
appstream-rpms                                  248 k
 python3-pip                                                                noarch
21.2.3-8.el9                                    rhel-9-for-x86_64-
appstream-rpms                                  2.0 M
Upgrading:
 openssl                                                                    x86_64
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
baseos-rpms                                     1.2 M
 openssl-devel                                                              x86_64
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
appstream-rpms                                  4.1 M
 openssl-libs                                                               i686
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
baseos-rpms                                     1.9 M
 openssl-libs                                                               x86_64
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
baseos-rpms                                     1.9 M
```

```
 python-unversioned-command                                    noarch
3.9.18-3.el9_4.5                                    rhel-9-for-x86_64-
appstream-rpms                                       10 k
 python3                                                       x86_64
3.9.18-3.el9_4.5                                    rhel-9-for-x86_64-
baseos-rpms                                          30 k
 python3-libs                                                  x86_64
3.9.18-3.el9_4.5                                    rhel-9-for-x86_64-
baseos-rpms                                         7.9 M
Installing dependencies:
 efi-filesystem                                                noarch
6-2.el9_0                                           rhel-9-for-x86_64-
baseos-rpms                                         9.5 k
 efivar-libs                                                   x86_64
38-3.el9                                            rhel-9-for-x86_64-
baseos-rpms                                         124 k
 perl-AutoSplit                                                noarch
5.74-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       22 k
 perl-Benchmark                                                noarch
1.23-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       27 k
 perl-CPAN-Meta-YAML                                           noarch
0.018-461.el9                                       rhel-9-for-x86_64-
appstream-rpms                                       29 k
 perl-Devel-PPPort                                             x86_64
3.62-4.el9                                          rhel-9-for-x86_64-
appstream-rpms                                      216 k
 perl-ExtUtils-Command                                         noarch
2:7.60-3.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       16 k
 perl-ExtUtils-Constant                                        noarch
0.25-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       49 k
 perl-ExtUtils-Install                                         noarch
2.20-4.el9                                          rhel-9-for-x86_64-
appstream-rpms                                       47 k
 perl-ExtUtils-Manifest                                        noarch
1:1.73-4.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       37 k
 perl-ExtUtils-ParseXS                                         noarch
1:3.40-460.el9                                      rhel-9-for-x86_64-
appstream-rpms                                      190 k
 perl-File-Compare                                             noarch
1.100.600-481.el9                                   rhel-9-for-x86_64-
appstream-rpms                                       14 k
```

```
 perl-JSON-PP                                                  noarch
1:4.06-4.el9                                          rhel-9-for-x86_64-
appstream-rpms                                         69 k
 perl-Test-Harness                                             noarch
1:3.42-461.el9                                        rhel-9-for-x86_64-
appstream-rpms                                        299 k
 perl-lib                                                      x86_64
0.65-481.el9                                          rhel-9-for-x86_64-
appstream-rpms                                         15 k
 perl-version                                                  x86_64
7:0.99.28-4.el9                                       rhel-9-for-x86_64-
appstream-rpms                                         67 k
 systemtap-sdt-devel                                           x86_64
5.0-4.el9                                             rhel-9-for-x86_64-
appstream-rpms                                         77 k
Installing weak dependencies:
 perl-CPAN-Meta                                                noarch
2.150010-460.el9                                      rhel-9-for-x86_64-
appstream-rpms                                        206 k
 perl-CPAN-Meta-Requirements                                   noarch
2.140-461.el9                                         rhel-9-for-x86_64-
appstream-rpms                                         34 k
 perl-devel                                                    x86_64
4:5.32.1-481.el9                                      rhel-9-for-x86_64-
appstream-rpms                                        680 k
 perl-doc                                                      noarch
5.32.1-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                        4.6 M

Transaction Summary
================================================================================
================================================================================
================================================================================
===========
Install  27 Packages
Upgrade   7 Packages

Total download size: 27 M
Is this ok [y/N]: y
Downloading Packages:
(1/34): perl-CPAN-Meta-YAML-0.018-461.el9.noarch.rpm
220 kB/s |  29 kB     00:00
(2/34): perl-CPAN-Meta-Requirements-2.140-461.el9.noarch.rpm
249 kB/s |  34 kB     00:00
(3/34): perl-ExtUtils-Install-2.20-4.el9.noarch.rpm
4.2 MB/s |  47 kB     00:00
```

```
(4/34): perl-CPAN-Meta-2.150010-460.el9.noarch.rpm
1.3 MB/s | 206 kB     00:00
(5/34): perl-version-0.99.28-4.el9.x86_64.rpm
5.5 MB/s |  67 kB     00:00
(6/34): perl-ExtUtils-Manifest-1.73-4.el9.noarch.rpm
3.9 MB/s |  37 kB     00:00
(7/34): perl-ExtUtils-MakeMaker-7.60-3.el9.noarch.rpm
16 MB/s | 304 kB     00:00
(8/34): perl-ExtUtils-ParseXS-3.40-460.el9.noarch.rpm
11 MB/s | 190 kB     00:00
(9/34): patch-2.7.6-16.el9.x86_64.rpm
15 MB/s | 130 kB     00:00
(10/34): perl-Test-Harness-3.42-461.el9.noarch.rpm
15 MB/s | 299 kB     00:00
(11/34): perl-Devel-PPPort-3.62-4.el9.x86_64.rpm
14 MB/s | 216 kB     00:00
(12/34): perl-ExtUtils-Command-7.60-3.el9.noarch.rpm
1.4 MB/s |  16 kB     00:00
(13/34): perl-JSON-PP-4.06-4.el9.noarch.rpm
6.9 MB/s |  69 kB     00:00
(14/34): perl-Benchmark-1.23-481.el9.noarch.rpm
3.9 MB/s |  27 kB     00:00
(15/34): systemtap-sdt-devel-5.0-4.el9.x86_64.rpm
9.4 MB/s |  77 kB     00:00
(16/34): perl-AutoSplit-5.74-481.el9.noarch.rpm
2.8 MB/s |  22 kB     00:00
(17/34): perl-ExtUtils-Constant-0.25-481.el9.noarch.rpm
5.9 MB/s |  49 kB     00:00
(18/34): perl-File-Compare-1.100.600-481.el9.noarch.rpm
1.7 MB/s |  14 kB     00:00
(19/34): perl-devel-5.32.1-481.el9.x86_64.rpm
21 MB/s | 680 kB     00:00
(20/34): perl-lib-0.65-481.el9.x86_64.rpm
2.1 MB/s |  15 kB     00:00
(21/34): python3-pip-21.2.3-8.el9.noarch.rpm
26 MB/s | 2.0 MB     00:00
(22/34): efi-filesystem-6-2.el9_0.noarch.rpm
1.8 MB/s | 9.5 kB     00:00
(23/34): python3-devel-3.9.18-3.el9_4.5.x86_64.rpm
8.6 MB/s | 248 kB     00:00
(24/34): efibootmgr-16-12.el9.x86_64.rpm
5.0 MB/s |  48 kB     00:00
(25/34): efivar-libs-38-3.el9.x86_64.rpm
15 MB/s | 124 kB     00:00
(26/34): mokutil-0.6.0-4.el9.x86_64.rpm
5.2 MB/s |  50 kB     00:00
```

```
(27/34): python-unversioned-command-3.9.18-3.el9_4.5.noarch.rpm
2.2 MB/s |  10 kB     00:00
(28/34): python3-3.9.18-3.el9_4.5.x86_64.rpm
6.9 MB/s |  30 kB     00:00
(29/34): perl-doc-5.32.1-481.el9.noarch.rpm
27 MB/s | 4.6 MB     00:00
(30/34): openssl-3.0.7-28.el9_4.x86_64.rpm
30 MB/s | 1.2 MB     00:00
(31/34): openssl-devel-3.0.7-28.el9_4.x86_64.rpm
25 MB/s | 4.1 MB     00:00
(32/34): openssl-libs-3.0.7-28.el9_4.x86_64.rpm
22 MB/s | 1.9 MB     00:00
(33/34): openssl-libs-3.0.7-28.el9_4.i686.rpm
29 MB/s | 1.9 MB     00:00
(34/34): python3-libs-3.9.18-3.el9_4.5.x86_64.rpm
27 MB/s | 7.9 MB     00:00
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
-----------
Total
44 MB/s |  27 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Upgrading        : openssl-libs-1:3.0.7-28.el9_4.x86_64
1/41
  Installing       : perl-version-7:0.99.28-4.el9.x86_64
2/41
  Installing       : perl-CPAN-Meta-Requirements-2.140-461.el9.noarch
3/41
  Upgrading        : python3-libs-3.9.18-3.el9_4.5.x86_64
4/41
  Upgrading        : python3-3.9.18-3.el9_4.5.x86_64
5/41
  Upgrading        : python-unversioned-command-3.9.18-3.el9_4.5.noarch
6/41
  Installing       : efivar-libs-38-3.el9.x86_64
7/41
  Installing       : perl-File-Compare-1.100.600-481.el9.noarch
8/41
  Installing       : perl-JSON-PP-1:4.06-4.el9.noarch
```

```
9/41
  Installing       : perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch
10/41
  Installing       : python3-pip-21.2.3-8.el9.noarch
11/41
  Installing       : systemtap-sdt-devel-5.0-4.el9.x86_64
12/41
  Installing       : efi-filesystem-6-2.el9_0.noarch
13/41
  Installing       : perl-lib-0.65-481.el9.x86_64
14/41
  Installing       : perl-doc-5.32.1-481.el9.noarch
15/41
  Installing       : perl-ExtUtils-Constant-0.25-481.el9.noarch
16/41
  Installing       : perl-AutoSplit-5.74-481.el9.noarch
17/41
  Installing       : perl-Benchmark-1.23-481.el9.noarch
18/41
  Installing       : perl-Test-Harness-1:3.42-461.el9.noarch
19/41
  Installing       : perl-ExtUtils-Command-2:7.60-3.el9.noarch
20/41
  Installing       : perl-Devel-PPPort-3.62-4.el9.x86_64
21/41
  Installing       : perl-ExtUtils-Manifest-1:1.73-4.el9.noarch
22/41
  Installing       : perl-CPAN-Meta-YAML-0.018-461.el9.noarch
23/41
  Installing       : perl-CPAN-Meta-2.150010-460.el9.noarch
24/41
  Installing       : perl-devel-4:5.32.1-481.el9.x86_64
25/41
  Installing       : perl-ExtUtils-Install-2.20-4.el9.noarch
26/41
  Installing       : perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch
27/41
  Installing       : efibootmgr-16-12.el9.x86_64
28/41
  Installing       : python3-devel-3.9.18-3.el9_4.5.x86_64
29/41
  Installing       : mokutil-2:0.6.0-4.el9.x86_64
30/41
  Upgrading        : openssl-devel-1:3.0.7-28.el9_4.x86_64
31/41
  Upgrading        : openssl-1:3.0.7-28.el9_4.x86_64
```

```
32/41
  Installing       : patch-2.7.6-16.el9.x86_64
33/41
  Upgrading        : openssl-libs-1:3.0.7-28.el9_4.i686
34/41
  Cleanup          : openssl-devel-1:3.0.7-27.el9.x86_64
35/41
  Cleanup          : python-unversioned-command-3.9.18-3.el9.noarch
36/41
  Cleanup          : openssl-1:3.0.7-27.el9.x86_64
37/41
  Cleanup          : openssl-libs-1:3.0.7-27.el9.i686
38/41
  Cleanup          : python3-3.9.18-3.el9.x86_64
39/41
  Cleanup          : python3-libs-3.9.18-3.el9.x86_64
40/41
  Cleanup          : openssl-libs-1:3.0.7-27.el9.x86_64
41/41
  Running scriptlet: openssl-libs-1:3.0.7-27.el9.x86_64
41/41
  Verifying        : perl-CPAN-Meta-2.150010-460.el9.noarch
1/41
  Verifying        : perl-CPAN-Meta-Requirements-2.140-461.el9.noarch
2/41
  Verifying        : perl-CPAN-Meta-YAML-0.018-461.el9.noarch
3/41
  Verifying        : perl-ExtUtils-Install-2.20-4.el9.noarch
4/41
  Verifying        : perl-version-7:0.99.28-4.el9.x86_64
5/41
  Verifying        : perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch
6/41
  Verifying        : perl-ExtUtils-Manifest-1:1.73-4.el9.noarch
7/41
  Verifying        : perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch
8/41
  Verifying        : perl-Test-Harness-1:3.42-461.el9.noarch
9/41
  Verifying        : patch-2.7.6-16.el9.x86_64
10/41
  Verifying        : perl-Devel-PPPort-3.62-4.el9.x86_64
11/41
  Verifying        : perl-ExtUtils-Command-2:7.60-3.el9.noarch
12/41
  Verifying        : perl-JSON-PP-1:4.06-4.el9.noarch
```

```
13/41
  Verifying        : perl-Benchmark-1.23-481.el9.noarch
14/41
  Verifying        : python3-pip-21.2.3-8.el9.noarch
15/41
  Verifying        : systemtap-sdt-devel-5.0-4.el9.x86_64
16/41
  Verifying        : perl-AutoSplit-5.74-481.el9.noarch
17/41
  Verifying        : perl-ExtUtils-Constant-0.25-481.el9.noarch
18/41
  Verifying        : perl-File-Compare-1.100.600-481.el9.noarch
19/41
  Verifying        : perl-devel-4:5.32.1-481.el9.x86_64
20/41
  Verifying        : perl-doc-5.32.1-481.el9.noarch
21/41
  Verifying        : perl-lib-0.65-481.el9.x86_64
22/41
  Verifying        : python3-devel-3.9.18-3.el9_4.5.x86_64
23/41
  Verifying        : efi-filesystem-6-2.el9_0.noarch
24/41
  Verifying        : efibootmgr-16-12.el9.x86_64
25/41
  Verifying        : efivar-libs-38-3.el9.x86_64
26/41
  Verifying        : mokutil-2:0.6.0-4.el9.x86_64
27/41
  Verifying        : python-unversioned-command-3.9.18-3.el9_4.5.noarch
28/41
  Verifying        : python-unversioned-command-3.9.18-3.el9.noarch
29/41
  Verifying        : openssl-devel-1:3.0.7-28.el9_4.x86_64
30/41
  Verifying        : openssl-devel-1:3.0.7-27.el9.x86_64
31/41
  Verifying        : python3-3.9.18-3.el9_4.5.x86_64
32/41
  Verifying        : python3-3.9.18-3.el9.x86_64
33/41
  Verifying        : python3-libs-3.9.18-3.el9_4.5.x86_64
34/41
  Verifying        : python3-libs-3.9.18-3.el9.x86_64
35/41
  Verifying        : openssl-1:3.0.7-28.el9_4.x86_64
```

```
36/41
  Verifying        : openssl-1:3.0.7-27.el9.x86_64
37/41
  Verifying        : openssl-libs-1:3.0.7-28.el9_4.x86_64
38/41
  Verifying        : openssl-libs-1:3.0.7-27.el9.x86_64
39/41
  Verifying        : openssl-libs-1:3.0.7-28.el9_4.i686
40/41
  Verifying        : openssl-libs-1:3.0.7-27.el9.i686
41/41
Installed products updated.

Upgraded:
  openssl-1:3.0.7-28.el9_4.x86_64       openssl-devel-1:3.0.7-
28.el9_4.x86_64       openssl-libs-1:3.0.7-28.el9_4.i686       openssl-
libs-1:3.0.7-28.el9_4.x86_64       python-unversioned-command-3.9.18-
3.el9_4.5.noarch
  python3-3.9.18-3.el9_4.5.x86_64       python3-libs-3.9.18-
3.el9_4.5.x86_64
Installed:
  efi-filesystem-6-2.el9_0.noarch
efibootmgr-16-12.el9.x86_64                          efivar-libs-38-
3.el9.x86_64                          mokutil-2:0.6.0-4.el9.x86_64
  patch-2.7.6-16.el9.x86_64                                  perl-
AutoSplit-5.74-481.el9.noarch                  perl-Benchmark-1.23-
481.el9.noarch                      perl-CPAN-Meta-2.150010-
460.el9.noarch
  perl-CPAN-Meta-Requirements-2.140-461.el9.noarch           perl-
CPAN-Meta-YAML-0.018-461.el9.noarch             perl-Devel-PPPort-
3.62-4.el9.x86_64                    perl-ExtUtils-Command-2:7.60-
3.el9.noarch
  perl-ExtUtils-Constant-0.25-481.el9.noarch                 perl-
ExtUtils-Install-2.20-4.el9.noarch              perl-ExtUtils-
MakeMaker-2:7.60-3.el9.noarch           perl-ExtUtils-Manifest-1:1.73-
4.el9.noarch
  perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch                perl-
File-Compare-1.100.600-481.el9.noarch           perl-JSON-PP-1:4.06-
4.el9.noarch                      perl-Test-Harness-1:3.42-
461.el9.noarch
  perl-devel-4:5.32.1-481.el9.x86_64                         perl-doc-
5.32.1-481.el9.noarch                        perl-lib-0.65-
481.el9.x86_64                           perl-version-7:0.99.28-
4.el9.x86_64
  python3-devel-3.9.18-3.el9_4.5.x86_64                      python3-
pip-21.2.3-8.el9.noarch                       systemtap-sdt-devel-5.0-
```

```
4.el9.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.T7uce6/ontap-
mediator-1.9.0/ontap-mediator-1.9.0/install_20241017092214.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20241017092214.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README

[root@mediator_host ~]# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Thu 2024-10-17 09:27:14 EDT; 1min
12s ago
    Process: 54470
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 54489 (uwsgi)
     Status: "uWSGI is ready"
      Tasks: 3 (limit: 11104)
     Memory: 77.1M
        CPU: 2.507s
     CGroup: /system.slice/ontap_mediator.service
             ├─54489 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
```

```
             ├─54504 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
             └─54507 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Creating
filesystem with 192000 4k blocks and 48000 inodes
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Filesystem UUID:
b1fa0a40-0e7d-4c67-bbff-33421f3ec61b
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Superblock backups
stored on blocks:
Oct 17 09:27:10 mediator_host ontap_mediator[54476]:         32768,
98304, 163840
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: [41B blob data]
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: [38B blob data]
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Creating journal
(4096 blocks): done
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: [75B blob data]
Oct 17 09:27:10 mediator_host ontap_mediator[54489]: [uWSGI] getting
INI configuration from
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
Oct 17 09:27:14 mediator_host systemd[1]: Started ONTAP Mediator.

[root@mediator_host ~]# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Thu 2024-10-17 09:27:08 EDT; 1min
32s ago
    Process: 54384 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 54467 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 54425 (iscsi-scstd)
      Tasks: 1 (limit: 11104)
     Memory: 1.2M
        CPU: 494ms
     CGroup: /system.slice/mediator-scst.service
             └─54425 /usr/local/sbin/iscsi-scstd

Oct 17 09:27:07 mediator_host systemd[1]: Starting mediator-
scst.service...
Oct 17 09:27:08 mediator_host iscsi-scstd[54423]: max_data_seg_len
1048576, max_queued_cmds 2048
Oct 17 09:27:08 mediator_host scst[54384]: Loading and configuring SCST
Oct 17 09:27:08 mediator_host systemd[1]: Started mediator-
```

```
scst.service.
[root@mediator_host ~]#
```

Verifique a instalação

Após a instalação do Mediador ONTAP, você deve verificar se os serviços do Mediador ONTAP estão em execução.

Passos

1. Veja o status dos serviços do Mediador ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme as portas usadas pelo serviço do Mediador ONTAP:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

Configuração pós-instalação

Depois que o serviço do Mediador ONTAP for instalado e executado, tarefas de configuração adicionais devem ser executadas no sistema de storage ONTAP para usar os recursos do Mediador:

- Para usar o serviço Mediador ONTAP em uma configuração IP do MetroCluster, "Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster"consulte .
- Para usar a sincronização ativa do SnapMirror, "Instale o Serviço do Mediador ONTAP e confirme a configuração do cluster do ONTAP"consulte .

Configurar as políticas de segurança do ONTAP Mediator

O servidor Mediador ONTAP suporta várias configurações de segurança configuráveis. Os valores padrão para todas as configurações são fornecidos em um `low_space_threshold_mib: 10` arquivo somente leitura:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Todos os valores colocados no `ontap_mediator.user_config.yaml` substituirão os valores padrão e serão mantidos em todas as atualizações do ONTAP Mediator.

Depois de modificar `ontap_mediator.user_config.yaml`, reinicie o serviço ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Modifique os atributos do Mediador ONTAP

Os atributos do Mediador ONTAP descritos nesta seção podem ser modificados se necessário.

> Outros valores padrão no `ontap_mediator.config.yaml` não devem ser alterados porque os valores modificados não são mantidos durante as atualizações do ONTAP Mediator.

Você modifica os atributos do Mediador do ONTAP copiando as variáveis necessárias `ontap_mediator.user_config.yaml` para o arquivo para substituir as configurações padrão.

Instale certificados SSL de terceiros

Se você precisar substituir os certificados autoassinados padrão por certificados SSL de terceiros, modifique determinados atributos nos seguintes arquivos:

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

As variáveis nesses arquivos são usadas para controlar os arquivos de certificado usados pelo serviço do Mediador ONTAP.

ONTAP Mediador 1,9 e posterior

As variáveis padrão listadas na tabela a seguir são incluídas no `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` arquivo.

Variável	Caminho
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` é usado para definir a expiração dos certificados de cliente. O valor máximo é de três anos (1095 dias).
- `x509_passin_pwd` é a senha para o certificado de cliente assinado.

As variáveis padrão listadas na tabela a seguir são incluídas no `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Variável	Caminho
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP Mediador 1,8 e anterior

As variáveis padrão listadas na tabela a seguir são incluídas no `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` arquivo.

Variável	Caminho
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` é usado para definir a expiração dos certificados de cliente. O valor máximo é de três anos (1095 dias).
- `x509_passin_pwd` é a senha para o certificado de cliente assinado.

As variáveis padrão listadas na tabela a seguir são incluídas no `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Variável	Caminho
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

Se você modificar esses atributos, reinicie o serviço do ONTAP Mediator para aplicar as alterações. Para obter instruções detalhadas sobre como substituir certificados padrão por certificados de terceiros, "Substitua certificados autoassinados por certificados de terceiros confiáveis"consulte .

Proteção contra ataque por senha

As configurações a seguir fornecem proteção contra ataques de adivinhação de senha de força bruta.

Para ativar a funcionalidade, defina um valor para a `window_seconds` e a `retry_limit`.

Exemplos:

- Forneça uma janela de 5 minutos para suposições e, em seguida, redefina a contagem para zero falhas:

  ```
  authentication_lock_window_seconds: 300
  ```

- Bloqueie a conta se ocorrerem cinco falhas dentro do período de tempo da janela:

  ```
  authentication_retry_limit: 5
  ```

- Reduza o impactos de ataques de adivinhação de senha de força bruta definindo um atraso que ocorre antes de rejeitar cada tentativa, o que retarda os ataques.

  ```
  authentication_failure_delay_seconds: 5
  ```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to allow
before locking API access, null = unlimited
```

Regras de complexidade de senha

Os campos a seguir controlam as regras de complexidade de senha da conta de usuário da API do ONTAP Mediator.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

Controle do espaço livre

Existem definições que controlam o espaço livre necessário no `/opt/netapp/lib/ontap_mediator` disco.

Se o espaço for inferior ao limite definido, o serviço emitirá um evento de aviso.

```
low_space_threshold_mib: 10
```

Controle do espaço de Registro de reserva

O RESERVE_LOG_SPACE é controlado por configurações específicas. Por padrão, a instalação do servidor Mediador do ONTAP cria um espaço em disco separado para os logs. O instalador cria um novo arquivo de tamanho fixo com um total de 700 MB de espaço em disco para ser usado explicitamente para o Registro do Mediator.

Para desativar esse recurso e usar o espaço em disco padrão, execute as seguintes etapas:

1. Altere o valor de RESERVE_LOG_SPACE de 1 para 0 no seguinte arquivo:

   ```
   /opt/netapp/lib/ontap_mediator/tools/mediator_env
   ```

2. Reinicie o Mediator:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

Para reativar a funcionalidade, altere o valor de 0 para 1 e reinicie o Mediador.

> Alternar entre espaços de disco não limpa logs existentes. Todos os logs anteriores são copiados e movidos para o espaço em disco atual depois de alternar e reiniciar o Mediator.

Gerenciar o serviço de mediador do ONTAP

Gerencie o serviço do ONTAP Mediator, incluindo alteração das credenciais do usuário, interrupção e reativação do serviço, verificação de sua integridade e instalação ou desinstalação do SCST para manutenção do host. Você também pode gerenciar certificados, como a geração de certificados autoassinados, a substituição deles por certificados de terceiros confiáveis e a solução de problemas relacionados a certificados.

Altere o nome de usuário

Você pode alterar o nome de usuário usando o procedimento a seguir.

Sobre esta tarefa

Execute esta tarefa no host Linux no qual o serviço Mediador ONTAP está instalado.

Se você não conseguir alcançar esse comando, talvez seja necessário executar o comando usando o caminho completo como mostrado no exemplo a seguir:

```
/usr/local/bin/mediator_username
```

Passos

Altere o nome de usuário escolhendo uma das seguintes opções:

- **Opção (a)**: Execute o comando `mediator_change_user` e responda aos prompts como mostrado no

exemplo a seguir:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- **Opção (b)**: Execute o seguinte comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

Altere a palavra-passe

Pode alterar a palavra-passe utilizando o seguinte procedimento.

Sobre esta tarefa

Execute esta tarefa no host Linux no qual o serviço Mediador ONTAP está instalado.

Se você não conseguir alcançar esse comando, talvez seja necessário executar o comando usando o caminho completo como mostrado no exemplo a seguir:

```
/usr/local/bin/mediator_change_password
```

Passos

Altere a senha escolhendo uma das seguintes opções:

- **Opção (a)**: Execute o `mediator_change_password` comando e responda aos prompts como mostrado no exemplo a seguir:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
          Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- **Opção (b)**: Execute o seguinte comando:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

O exemplo mostra que a senha foi alterada de "mediator1" para "mediator2".

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

Pare o serviço Mediador ONTAP

Para interromper o serviço do Mediador ONTAP, execute as seguintes etapas:

Passos

1. Pare o Mediador ONTAP:

```
systemctl stop ontap_mediator
```

2. Parar SCST:

```
systemctl stop mediator-scst
```

3. Desative o Mediador ONTAP e o SCST:

```
systemctl diable ontap_mediator mediator-scst
```

Reative o serviço Mediador ONTAP

Para reativar o serviço do Mediador ONTAP, execute as seguintes etapas:

Passos

1. Ative o Mediador ONTAP e o SCST:

```
systemctl enable ontap_mediator mediator-scst
```

2. Iniciar SCST:

```
systemctl start mediator-scst
```

3. Iniciar o Mediador ONTAP:

```
systemctl start ontap_mediator
```

Verifique se o Mediador ONTAP está saudável

Após a instalação do Mediador ONTAP, você deve verificar se os serviços do Mediador ONTAP estão em execução.

Passos

1. Veja o status dos serviços do Mediador ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme as portas usadas pelo serviço do Mediador ONTAP:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Desinstale manualmente o SCST para executar a manutenção do host

Para desinstalar o SCST, você precisa do pacote tar SCST que é usado para a versão instalada do ONTAP Mediator.

Passos

1. Baixe o pacote SCST apropriado (como mostrado na tabela a seguir) e descompacte-o.

Para esta versão …	Use este pacote tar…
ONTAP Mediador 1,9	scst-3,8.0.tar.bz2
ONTAP Mediador 1,8	scst-3,8.0.tar.bz2
ONTAP Mediador 1,7	scst-3,7.0.tar.bz2
ONTAP Mediador 1,6	scst-3,7.0.tar.bz2

ONTAP Mediador 1,5	scst-3,6.0.tar.bz2
ONTAP Mediador 1,4	scst-3,6.0.tar.bz2
ONTAP Mediador 1,3	scst-3,5.0.tar.bz2
ONTAP Mediador 1,1	scst-3,4.0.tar.bz2
ONTAP Mediador 1,0	scst-3,3.0.tar.bz2

2. Emita os seguintes comandos no diretório "scst":
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Instale manualmente o SCST para executar a manutenção do host

Para instalar manualmente o SCST, você precisa do pacote tar SCST que é usado para a versão instalada do ONTAP Mediator (consulte a tabela acima).

1. Emita os seguintes comandos no diretório "scst":
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`
   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`
2. Opcionalmente, se o Secure Boot estiver ativado, antes de reiniciar, execute as seguintes etapas:
   a. Determine cada nome de arquivo para os módulos "scst_vdisk", "scst" e "iscsi_scst":

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

b. Determine a versão do kernel:

```
[root@localhost ~]# uname -r
```

c. Assine cada arquivo com o kernel:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. Instale a chave correta com o firmware UEFI.

As instruções para instalar a chave UEFI estão localizadas em:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

A chave UEFI gerada está localizada em:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der`

3. Execute uma reinicialização:

`reboot`

Desinstale o serviço ONTAP Mediator

Se necessário, pode remover o serviço Mediador ONTAP.

Antes de começar

O Mediador ONTAP tem de ser desligado do ONTAP antes de remover o serviço Mediador ONTAP.

Sobre esta tarefa

Você precisa executar esta tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.

Se você não conseguir alcançar esse comando, talvez seja necessário executar o comando usando o caminho completo como mostrado no exemplo a seguir:

`/usr/local/bin/uninstall_ontap_mediator`

Passo

1. Desinstale o serviço ONTAP Mediator:

`uninstall_ontap_mediator`

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Regenerar um certificado temporário autoassinado

A partir do ONTAP Mediator 1,7, você pode regenerar um certificado auto-assinado temporário usando o seguinte procedimento.

> Este procedimento só é suportado em sistemas que executam o ONTAP Mediator 1,7 ou posterior.

Sobre esta tarefa

- Você executa essa tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.
- Só é possível executar esta tarefa se os certificados autoassinados gerados se tornarem obsoletos devido a alterações no nome de host ou endereço IP do host após a instalação do Mediador ONTAP.
- Depois que o certificado auto-assinado temporário for substituído por um certificado de terceiros confiável, você *não* usará essa tarefa para regenerar um certificado. A ausência de um certificado auto-assinado fará com que este procedimento falhe.

Passo

Para regenerar um novo certificado auto-assinado temporário para o host atual, execute o seguinte passo:

1. Reinicie o serviço do Mediador ONTAP:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

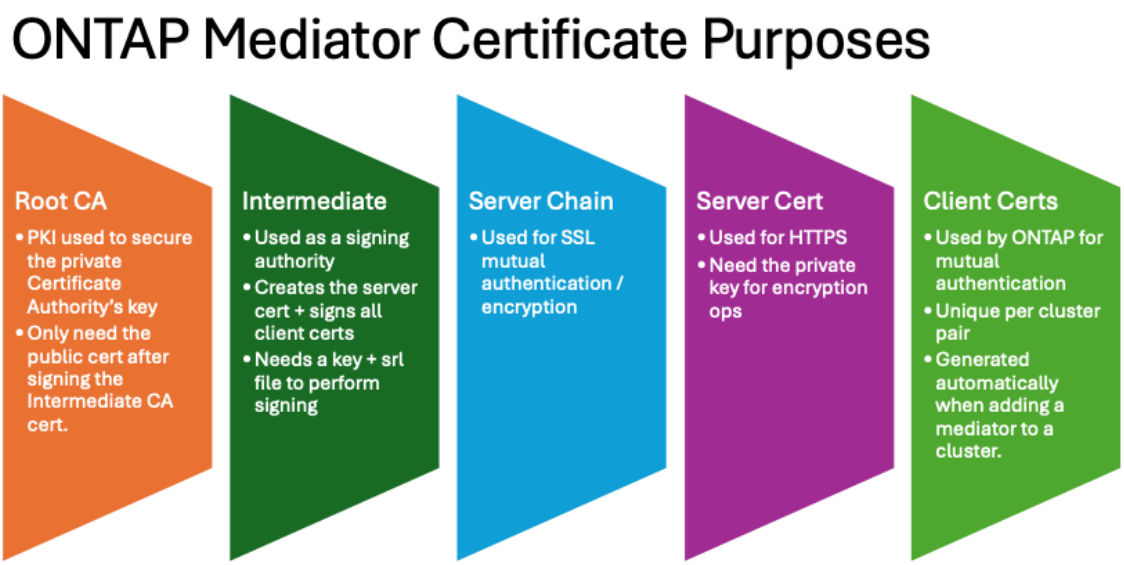
Substitua certificados autoassinados por certificados de terceiros confiáveis

Se suportado, você pode substituir certificados autoassinados por certificados de terceiros confiáveis.

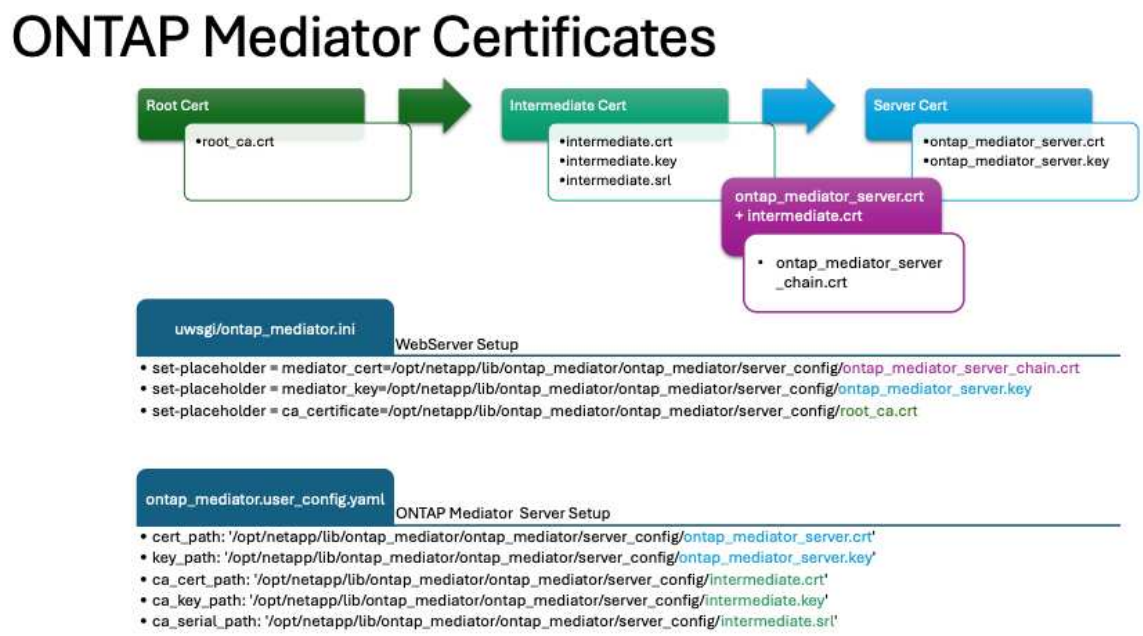
- Os certificados de terceiros são suportados apenas a partir do ONTAP 9.16,1 e em algumas versões de patch anteriores do ONTAP. "NetApp Bugs Online ID de erro CONTAP-243278"Consulte .
- Os certificados de terceiros são suportados apenas em sistemas que executam o ONTAP Mediator 1,7 ou posterior.

Sobre esta tarefa

- Você executa essa tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.
- Você pode executar esta tarefa se os certificados autoassinados gerados precisarem ser substituídos por certificados obtidos de uma autoridade de certificação subordinada (CA) confiável. Para isso, você deve ter acesso a uma autoridade de infraestrutura de chave pública (PKI) confiável.
- A imagem a seguir mostra as finalidades de cada certificado do Mediador ONTAP.



- A imagem a seguir mostra a configuração para a configuração do servidor web e a configuração do servidor do ONTAP Mediator.



Etapa 1: Obter um certificado de um terceiro que emite um certificado de CA

Você pode obter um certificado de uma autoridade PKI usando o procedimento a seguir.

O exemplo a seguir demonstra a substituição dos atores de certificados autoassinados pelos agentes de certificados de terceiros localizados em

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.

- O exemplo ilustra os critérios necessários para os certificados necessários para o serviço Mediador ONTAP. Você pode obter os certificados de uma autoridade PKI de uma forma que pode ser diferente deste procedimento. Ajuste o procedimento de acordo com sua necessidade do negócio.

ONTAP Mediador 1,9 e posterior

1. Crie uma chave `intermediate.key` privada e um arquivo de configuração `openssl_ca.cnf` que serão consumidos pela autoridade PKI para gerar um certificado.

   a. Gerar a chave privada `intermediate.key` :

      Exemplo

```
openssl genrsa -aes256 -out intermediate.key 4096
```

   a. O arquivo de `openssl_ca.cnf` configuração (localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define as propriedades que o certificado gerado deve ter.

2. Use a chave privada e o arquivo de configuração para criar uma solicitação de assinatura de certificado `intermediate.csr` :

   Exemplo:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key
-new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@scs000216655 server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIE6TCCAtECAQAwgaMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh
...
erARKhY9z0e8BHPl3g==
-----END CERTIFICATE REQUEST-----
```

3. Envie a solicitação de assinatura de certificado `intermediate.csr` para uma autoridade PKI para sua assinatura.

   A autoridade PKI verifica a solicitação e assina o `.csr`, gerando o certificado `intermediate.crt`. Além disso, você precisa obter o `root_intermediate.crt` certificado que assinou o `intermediate.crt` certificado da autoridade PKI.

   > Para clusters do SnapMirror Business Continuity (SM-BC), é necessário adicionar os `intermediate.crt` certificados e `root_intermediate.crt` a um cluster do ONTAP. "Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

ONTAP Mediador 1,8 e anterior

1. Crie uma chave `ca.key` privada e um arquivo de configuração `openssl_ca.cnf` que serão consumidos pela autoridade PKI para gerar um certificado.

a. Gerar a chave privada `ca.key` :

Exemplo

```
openssl genrsa -aes256 -out ca.key 4096
```

a. O arquivo de `openssl_ca.cnf` configuração (localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define as propriedades que o certificado gerado deve ter.

2. Use a chave privada e o arquivo de configuração para criar uma solicitação de assinatura de certificado `ca.csr` :

Exemplo:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIE6TCCAtECAQAwgaMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh
...
erARKhY9z0e8BHPl3g==
-----END CERTIFICATE REQUEST-----
```

3. Envie a solicitação de assinatura de certificado `ca.csr` para uma autoridade PKI para sua assinatura.

A autoridade PKI verifica a solicitação e assina o `.csr`, gerando o certificado `ca.crt`. Além disso, você precisa obter o `root_ca.crt that signed the `ca.crt` certificado da autoridade PKI.

Para clusters do SnapMirror Business Continuity (SM-BC), é necessário adicionar os `ca.crt` certificados e `root_ca.crt` a um cluster do ONTAP. "Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

Etapa 2: Gere um certificado de servidor assinando com uma certificação de CA de terceiros

ONTAP Mediador 1,9 e posterior

Um certificado de servidor deve ser assinado pela chave privada `intermediate.key` e pelo certificado de `intermediate.crt` terceiros . Além disso, o arquivo de configuração `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contém certos atributos que especificam as propriedades necessárias para certificados de servidor emitidos pelo OpenSSL.

Os comandos a seguir podem gerar um certificado de servidor.

Passos

1. Para gerar uma solicitação de assinatura de certificado de servidor (CSR), execute o seguinte comando `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` na pasta:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. para gerar um certificado de servidor a partir do CSR, execute o seguinte comando a partir `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` da pasta:

   > Esses arquivos foram obtidos de uma autoridade PKI. Se você estiver usando um nome de certificado diferente, substitua `intermediate.crt` e `intermediate.key` pelos nomes de arquivo relevantes.

   ```
   openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
   intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
   -req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
   ```

   - A `-CAcreateserial` opção é usada para gerar os `intermediate.srl` arquivos.

ONTAP Mediador 1,8 e anterior

Um certificado de servidor deve ser assinado pela chave privada `ca.key` e pelo certificado de `ca.crt` terceiros . Além disso, o arquivo de configuração `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contém certos atributos que especificam as propriedades necessárias para certificados de servidor emitidos pelo OpenSSL.

Os comandos a seguir podem gerar um certificado de servidor.

Passos

1. Para gerar uma solicitação de assinatura de certificado de servidor (CSR), execute o seguinte comando `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` na pasta:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. para gerar um certificado de servidor a partir do CSR, execute o seguinte comando a partir `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` da pasta:

Esses arquivos foram obtidos de uma autoridade PKI. Se você estiver usando um nome de certificado diferente, substitua `ca.crt` e `ca.key` pelos nomes de arquivo relevantes.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- A `-CAcreateserial` opção é usada para gerar os `ca.srl` arquivos.

Etapa 3: Substitua o novo certificado de CA de terceiros e o certificado de servidor na configuração do ONTAP Mediator

ONTAP Mediador 1,9 e posterior

A configuração do certificado é fornecida ao serviço do Mediador ONTAP no arquivo de configuração localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. O arquivo inclui os seguintes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` e `key_path` são variáveis de certificado de servidor.
- `ca_cert_path`, `ca_key_path`, E `ca_serial_path` são variáveis de certificado CA.

Passos

1. Substitua todos `intermediate.*` os arquivos por certificados de terceiros.
2. Crie uma cadeia de certificados a partir dos `intermediate.crt` certificados e `ontap_mediator_server.crt`:

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ficheiro.

   Atualizar os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   set-placeholder = ca_certificate =
   ```

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_intermediate.crt`

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- `mediator_key value`O é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_intermediate.crt` arquivo.

4. Verifique se os seguintes atributos dos certificados recém-gerados estão definidos corretamente:
   - Proprietário do Grupo Linux: `netapp:netapp`
   - Permissões do Linux: `600`
5. Reinicie o Mediador ONTAP:

```
systemctl restart ontap_mediator
```

ONTAP Mediador 1,8 e anterior

A configuração do certificado é fornecida ao serviço do Mediador ONTAP no arquivo de configuração localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. O arquivo inclui os seguintes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` e `key_path` são variáveis de certificado de servidor.
- `ca_cert_path`, `ca_key_path`, E `ca_serial_path` são variáveis de certificado CA.

Passos

1. Substitua todos `ca.*` os arquivos por certificados de terceiros.
2. Crie uma cadeia de certificados a partir dos `ca.crt` certificados e `ontap_mediator_server.crt`:

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

3. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ficheiro.

Atualizar os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- `mediator_key value`O é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.

4. Verifique se os seguintes atributos dos certificados recém-gerados estão definidos corretamente:
   - Proprietário do Grupo Linux: `netapp:netapp`
   - Permissões do Linux: `600`
5. Reinicie o Mediador ONTAP:

```
systemctl restart ontap_mediator
```

Passo 4: Opcionalmente, use um caminho ou nome diferente para seus certificados de terceiros

ONTAP Mediador 1,9 e posterior

Você pode usar certificados de terceiros com um nome diferente `intermediate.*` ou armazenar os certificados de terceiros em um local diferente.

Passos

1. Configure o `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` arquivo para substituir os valores de variável padrão no `ontap_mediator.config.yaml` arquivo.

   Se você tiver obtido `intermediate.crt` de uma autoridade PKI e armazenar sua chave privada `intermediate.key` no local `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, o `ontap_mediator.user_config.yaml` arquivo deverá ser parecido com o seguinte exemplo:

   > Se você usou `intermediate.crt` para assinar o `ontap_mediator_server.crt` certificado, o `intermediate.srl` arquivo será gerado. Consulte Etapa 2: Gere um certificado de servidor assinando com uma certificação de CA de terceiros para obter mais informações.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. Se estiver a utilizar uma estrutura de certificados onde o `root_intermediate.crt` certificado forneça um `intermediate.crt` certificado que assine o `ontap_mediator_server.crt` certificado, crie uma cadeia de certificados a partir dos `intermediate.crt` certificados e `ontap_mediator_server.crt`:

> Você deve ter obtido os `intermediate.crt` certificados e `ontap_mediator_server.crt` de uma autoridade PKI anteriormente no procedimento.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ficheiro.

   Atualizar os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_interme
   diate.crt
   ```

   - O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
   - O `mediator_key` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
   - O `ca_certificate` valor é o caminho do `root_intermediate.crt` arquivo.

   > Para clusters do SnapMirror Business Continuity (SM-BC), é necessário adicionar os `intermediate.crt` certificados e `root_intermediate.crt` a um cluster do ONTAP. "Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

c. Verifique se os seguintes atributos dos certificados recém-gerados estão definidos corretamente:
   - Proprietário do Grupo Linux: `netapp:netapp`
   - Permissões do Linux: `600`

2. Reinicie o Mediador ONTAP quando os certificados forem atualizados no arquivo de configuração:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediador 1,8 e anterior

Você pode usar certificados de terceiros com um nome diferente `ca.*` ou armazenar os certificados de terceiros em um local diferente.

Passos

1. Configure o `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` arquivo para substituir os valores de variável padrão no `ontap_mediator.config.yaml` arquivo.

   Se você tiver obtido `ca.crt` de uma autoridade PKI e armazenar sua chave privada `ca.key` no local `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, o `ontap_mediator.user_config.yaml` arquivo deverá ser parecido com o seguinte exemplo:

Se você usou `ca.crt` para assinar o `ontap_mediator_server.crt` certificado, o `ca.srl` arquivo será gerado. Consulte Etapa 2: Gere um certificado de servidor assinando com uma certificação de CA de terceiros para obter mais informações.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. Se estiver a utilizar uma estrutura de certificados onde o `root_ca.crt` certificado forneça um `ca.crt` certificado que assine o `ontap_mediator_server.crt` certificado, crie uma cadeia de certificados a partir dos `ca.crt` certificados e `ontap_mediator_server.crt`:

Você deve ter obtido os `ca.crt` certificados e `ontap_mediator_server.crt` de uma autoridade PKI anteriormente no procedimento.

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ficheiro.

Atualizar os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- O `mediator_key` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.

> Para clusters do SnapMirror Business Continuity (SM-BC), é necessário adicionar os `ca.crt` certificados e `root_ca.crt` a um cluster do ONTAP. "Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

c. Verifique se os seguintes atributos dos certificados recém-gerados estão definidos corretamente:
   - Proprietário do Grupo Linux: `netapp:netapp`
   - Permissões do Linux: `600`

2. Reinicie o Mediador ONTAP quando os certificados forem atualizados no arquivo de configuração:

```
systemctl restart ontap_mediator
```

Solucionar problemas relacionados ao certificado

Você pode verificar certas propriedades dos certificados.

Verifique a expiração do certificado

Use o comando a seguir para identificar o intervalo de validade do certificado.

ONTAP Mediador 1,9 e posterior

```
[root@scs000216982 server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediador 1,8 e anterior

```
[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

Verifique as extensões X509v3 na certificação CA

Use o comando a seguir para verificar as extensões X509v3 na certificação CA.

ONTAP Mediador 1,9 e posterior

As propriedades definidas em **v3_ca** em `openssl_ca.cnf` são apresentadas como `X509v3 extensions` em `intermediate.crt`.

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@scs000216982 server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediador 1,8 e anterior

As propriedades definidas em **v3_ca** em `openssl_ca.cnf` são apresentadas como `X509v3 extensions` em `ca.crt`.

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

Verifique as extensões X509v3 nos nomes Alt do certificado do servidor e do assunto

As `v3_req` propriedades definidas no `openssl_server.cnf` arquivo de configuração são exibidas como `X509v3 extensions` no certificado.

No exemplo a seguir, você pode obter as variáveis nas `alt_names` seções executando os comandos `hostname -A` e `hostname -I` na VM Linux na qual o Mediador ONTAP está instalado.

Verifique com o administrador da rede os valores corretos das variáveis.

ONTAP Mediador 1,9 e posterior

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@scs000216982 server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediador 1,8 e anterior

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Verifique se uma chave privada corresponde a um certificado

Você pode verificar se uma chave particular corresponde a um certificado.

Use os seguintes comandos OpenSSL na chave e no certificado, respetivamente.

ONTAP Mediador 1,9 e posterior

```
[root@scs000216982 server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@scs000216982 server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediador 1,8 e anterior

```
[root@scs000216982 server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@scs000216982 server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Se o `-modulus` atributo para ambos corresponder, ele indica que a chave privada e o par de certificados são compatíveis e podem funcionar entre si.

Verifique se um certificado de servidor é criado a partir de um certificado de CA específico

Você pode usar o comando a seguir para verificar se o certificado do servidor foi criado a partir de um certificado de CA específico.

ONTAP Mediador 1,9 e posterior

```
[root@scs000216982 server_config]# openssl verify -CAfile
intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

ONTAP Mediador 1,8 e anterior

```
[root@scs000216982 server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Se a validação OCSP (Online Certificate Status Protocol) estiver sendo usada, use o comando "verificação do openssl".

Mantenha o host do SO para o ONTAP Mediator

Para um desempenho ideal, você deve manter o sistema operacional do host para o ONTAP Mediator regularmente.

Reinicie o host

Reinicie o host quando os clusters estiverem saudáveis. Embora o Mediador ONTAP esteja offline, os clusters correm o risco de não poderem reagir adequadamente às falhas. Recomenda-se uma janela de serviço se for necessário reiniciar.

O Mediador ONTAP será retomado automaticamente durante uma reinicialização e reentrará as relações que foram configuradas anteriormente com clusters ONTAP.

Atualizações do pacote de host

Qualquer biblioteca ou pacote yum (exceto o kernel) pode ser atualizado com segurança, mas pode exigir uma reinicialização para entrar em vigor. Recomenda-se uma janela de serviço se for necessário reiniciar.

Se você instalar o `yum-utils` pacote, use o `needs-restarting` comando para detetar se alguma alteração de pacote requer uma reinicialização.

Você deve reiniciar se alguma das dependências do ONTAP Mediator for atualizada porque elas não terão efeito imediato nos processos em execução.

Atualizações menores do kernel do sistema operacional do host

SCST deve ser compilado para o kernel que está sendo usado. Para atualizar o SO, é necessária uma janela de manutenção.

Passos

Execute as etapas a seguir para atualizar o kernel do sistema operacional do host.

1. Pare o Mediador ONTAP
2. Desinstale o pacote SCST. (O SCST não fornece um mecanismo de atualização.)
3. Atualize o sistema operacional e reinicie.
4. Volte a instalar o pacote SCST.
5. Reative os serviços do Mediador ONTAP.

O host muda para o nome de host ou IP

Sobre esta tarefa

- Você executa essa tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.
- Só é possível executar esta tarefa se os certificados autoassinados gerados se tornarem obsoletos devido a alterações no nome de host ou endereço IP do host após a instalação do Mediador ONTAP.
- Depois que o certificado auto-assinado temporário for substituído por um certificado de terceiros confiável, você *não* usará essa tarefa para regenerar um certificado. A ausência de um certificado auto-assinado fará com que este procedimento falhe.

Passo

Para regenerar um novo certificado auto-assinado temporário para o host atual, execute o seguinte passo:

1. Reinicie o Mediador ONTAP:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.............................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Gerenciamento de site IP do MetroCluster com o Gerenciador do sistema

As configurações do MetroCluster espelham os dados e a configuração de forma síncrona entre dois clusters ONTAP em locais separados. A partir do ONTAP 9.8, você pode usar o Gerenciador de sistema como uma interface simplificada para gerenciar uma configuração IP do MetroCluster.

Você só pode executar operações do MetroCluster usando o Gerenciador de sistema em uma configuração IP do MetroCluster. Em uma configuração MetroCluster FC, você ainda pode usar o Gerenciador do sistema para gerenciar cada nó na configuração do MetroCluster, mas não pode executar nenhuma operação específica do MetroCluster.

Normalmente, você configura e configura clusters em uma configuração do MetroCluster em dois locais geográficos separados. Em seguida, configure o peering entre os clusters para que eles sincronizem e compartilhem dados. Os dois clusters na rede com peering fornecem recuperação de desastres (DR) bidirecional, onde cada cluster pode ser a origem e o backup do outro cluster. Em configurações IP do MetroCluster de oito ou quatro nós, cada local consiste em controladores de storage configurados como um ou dois pares de alta disponibilidade (HA).

Em um terceiro local, é possível "Instale o serviço do Mediador ONTAP"monitorar o estado dos nós e seus parceiros de DR. O serviço de Mediador ONTAP pode implementar um switchover não planejado assistido por Mediador (MAUSO) em caso de desastre.

Você também pode executar um switchover negociado a fim de reduzir um dos clusters para manutenção planejada. O cluster de parceiros manipula todas as operações de e/S de dados dos dois clusters até você abrir o cluster no qual você realizou a manutenção e executar uma operação de switchback.

Você pode encontrar procedimentos para configurar e gerenciar uma configuração IP do MetroCluster usando o Gerenciador de sistema no "Documentação do MetroCluster".

Proteção de dados usando backup em fita

Visão geral do backup em fita do FlexVol volumes

O ONTAP oferece suporte a backup e restauração em fita por meio do protocolo NDMP (Network Data Management Protocol). O NDMP permite que você faça backup de dados em sistemas de armazenamento diretamente para fita, resultando em uso eficiente da largura de banda da rede. O ONTAP suporta ambos os motores dump e SMTape para backup em fita.

Você pode executar um backup ou restauração de despejo ou SMTape usando aplicativos de backup compatíveis com NDMP. Apenas a versão NDMP 4 é suportada.

Backup em fita usando despejo

Dump é um backup baseado em cópia Snapshot no qual os dados do sistema de arquivos são copiados para a fita. O mecanismo de despejo do ONTAP faz backup de arquivos, diretórios e as informações da lista de controle de acesso (ACL) aplicáveis à fita. É possível fazer backup de um volume inteiro, de uma qtree inteira ou de uma subárvore que não seja um volume inteiro ou uma qtree inteiro. O dump suporta backups de linha de base, diferenciais e incrementais.

Backup em fita usando SMTape

O SMTape é uma solução de recuperação de desastres baseada em cópia Snapshot da ONTAP que faz backup de blocos de dados em fita. Você pode usar o SMTape para realizar backups de volume em fitas. No entanto, você não pode executar um backup no nível de qtree ou subárvore. O SMTape suporta backups de linha de base, diferenciais e incrementais.

A partir do ONTAP 9.13,1, o backup de fita usando Sincronização ativa do SnapMirroro SMTape é compatível com o .

Fluxo de trabalho de backup e restauração em fita

Você pode executar operações de backup e restauração em fita usando um aplicativo de

backup habilitado para NDMP.

Sobre esta tarefa

O fluxo de trabalho de backup e restauração de fita fornece uma visão geral das tarefas envolvidas na execução de operações de backup e restauração de fita. Para obter informações detalhadas sobre como executar uma operação de backup e restauração, consulte a documentação do aplicativo de backup.

Passos

1. Configure uma configuração de biblioteca de fitas escolhendo uma topologia de fita compatível com NDMP.
2. Habilite serviços NDMP em seu sistema de storage.

   Você pode ativar os serviços NDMP no nível de nó ou no nível de máquina virtual de storage (SVM). Isso depende do modo NDMP no qual você optar por executar a operação de backup e restauração de fita.

3. Use as opções NDMP para gerenciar o NDMP em seu sistema de storage.

   Você pode usar opções NDMP no nível de nó ou no nível SVM. Isso depende do modo NDMP no qual você optar por executar a operação de backup e restauração de fita.

   Você pode modificar as opções NDMP no nível do nó usando o `system services ndmp modify` comando e no nível SVM usando o `vserver services ndmp modify` comando. Para obter mais informações sobre esses comandos, consulte as páginas man.

4. Execute uma operação de backup ou restauração em fita usando um aplicativo de backup habilitado para NDMP.

   O ONTAP suporta ambos os motores dump e SMTape para backup e restauração de fita.

   Para obter mais informações sobre como usar o aplicativo de backup (também chamado de *Data Management Applications* ou *DMAs*) para executar operações de backup ou restauração, consulte a documentação do aplicativo de backup.

Informações relacionadas

Topologias comuns de backup de fita NDMP

Compreender o motor de descarga para volumes FlexVol

Casos de uso para escolher um mecanismo de backup de fita

O ONTAP suporta dois mecanismos de backup: SMTape e dump. Você deve estar ciente dos casos de uso dos mecanismos de backup SMTape e dump para ajudá-lo a escolher o mecanismo de backup para executar operações de backup e restauração de fita.

O despejo pode ser usado nos seguintes casos:

- Direct Access Recovery (DAR) de arquivos e diretórios
- Backup de um subconjunto de subdiretórios ou arquivos em um caminho específico
- Excluindo arquivos e diretórios específicos durante backups
- Preservando o backup por longos períodos

SMTape pode ser usado nos seguintes casos:

- Solução de recuperação de desastres
- Preservar a economia de deduplicação e as configurações de deduplicação nos dados de backup durante uma operação de restauração
- Backup de grandes volumes

Gerenciar unidades de fita

Visão geral de gerenciar unidades de fita

Você pode verificar as conexões da biblioteca de fitas e exibir informações da unidade de fita antes de executar uma operação de backup ou restauração de fita. Você pode usar uma unidade de fita não qualificada emulando-a em uma unidade de fita qualificada. Você também pode atribuir e remover aliases de fita, além de exibir aliases existentes.

Quando você faz backup de dados para fita, os dados são armazenados em arquivos de fita. As marcas de arquivo separam os arquivos de fita e os arquivos não têm nomes. Você especifica um arquivo de fita pela sua posição na fita. Você escreve um arquivo de fita usando um dispositivo de fita. Ao ler o arquivo de fita, você deve especificar um dispositivo que tenha o mesmo tipo de compactação usado para gravar esse arquivo de fita.

Comandos para gerenciar unidades de fita, trocadores de Mídia e operações de unidade de fita

Existem comandos para visualizar informações sobre unidades de fita e trocadores de Mídia em um cluster, colocar uma unidade de fita on-line e colocá-la off-line, modificar a posição do cartucho da unidade de fita, definir e limpar o nome do alias da unidade de fita e redefinir uma unidade de fita. Você também pode exibir e redefinir estatísticas de unidade de fita.

Se você quiser…	Use este comando…
Coloque uma unidade de fita on-line	`storage tape online`
Limpe um nome de alias para unidade de fita ou trocador de Mídia	`storage tape alias clear`
Ative ou desative uma operação de rastreamento de fita para uma unidade de fita	`storage tape trace`
Modifique a posição do cartucho da unidade de fita	`storage tape position`
Redefina uma unidade de fita	`storage tape reset` Este comando está disponível apenas no nível avançado de privilégios.

Se você quiser…	Use este comando…
Defina um nome de alias para unidade de fita ou trocador de Mídia	`storage tape alias set`
Tire uma unidade de fita off-line	`storage tape offline`
Veja informações sobre todas as unidades de fita e trocadores de Mídia	`storage tape show`
Exibir informações sobre unidades de fita conetadas ao cluster	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Veja informações sobre os modificadores de Mídia conetados ao cluster	`storage tape show-media-changer`
Exibir informações de erro sobre unidades de fita conetadas ao cluster	`storage tape show-errors`
Veja todas as unidades de fita qualificadas e compatíveis do ONTAP conetadas a cada nó no cluster	`storage tape show-supported-status`
Exibir aliases de todas as unidades de fita e alteradores de Mídia conetados a cada nó no cluster	`storage tape alias show`
Redefina a leitura de estatísticas de uma unidade de fita para zero	`storage stats tape zero tape_name` Você deve usar este comando no nodeshell.
Ver unidades de fita suportadas pelo ONTAP	`storage show tape supported [-v]` Você deve usar este comando no nodeshell. Você pode usar a `-v` opção para exibir mais detalhes sobre cada unidade de fita.
Veja as estatísticas do dispositivo de fita para entender o desempenho da fita e verificar o padrão de uso	`storage stats tape tape_name` Você deve usar este comando no nodeshell.

Para obter mais informações sobre esses comandos, consulte as páginas man.

Use uma unidade de fita não qualificada

Você pode usar uma unidade de fita não qualificada em um sistema de storage se ele puder emular uma unidade de fita qualificada. É então Tratado como uma unidade de fita qualificada. Para usar uma unidade de fita não qualificada, primeiro você deve

determinar se ela emula qualquer uma das unidades de fita qualificadas.

Sobre esta tarefa

Uma unidade de fita não qualificada é aquela que está conetada ao sistema de storage, mas não é suportada ou reconhecida pela ONTAP.

Passos

1. Visualize as unidades de fita não qualificadas conetadas a um sistema de armazenamento usando o `storage tape show-supported-status` comando.

   O comando a seguir exibe as unidades de fita conetadas ao sistema de armazenamento e o status de suporte e qualificação de cada unidade de fita. As unidades de fita não qualificadas também são listadas. `tape_drive_vendor_name` É uma unidade de fita não qualificada conetada ao sistema de storage, mas não suportada pelo ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Emular a unidade de fita qualificada.

   "Downloads do NetApp: Arquivos de configuração do dispositivo de fita"

Informações relacionadas

Quais são as unidades de fita qualificadas

Atribua aliases de fita

Para facilitar a identificação do dispositivo, você pode atribuir aliases de fita a uma unidade de fita ou trocador de médio porte. Os aliases fornecem uma correspondência entre os nomes lógicos dos dispositivos de backup e um nome atribuído permanentemente à unidade de fita ou ao trocador de Mídia.

Passos

1. Atribua um alias a uma unidade de fita ou trocador de médio usando o `storage tape alias set` comando.

Para obter mais informações sobre esse comando, consulte as páginas man.

Você pode visualizar as informações do número de série (SN) sobre as unidades de fita usando o `system node hardware tape drive show` comando e sobre bibliotecas de fitas usando os `system node hardware tape library show` comandos.

O comando a seguir define um nome de alias para uma unidade de fita com o número de série SN[123456]L4 anexado ao nó, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

O comando a seguir define um nome de alias para um trocador de Mídia com número de série SN[65432] anexado ao nó, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

Informações relacionadas

O que é a distorção da fita

Removendo aliases de fita

Remover aliases de fita

Você pode remover aliases usando o `storage tape alias clear` comando quando aliases persistentes não são mais necessários para uma unidade de fita ou um trocador de médio.

Passos

1. Remova um alias de uma unidade de fita ou trocador de médio usando o `storage tape alias clear` comando.

   Para obter mais informações sobre esse comando, consulte as páginas man.

   O comando a seguir remove os aliases de todas as unidades de fita especificando o escopo da operação de eliminação de alias para `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Depois de terminar

Se você estiver executando uma operação de backup ou restauração de fita usando NDMP, depois de remover um alias de uma unidade de fita ou trocador de médio porte, você deve atribuir um novo nome de alias à unidade de fita ou trocador de médio para continuar o acesso ao dispositivo de fita.

Informações relacionadas

O que é a distorção da fita

Atribuindo aliases de fita

Ativar ou desativar reservas de fita

Você pode controlar como o ONTAP gerencia as reservas de dispositivos de fita usando a `tape.reservations` opção. Por padrão, a reserva de fita é desativada.

Sobre esta tarefa

Ativar a opção de reservas de fita pode causar problemas se as unidades de fita, trocadores médios, pontes ou bibliotecas não funcionarem corretamente. Se os comandos de fita relatarem que o dispositivo está reservado quando nenhum outro sistema de armazenamento está usando o dispositivo, essa opção deve ser desativada.

Passos

1. Para usar o mecanismo de reserva/Liberação SCSI ou SCSI Persistent Reservationsor para desativar as reservas de fita, digite o seguinte comando no clustershell:

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi` Seleciona o mecanismo de reserva/Liberação SCSI.

   `persistent` Seleciona as reservas persistentes SCSI.

   `off` desativa as reservas de fita.

Informações relacionadas

Quais são as reservas de fita

Comandos para verificar as conexões da biblioteca de fitas

Você pode exibir informações sobre o caminho de conexão entre um sistema de armazenamento e uma configuração de biblioteca de fitas conetada ao sistema de armazenamento. Você pode usar essas informações para verificar o caminho de conexão para a configuração da biblioteca de fitas ou para solucionar problemas relacionados aos caminhos de conexão.

Você pode exibir os detalhes da biblioteca de fitas a seguir para verificar as conexões da biblioteca de fitas depois de adicionar ou criar uma nova biblioteca de fitas, ou depois de restaurar um caminho com falha em um acesso de caminho único ou multipath a uma biblioteca de fitas. Você também pode usar essas informações ao solucionar erros relacionados ao caminho ou se o acesso a uma biblioteca de fitas falhar.

- Nó ao qual a biblioteca de fitas está conetada
- ID do dispositivo
- Caminho NDMP
- Nome da biblioteca de fitas
- IDs da porta de destino e da porta do iniciador
- Acesso de caminho único ou multipath a uma biblioteca de fitas para cada porta de destino ou iniciador de

FC

- Detalhes de integridade de dados relacionados ao caminho, como "'erros de caminho'" e "'caminho qual'"
- Grupos LUN e contagens LUN

Se você quiser…	Use este comando…
Exibir informações sobre uma biblioteca de fitas em um cluster	`system node hardware tape library show`
Exibir informações de caminho para uma biblioteca de fitas	`storage tape library path show`
Exibir informações de caminho para uma biblioteca de fitas para cada porta do iniciador	`storage tape library path show-by-initiator`
Exibir informações de conetividade entre uma biblioteca de fitas de armazenamento e um cluster	`storage tape library config show`

Para obter mais informações sobre esses comandos, consulte as páginas man.

Sobre unidades de fita

Visão geral das unidades de fita qualificadas

Você deve usar uma unidade de fita qualificada que tenha sido testada e encontrada para funcionar corretamente em um sistema de armazenamento. Você pode seguir a distorção da fita e também ativar as reservas de fita para garantir que apenas um sistema de armazenamento acesse uma unidade de fita em qualquer momento específico.

Uma unidade de fita qualificada é uma unidade de fita que foi testada e encontrada para funcionar corretamente em sistemas de armazenamento. Você pode qualificar unidades de fita para versões existentes do ONTAP usando o arquivo de configuração de fita.

Formato do ficheiro de configuração da cassete

O formato do arquivo de configuração da fita consiste em campos como ID do fornecedor, ID do produto e detalhes dos tipos de compactação para uma unidade de fita. Este arquivo também consiste em campos opcionais para ativar o recurso de autoload de uma unidade de fita e alterar os valores de tempo limite do comando de uma unidade de fita.

A tabela a seguir exibe o formato do arquivo de configuração da fita:

Item	Tamanho	Descrição
`vendor_id` (string)	até 8 bytes	O ID do fornecedor conforme relatado pelo `SCSI Inquiry` comando.
`product_id`(string)	até 16 bytes	O ID do produto conforme relatado pelo `SCSI Inquiry` comando.
`id_match_size`(número)		O número de bytes do ID do produto a ser usado para correspondência para detetar a unidade de fita a ser identificada, começando com o primeiro caractere do ID do produto nos dados de consulta.
`vendor_pretty` (string)	até 16 bytes	Se este parâmetro estiver presente, ele será especificado pela cadeia de carateres exibida pelo comando `storage tape show -device-names`; caso contrário, INQ_VENDOR_ID será exibido.
`product_pretty`(string)	até 16 bytes	Se este parâmetro estiver presente, ele será especificado pela cadeia de carateres exibida pelo comando `storage tape show -device-names`; caso contrário, INQ_PRODUCT_ID será exibido.

Os `vendor_pretty` campos e `product_pretty` são opcionais, mas se um desses campos tiver um valor, o outro também deve ter um valor.

A tabela a seguir explica a descrição, o código de densidade e o algoritmo de compressão para os vários tipos de compactação, como `l`, `m`, `h` e `a`:

Item	Tamanho	Descrição
`{l	m	h
a}_description=(string)`	até 24 bytes	A cadeia de carateres a imprimir para o comando nodeshell , `sysconfig -t`, que descreve as caraterísticas da configuração de densidade específica.

Item	Tamanho	Descrição
`{l	m	h
a}_density=(hex codes)`		O código de densidade a ser definido no descritor de bloco de página do modo SCSI correspondente ao código de densidade desejado para l, m, h ou a.
`{l	m	h
a}_algorithm=(hex codes)`		O algoritmo de compressão a ser definido na página do modo de compressão SCSI correspondente ao código de densidade e à caraterística de densidade desejada.

A tabela a seguir descreve os campos opcionais disponíveis no arquivo de configuração da fita:

Campo	Descrição
`autoload=(Boolean yes/no)`	Este campo é definido como `yes` se a unidade de fita tiver um recurso de carregamento automático; ou seja, depois que o cartucho de fita é inserido, a unidade de fita fica pronta sem a necessidade de executar um `SCSI load` comando (unidade de inicialização/parada). A predefinição para este campo é `no`.
`cmd_timeout_0x`	Valor de tempo limite individual. Você deve usar este campo somente se quiser especificar um valor de tempo limite diferente daquele que está sendo usado como padrão pelo driver de fita. O arquivo de exemplo lista os valores padrão de tempo limite do comando SCSI usados pela unidade de fita. O valor de tempo limite pode ser expresso em minutos (m), segundos (s) ou milissegundos (ms). Não deve alterar este campo.

Você pode baixar e exibir o arquivo de configuração de fita no site de suporte da NetApp.

Exemplo de um formato de arquivo de configuração de fita

O formato de arquivo de configuração de fita para a unidade de fita HP LTO5 ULTRIUM é o seguinte:

`vendor_id`"HP"

`product_id`Ultrium 5-SCSI

`id_match_size`9

`vendor_pretty`Hewlett-Packard

`product_pretty`"LTO-5"

`l_description`LTO-3(ro)/4 4/800GB"

`l_density`0x00

`l_algorithm`0x00

`m_description`LTO-3(ro)/4 8/1600GB cmp"

`m_density`0x00

`m_algorithm`0 x 01

`h_description`"LTO-5 1600GB"

`h_density`0 x 58

`h_algorithm`0x00

`a_description`LTO-5 3200GB cmp

`a_density`0 x 58

`a_algorithm`0 x 01

`autoload`"sim"

Informações relacionadas

"Ferramentas do NetApp: Arquivos de configuração do dispositivo de fita"

Como o sistema de armazenamento qualifica uma nova unidade de fita dinamicamente

O sistema de armazenamento qualifica uma unidade de fita dinamicamente, combinando a ID do fornecedor e a ID do produto com as informações contidas na tabela de qualificação da fita.

Quando você coneta uma unidade de fita ao sistema de armazenamento, ela procura uma correspondência de ID de fornecedor e ID de produto entre as informações obtidas durante a descoberta de fita e as informações na tabela de qualificação de fita interna. Se o sistema de armazenamento detetar uma correspondência, ele marca a unidade de fita como qualificada e pode acessar a unidade de fita. Se o sistema de armazenamento não conseguir encontrar uma correspondência, a unidade de fita permanece no estado não qualificado e não é acessada.

Visão geral dos dispositivos de fita

Visão geral dos dispositivos de fita

Um dispositivo de fita é uma representação de uma unidade de fita. É uma combinação específica do tipo de rebobinagem e capacidade de compressão de uma unidade de fita.

Um dispositivo de fita é criado para cada combinação de tipo de rebobinagem e capacidade de compressão. Portanto, uma unidade de fita ou biblioteca de fitas pode ter vários dispositivos de fita associados a ela. Você deve especificar um dispositivo de fita para mover, gravar ou ler fitas.

Quando você instala uma unidade de fita ou uma biblioteca de fitas em um sistema de armazenamento, o ONTAP cria dispositivos de fita associados à unidade de fita ou à biblioteca de fitas.

O ONTAP deteta unidades de fita e bibliotecas de fitas e atribui números lógicos e dispositivos de fita a elas. O ONTAP deteta as bibliotecas e unidades de fita Fibre Channel, SAS e SCSI paralelo quando elas são conetadas às portas de interface. O ONTAP deteta essas unidades quando suas interfaces estão ativadas.

Formato do nome do dispositivo de fita

Cada dispositivo de fita tem um nome associado que aparece em um formato definido. O formato inclui informações sobre o tipo de dispositivo, tipo de rebobinagem, alias e tipo de compressão.

O formato do nome de um dispositivo de fita é o seguinte:

`rewind_type st alias_number compression_type`

`rewind_type` é o tipo de rebobinagem.

A lista a seguir descreve os vários valores do tipo de rebobinagem:

- **r**

  ONTAP rebobinam a fita depois que ela termina de escrever o arquivo de fita.

- **nº**

  O ONTAP não volta a gravar a fita depois de terminar de escrever o arquivo de fita. Você deve usar esse tipo de rebobinagem quando quiser gravar vários arquivos de fita na mesma fita.

- **ur**

  Este é o tipo de retorno de descarga/recarga. Quando você usa esse tipo de rebobinagem, a biblioteca de fitas descarrega a fita quando ela chega ao final de um arquivo de fita e, em seguida, carrega a próxima fita, se houver uma.

  Você deve usar esse tipo de rebobinagem somente nas seguintes circunstâncias:

  - A unidade de fita associada a esse dispositivo está em uma biblioteca de fitas ou está em um trocador médio que está no modo de biblioteca.
  - A unidade de fita associada a este dispositivo está conetada a um sistema de armazenamento.
  - Fitas suficientes para a operação que você está executando estão disponíveis na sequência de fitas da biblioteca definida para esta unidade de fita.

Se você gravar uma fita usando um dispositivo sem rebobinagem, você deve rebobinar a fita antes de lê-la.

`st` é a designação padrão para uma unidade de fita.

`alias_number` É o alias que o ONTAP atribui à unidade de fita. Quando o ONTAP deteta uma nova unidade de fita, o ONTAP atribui um alias à unidade de fita.

`compression_type` é um código específico da unidade para a densidade de dados na fita e o tipo de compressão.

A lista a seguir descreve os vários valores para `compression_type`:

- **a**

  Compressão mais elevada

- **h**

  Alta compressão

- **m**

  Compressão média

- **l**

  Baixa compressão

Exemplos

`nrst0a` especifica um dispositivo sem rebobinagem na unidade de fita 0 usando a compressão mais alta.

Exemplo de uma lista de dispositivos de fita

O exemplo a seguir mostra os dispositivos de fita associados ao HP Ultrium 2-SCSI:

```
       Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,        format is: HP (200GB)
nrst0l -  no rewind device,     format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,        format is: HP (200GB)
nrst0m -  no rewind device,     format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,        format is: HP (200GB)
nrst0h -  no rewind device,     format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,        format is: HP (400GB w/comp)
nrst0a -  no rewind device,     format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

A lista a seguir descreve as abreviaturas no exemplo anterior:

- GB—Gigabytes; esta é a capacidade da fita.
- w/comp—com compressão; isto mostra a capacidade da fita com compressão.

Número suportado de dispositivos de fita simultâneos

O ONTAP suporta um máximo de 64 conexões simultâneas de unidade de fita, 16 trocadores médios e 16 dispositivos de bridge ou roteador para cada sistema de armazenamento (por nó) em qualquer combinação de anexos Fibre Channel, SCSI ou SAS.

As unidades de fita ou os trocadores médios podem ser dispositivos em bibliotecas de fitas físicas ou virtuais ou em dispositivos autônomos.

Embora um sistema de armazenamento possa detetar 64 conexões de unidade de fita, o número máximo de sessões de backup e restauração que podem ser executadas simultaneamente depende dos limites de escalabilidade do mecanismo de backup.

Informações relacionadas

Limites de escalabilidade para sessões de backup e restauração de despejo

Aliasing de fita

Visão geral da distorção da fita

Aliasing simplifica o processo de identificação do dispositivo. A distorção liga um nome de caminho físico (PPN) ou um número de série (SN) de uma fita ou um trocador de meio a um nome de alias persistente, mas modificável.

A tabela a seguir descreve como a distorção de fita permite garantir que uma unidade de fita (ou biblioteca de fitas ou trocador de médio) esteja sempre associada a um único nome de alias:

Cenário	Reatribuir o alias
Quando o sistema reinicia	A unidade de fita é reatribuída automaticamente seu alias anterior.
Quando um dispositivo de fita se move para outra porta	O alias pode ser ajustado para apontar para o novo endereço.
Quando mais de um sistema utiliza um dispositivo de fita específico	O usuário pode definir o alias para ser o mesmo para todos os sistemas.

Quando você atualiza do Data ONTAP 8.1.x para Data ONTAP 8.2.x, o recurso de alias de fita do Data ONTAP 8.2.x modifica os nomes de alias de fita existentes. Nesse caso, você pode ter que atualizar os nomes de alias de fita no aplicativo de backup.

A atribuição de aliases de fita fornece uma correspondência entre os nomes lógicos dos dispositivos de backup (por exemplo, st0 ou MC1) e um nome atribuído permanentemente a uma porta, uma unidade de fita

ou um trocador de Mídia.

st0 e st00 são nomes lógicos diferentes.

Nomes lógicos e números de série são usados apenas para acessar um dispositivo. Depois que o dispositivo é acessado, ele retorna todas as mensagens de erro usando o nome do caminho físico.

Existem dois tipos de nomes disponíveis para a distorção: Nome do caminho físico e número de série.

Quais são os nomes de caminhos físicos

Nomes de caminho físico (PPNs) são as sequências de endereços numéricos que o ONTAP atribui a unidades de fita e bibliotecas de fitas com base no adaptador ou switch SCSI-2/3 (local específico) que estão conetados ao sistema de armazenamento. PPNs também são conhecidos como nomes elétricos.

Os PPNs de dispositivos com conexão direta usam o seguinte formato `host_adapter:.device_id_lun`

O valor LUN é exibido apenas para dispositivos de troca de fita e médio cujos valores de LUN não são zero; ou seja, se o valor LUN for zero, a `lun` parte do PPN não é exibida.

Por exemplo, o PPN 8,6 indica que o número do adaptador host é 8, o ID do dispositivo é 6 e o número da unidade lógica (LUN) é 0.

Os dispositivos de fita SAS também são dispositivos de conexão direta. Por exemplo, o PPN 5c.4 indica que em um sistema de armazenamento, o HBA SAS está conetado no slot 5, a fita SAS está conetada à porta C do HBA SAS e o ID do dispositivo é 4.

Os PPNs de dispositivos conetados a switch Fibre Channel usam o seguinte formato `switch:port_id:.device_id_lun`

Por exemplo, o PPN my_SWITCH:5.3L2 indica que a unidade de fita conetada à porta 5 de um switch chamado MY_SWITCH está definida com ID de dispositivo 3 e tem o LUN 2.

O LUN (número de unidade lógica) é determinado pela unidade. Fibre Channel, unidades de fita SCSI e bibliotecas e discos têm PPNs.

Os PPNs de unidades de fita e bibliotecas não mudam a menos que o nome do switch mude, a unidade de fita ou a biblioteca se mova ou a unidade de fita ou a biblioteca seja reconfigurada. Os PPNs permanecem inalterados após a reinicialização. Por exemplo, se uma unidade de fita chamada MY_SWITCH:5.3L2 for removida e uma nova unidade de fita com o mesmo ID de dispositivo e LUN estiver conetada à porta 5 do switch my_SWITCH, a nova unidade de fita será acessível usando MY_SWITCH:5.3L2.

Quais são os números de série

Um número de série (SN) é um identificador exclusivo para uma unidade de fita ou um carregador médio. O ONTAP gera aliases baseados no SN em vez do WWN.

Como o SN é um identificador exclusivo para uma unidade de fita ou um trocador de médio, o alias permanece o mesmo independentemente dos caminhos de conexão múltiplos para a unidade de fita ou trocador de médio. Isso ajuda os sistemas de armazenamento a rastrear a mesma unidade de fita ou

carregador médio em uma configuração de biblioteca de fitas.

O SN de uma unidade de fita ou de um trocador de médio não muda mesmo se você renomear o switch Fibre Channel ao qual a unidade de fita ou o trocador de médio está conetado. No entanto, em uma biblioteca de fitas, se você substituir uma unidade de fita existente por uma nova, o ONTAP gera novos aliases porque o SN da unidade de fita muda. Além disso, se você mover uma unidade de fita existente para um novo slot em uma biblioteca de fitas ou remapear o LUN da unidade de fita, o ONTAP gera um novo alias para essa unidade de fita.

Você deve atualizar os aplicativos de backup com os aliases recém-gerados.

O SN de um dispositivo de fita usa o seguinte formato: `SN[xxxxxxxxxx]L[X]`

`x` É um caractere alfanumérico e `LX` é o LUN do dispositivo de fita. Se o LUN for 0, a parte `LX` da cadeia de carateres não será exibida.

Cada SN é composto por até 32 carateres; o formato para o SN não é sensível a maiúsculas e minúsculas.

Considerações ao configurar o acesso à fita multipath

Você pode configurar dois caminhos do sistema de armazenamento para acessar as unidades de fita em uma biblioteca de fitas. Se um caminho falhar, o sistema de armazenamento pode usar os outros caminhos para acessar as unidades de fita sem ter que reparar imediatamente o caminho com falha. Isso garante que as operações de fita possam ser reiniciadas.

Você deve considerar o seguinte ao configurar o acesso à fita multipath a partir do seu sistema de storage:

- Em bibliotecas de fitas que suportam mapeamento LUN, para acesso multipath a um grupo LUN, o mapeamento LUN deve ser simétrico em cada caminho.

  As unidades de fita e os modificadores de Mídia são atribuídos a grupos LUN (conjunto de LUNs que compartilham o mesmo conjunto de caminhos do iniciador) em uma biblioteca de fitas. Todas as unidades de fita de um grupo LUN devem estar disponíveis para operações de backup e restauração em todos os vários caminhos.

- Um máximo de dois caminhos pode ser configurado a partir do sistema de armazenamento para acessar as unidades de fita em uma biblioteca de fitas.
- O acesso à fita multipath é compatível com o balanceamento de carga. O balanceamento de carga está desativado por padrão.

No exemplo a seguir, o sistema de armazenamento acessa o grupo LUN 0 através de dois caminhos de iniciador: 0B e 0d. Em ambos os caminhos, o grupo LUN tem o mesmo número de LUN, 0 e contagem de LUN, 5. O sistema de armazenamento acede ao grupo LUN 1 através de apenas um caminho de iniciador, 3D.

```
STSW-3070-2_cluster::> storage tape library config show

Node                    LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Para obter mais informações, consulte as páginas de manual.

Como você adiciona unidades de fita e bibliotecas aos sistemas de armazenamento

Você pode adicionar unidades de fita e bibliotecas ao sistema de armazenamento dinamicamente (sem colocar o sistema de armazenamento offline).

Quando você adiciona um novo trocador médio, o sistema de armazenamento deteta sua presença e adiciona-a à configuração. Se o trocador de meio já estiver referenciado nas informações de alias, não serão criados novos nomes lógicos. Se a biblioteca não for referenciada, o sistema de armazenamento cria um novo alias para o trocador de médio.

Em uma configuração de biblioteca de fitas, você deve configurar uma unidade de fita ou um carregador médio no LUN 0 de uma porta de destino para o ONTAP descobrir todos os trocadores médios e unidades de fita nessa porta de destino.

Quais são as reservas de fita

Vários sistemas de armazenamento podem compartilhar o acesso a unidades de fita, trocadores médios, pontes ou bibliotecas de fitas. As reservas de fita garantem que apenas um sistema de armazenamento acesse um dispositivo em qualquer momento específico, ativando o mecanismo de reserva/Liberação SCSI ou as reservas persistentes SCSI para todas as unidades de fita, trocadores médios, bridges e bibliotecas de fitas.

Todos os sistemas que compartilham dispositivos em uma biblioteca, independentemente de os switches estarem envolvidos ou não, devem usar o mesmo método de reserva.

O mecanismo de reserva/Liberação SCSI para reservar dispositivos funciona bem em condições normais. No entanto, durante os procedimentos de recuperação de erros de interface, as reservas podem ser perdidas. Se isso ocorrer, iniciadores que não o proprietário reservado podem acessar o dispositivo.

As reservas feitas com SCSI Persistent Reservations não são afetadas por mecanismos de recuperação de

erros, como restauração de loop ou restauração de destino; no entanto, nem todos os dispositivos implementam as reservas persistentes SCSI corretamente.

Transfira dados usando ndmpcopy

Transfira dados usando a visão geral do ndmpcopy

O `ndmpcopy` comando nodeshell transfere dados entre sistemas de storage que suportam o NDMP v4. Você pode realizar transferências de dados completas e incrementais. Você pode transferir volumes completos ou parciais, qtrees, diretórios ou arquivos individuais.

Sobre esta tarefa

Usando o ONTAP 8.x e versões anteriores, as transferências incrementais são limitadas a um máximo de dois níveis (um total e até dois backups incrementais).

A partir do ONTAP 9.0 e versões posteriores, as transferências incrementais são limitadas a um máximo de nove níveis (um backup completo e até nove backups incrementais).

Você pode executar `ndmpcopy` na linha de comando nodeshell dos sistemas de armazenamento de origem e destino, ou um sistema de armazenamento que não seja a origem nem o destino da transferência de dados. Você também pode executar `ndmpcopy` em um único sistema de armazenamento que seja a origem e o destino da transferência de dados.

Você pode usar endereços IPv4 ou IPv6 dos sistemas de armazenamento de origem e destino no `ndmpcopy` comando. O formato do caminho é `/vserver_name/volume_name \[path\]`.

Passos

1. Habilite o serviço NDMP nos sistemas de storage de origem e destino:

Se estiver a efetuar a transferência de dados na origem ou destino em…	Use o seguinte comando…
Modo NDMP com escopo SVM	`vserver services ndmp on` Para autenticação NDMP no SVM admin, a conta de usuário é e a função de usuário `admin` é `admin` ou `backup`. No data SVM, a conta de usuário é `vsadmin` e a função de usuário é `vsadmin` ou `vsadmin-backup` função.
Modo NDMP com escopo de nó	`system services ndmp on`

2. Transfira dados dentro de um sistema de armazenamento ou entre sistemas de armazenamento usando o `ndmpcopy` comando no nodeshell:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
```

mcd {inet|inet6}] [-md {inet|inet6}]

> Nomes DNS não são suportados no ndmpcopy. Você deve fornecer o endereço IP da origem e do destino. O endereço de loopback (127,0.0,1) não é suportado para o endereço IP de origem ou o endereço IP de destino.

- O `ndmpcopy` comando determina o modo de endereço para conexões de controle da seguinte forma:
  - O modo de endereço para conexão de controle corresponde ao endereço IP fornecido.
  - Você pode substituir essas regras usando as `-mcs` opções e. `-mcd`
- Se a origem ou o destino for o sistema ONTAP, então, dependendo do modo NDMP (com escopo de nó ou escopo SVM), use um endereço IP que permita acesso ao volume de destino.
- `source_path` e `destination_path` são os nomes de caminho absolutos até o nível granular de volume, qtree, diretório ou arquivo.
- `-mcs` especifica o modo de endereçamento preferido para a conexão de controle ao sistema de armazenamento de origem.

  `inet` Indica um modo de endereço IPv4 e `inet6` indica um modo de endereço IPv6.

- `-mcd` especifica o modo de endereçamento preferido para a conexão de controle ao sistema de armazenamento de destino.

  `inet` Indica um modo de endereço IPv4 e `inet6` indica um modo de endereço IPv6.

- `-md` especifica o modo de endereçamento preferido para transferências de dados entre os sistemas de armazenamento de origem e destino.

  `inet` Indica um modo de endereço IPv4 e `inet6` indica um modo de endereço IPv6.

  Se você não usar a `-md` opção no `ndmpcopy` comando, o modo de endereçamento para a conexão de dados é determinado da seguinte forma:

  - Se um dos endereços especificados para as conexões de controle for um endereço IPv6, o modo de endereço para a conexão de dados é IPv6.
  - Se ambos os endereços especificados para as conexões de controle forem endereços IPv4, o `ndmpcopy` comando tentará primeiro um modo de endereço IPv6 para a conexão de dados.

    Se isso falhar, o comando usará um modo de endereço IPv4.

    > Um endereço IPv6, se especificado, deve estar entre colchetes.

    Este comando de exemplo migra dados de um caminho de (`source_path`origem) para um caminho de (`destination_path`destino).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

Este comando de exemplo define explicitamente as conexões de controle e a conexão de dados para usar o modo de endereço IPv6:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Opções para o comando ndmpcopy

Você deve entender as opções disponíveis para o `ndmpcopy` comando nodeshell para transferir dados com sucesso.

A tabela a seguir lista as opções disponíveis. Para obter mais informações, consulte as `ndmpcopy` páginas de manual disponíveis através do nodeshell.

Opção	Descrição
`-sa username[password: ]`	Esta opção define o nome de usuário de autenticação de origem e a senha para conexão com o sistema de armazenamento de origem. Esta é uma opção obrigatória. Para um usuário sem privilégio de administrador, você deve especificar a senha específica do NDMP gerada pelo sistema do usuário. A senha gerada pelo sistema é obrigatória para usuários admin e não admin.
`-da username[password: ]`	Esta opção define o nome de utilizador e a palavra-passe de autenticação de destino para ligação ao sistema de armazenamento de destino. Esta é uma opção obrigatória.
`-st {md5`	`text`Selecione
Esta opção define o tipo de autenticação de origem a ser usado ao se conetar ao sistema de armazenamento de origem. Esta é uma opção obrigatória e, portanto, o usuário deve fornecer a `text` opção ou `md5`.	`-dt {md5`
`text`Selecione	Esta opção define o tipo de autenticação de destino a ser usado ao se conetar ao sistema de armazenamento de destino.

Opção	Descrição
`-l`	Esta opção define o nível de despejo usado para a transferência para o valor especificado de level.valid values are `0 1` , , to `9`, where `0` indica uma transferência completa e `1 9` especifica uma transferência incremental. A predefinição é `0`.
`-d`	Esta opção permite a geração de mensagens de log de depuração ndmpcopy. Os arquivos de log de depuração do ndmpcopy estão localizados no `/mroot/etc/log` volume raiz. Os nomes dos arquivos de log de depuração do ndmpcopy estão no `ndmpcopy.yyyymmdd` formato.
`-f`	Esta opção ativa o modo forçado. Este modo permite que os arquivos do sistema sejam sobrescritos no `/etc` diretório na raiz do volume do 7-Mode.
`-h`	Esta opção imprime a mensagem de ajuda.
`-p`	Esta opção solicita que você insira a senha para autorização de origem e destino. Esta palavra-passe substitui a palavra-passe especificada para `-sa` as opções e. `-da` Você pode usar essa opção somente quando o comando estiver sendo executado em um console interativo.
`-exclude`	Esta opção exclui arquivos ou diretórios especificados do caminho especificado para transferência de dados. O valor pode ser uma lista separada por vírgulas de nomes de diretórios ou arquivos, como **`.pst`** `.txt` ou .

NDMP para volumes FlexVol

Sobre o NDMP para volumes FlexVol

O Network Data Management Protocol (NDMP) é um protocolo padronizado para controle de backup, recuperação e outros tipos de transferência de dados entre dispositivos de armazenamento primário e secundário, como sistemas de armazenamento e bibliotecas de fitas.

Ao ativar o suporte NDMP em um sistema de armazenamento, você permite que esse sistema de armazenamento se comunique com aplicativos de backup conetados à rede habilitados para NDMP (também chamados de *Data Management Applications* ou *DMAs*), servidores de dados e servidores de fita participantes de operações de backup ou recuperação. Todas as comunicações de rede ocorrem através da

rede TCPIP ou TCP/IPv6. O NDMP também fornece controle de baixo nível de unidades de fita e trocadores médios.

Você pode executar operações de backup em fita e restauração no modo NDMP com escopo de nó ou no modo NDMP com escopo de máquina virtual de armazenamento (SVM).

Você deve estar ciente das considerações que você deve levar em conta ao usar NDMP, lista de variáveis de ambiente e topologias de backup em fita NDMP compatíveis. Você também pode ativar ou desativar a funcionalidade DAR aprimorada. Os dois métodos de autenticação suportados pelo ONTAP para autenticar o acesso NDMP a um sistema de armazenamento são: Texto simples e desafio.

Informações relacionadas

Variáveis de ambiente suportadas pelo ONTAP

Sobre os modos de operação NDMP

Sobre os modos de operação NDMP

Você pode optar por realizar backup em fita e restaurar operações no nível do nó ou no nível da máquina virtual de storage (SVM). Para realizar essas operações com sucesso no nível do SVM, o serviço NDMP precisa estar habilitado no SVM.

Se você atualizar do Data ONTAP 8.2 para o Data ONTAP 8.3, o modo de operação NDMP usado no 8,2 continuará sendo mantido após a atualização de 8,2 para 8,3.

Se você instalar um novo cluster com o Data ONTAP 8.2 ou posterior, o NDMP estará no modo NDMP com escopo SVM por padrão. Para executar operações de backup e restauração de fita no modo NDMP com escopo de nó, você deve ativar explicitamente o modo NDMP com escopo de nó.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo de nó

Gerenciamento do modo NDMP com escopo de nó para volumes FlexVol

Gerenciamento do modo NDMP com escopo da SVM para volumes FlexVol

Qual é o modo NDMP com escopo de nó

No modo NDMP com escopo de nó, você pode executar operações de backup em fita e restauração no nível do nó. O modo NDMP de operação usado no Data ONTAP 8.2 continuará sendo mantido após a atualização de 8,2 para 8,3.

No modo NDMP com escopo de nó, você pode executar operações de backup em fita e restauração em um nó que possua o volume. Para executar essas operações, você deve estabelecer conexões de controle NDMP em um LIF hospedado no nó que possui o volume ou os dispositivos de fita.

Este modo está obsoleto e será removido em uma futura versão principal.

Informações relacionadas

Gerenciamento do modo NDMP com escopo de nó para volumes FlexVol

Qual é o modo NDMP com escopo SVM

Você pode executar com êxito as operações de backup em fita e restauração no nível da máquina virtual de storage (SVM) se o serviço NDMP estiver habilitado no SVM. Você pode fazer backup e restaurar todos os volumes hospedados em diferentes nós na SVM de um cluster, se a aplicação de backup suportar a EXTENSÃO CAB.

Uma conexão de controle NDMP pode ser estabelecida em diferentes tipos de LIF. No modo NDMP com escopo da SVM, esses LIFs pertencem ao data SVM ou admin SVM. A conexão pode ser estabelecida em um LIF somente se o serviço NDMP estiver habilitado no SVM que possui esse LIF.

Um LIF de dados pertence ao data SVM e o LIF entre clusters, LIF de gerenciamento de nós e LIF de clusters pertencem ao administrador SVM.

No modo NDMP com escopo SVM, a disponibilidade de volumes e dispositivos de fita para operações de backup e restauração depende do tipo de LIF no qual a conexão de controle NDMP é estabelecida e do status da extensão DA CABINE. Se o aplicativo de backup suportar a EXTENSÃO CAB e um volume e o dispositivo de fita compartilharem a mesma afinidade, o aplicativo de backup poderá executar uma operação de backup ou restauração local, em vez de uma operação de backup ou restauração de três vias.

Informações relacionadas

Gerenciamento do modo NDMP com escopo da SVM para volumes FlexVol

Considerações ao usar NDMP

Você precisa levar em conta várias considerações ao iniciar o serviço NDMP no sistema de storage.

- Cada nó dá suporte a um máximo de 16 backups, restaurações ou combinações simultâneos dos dois usando unidades de fita conetadas.
- Os serviços NDMP podem gerar dados do histórico de arquivos a pedido de aplicativos de backup NDMP.

  O histórico de arquivos é usado por aplicativos de backup para permitir a recuperação otimizada de subconjuntos de dados selecionados de uma imagem de backup. A geração e o processamento do histórico de arquivos podem consumir muito tempo e uso intenso de CPU para o sistema de storage e para o aplicativo de backup.

  SMTape não suporta histórico de arquivos.

  Se sua proteção de dados estiver configurada para recuperação de desastres - onde toda a imagem de backup será recuperada - você pode desativar a geração do histórico de arquivos para reduzir o tempo de backup. Consulte a documentação do aplicativo de backup para determinar se é possível desativar a geração do histórico de arquivos NDMP.

- A política de firewall para NDMP é ativada por padrão em todos os tipos de LIF.
- No modo NDMP com escopo de nó, o backup de um FlexVol volume requer que você use o aplicativo de backup para iniciar um backup em um nó que possua o volume.

  No entanto, não é possível fazer backup de um volume raiz de nó.

- Você pode executar backup NDMP de qualquer LIF conforme permitido pelas políticas de firewall.

Se você usar um LIF de dados, deverá selecionar um LIF que não esteja configurado para failover. Se um LIF de dados falhar durante uma operação NDMP, a operação NDMP falhará e deverá ser executada novamente.

- No modo NDMP com escopo de nó e no modo NDMP com escopo de máquina virtual de armazenamento (SVM) sem suporte de extensão DE CAB, a conexão de dados NDMP usa o mesmo LIF da conexão de controle NDMP.
- Durante a migração de LIF, as operações de backup e restauração contínuas são interrompidas.

  Você deve iniciar as operações de backup e restauração após a migração de LIF.

- O caminho de backup NDMP é do formato */vserver_name/volume_name/path_name*.

  path_name É opcional e especifica o caminho do diretório, arquivo ou cópia Snapshot.

- Quando um destino SnapMirror é feito backup em fita usando o mecanismo de despejo, apenas os dados no volume são copiados.

  No entanto, se um destino SnapMirror for feito backup em fita usando SMTape, os metadados também serão copiados. As relações do SnapMirror e os metadados associados não são copiados para a fita. Portanto, durante a restauração, apenas os dados nesse volume são restaurados, mas as relações SnapMirror associadas não são restauradas.

Informações relacionadas

O que a extensão Cluster Aware Backup faz

"Administração do sistema"

Variável de ambiente

Visão geral das variáveis de ambiente

As variáveis de ambiente são usadas para comunicar informações sobre uma operação de backup ou restauração entre um aplicativo de backup habilitado para NDMP e um sistema de armazenamento.

Por exemplo, se um usuário especificar que um aplicativo de backup deve fazer `/vserver1/vol1/dir1` backup , o aplicativo de backup define a variável de ambiente DO SISTEMA DE ARQUIVOS como `/vserver1/vol1/dir1`. Da mesma forma, se um usuário especificar que um backup deve ser um backup de nível 1, o aplicativo de backup define a variável de ambiente de NÍVEL como 1 (um).

A configuração e a análise de variáveis de ambiente são geralmente transparentes para os administradores de backup, ou seja, o aplicativo de backup as define automaticamente.

Um administrador de backup raramente especifica variáveis de ambiente; no entanto, você pode querer alterar o valor de uma variável de ambiente daquele definido pelo aplicativo de backup para caraterizar ou contornar um problema funcional ou de desempenho. Por exemplo, um administrador pode querer desativar temporariamente a geração do histórico de arquivos para determinar se o processamento de informações do histórico de arquivos do aplicativo de backup está contribuindo para problemas de desempenho ou problemas funcionais.

Muitos aplicativos de backup fornecem um meio de substituir ou modificar variáveis de ambiente ou

especificar variáveis de ambiente adicionais. Para obter informações, consulte a documentação do aplicativo de backup.

Variáveis de ambiente suportadas pelo ONTAP

As variáveis de ambiente são usadas para comunicar informações sobre uma operação de backup ou restauração entre um aplicativo de backup habilitado para NDMP e um sistema de armazenamento. O ONTAP suporta variáveis de ambiente, que têm um valor padrão associado. No entanto, você pode modificar manualmente esses valores padrão.

Se você modificar manualmente os valores definidos pelo aplicativo de backup, o aplicativo pode se comportar de forma imprevisível. Isso ocorre porque as operações de backup ou restauração podem não estar fazendo o que o aplicativo de backup esperava que fizessem, mas em alguns casos, a modificação criteriosa pode ajudar a identificar ou solucionar problemas.

As tabelas a seguir listam as variáveis de ambiente cujo comportamento é comum para dump e SMTape e aquelas variáveis que são suportadas apenas para dump e SMTape. Essas tabelas também contêm descrições de como as variáveis de ambiente que são suportadas pelo ONTAP funcionam se forem usadas:

Na maioria dos casos, variáveis que têm o valor, `Y` também aceitam `T` e `N` também aceitam `F`.

Variáveis de ambiente suportadas para dump e SMTape

Variável de ambiente	Valores válidos	Padrão	Descrição
DEPURAR	`Y` ou `N`	`N`	Especifica que as informações de depuração são impressas.
SISTEMA DE FICHEIROS	`string`	`none`	Especifica o nome do caminho da raiz dos dados que estão sendo copiados.

Variável de ambiente	Valores válidos	Padrão	Descrição
NDMP_VERSION	`return_only`	`none`	Você não deve modificar a variável NDMP_VERSION. Criada pela operação de backup, a variável NDMP_VERSION retorna a versão NDMP. O ONTAP define a variável NDMP_VERSION durante um backup para uso interno e para passar para um aplicativo de backup para fins informativos. A versão NDMP de uma sessão NDMP não é definida com esta variável.
PATHNAME_SEPARATOR	`return_value`	`none`	Especifica o caractere separador do nome do caminho. Este caractere depende do backup do sistema de arquivos. Para ONTAP, o caractere "'/'" é atribuído a essa variável. O servidor NDMP define essa variável antes de iniciar uma operação de backup em fita.
TIPO	`dump` ou `smtape`	`dump`	Especifica o tipo de backup suportado para executar operações de backup e restauração em fita.
VERBOSO	`Y` ou `N`	`N`	Aumenta as mensagens de log durante a execução de uma operação de backup ou restauração de fita.

Variáveis de ambiente suportadas para dump

Variável de ambiente	Valores válidos	Padrão	Descrição
ACL_START	`return_only`	`none`	Criada pela operação de backup, a variável ACL_START é um valor de deslocamento usado por uma restauração de acesso direto ou operação de backup NDMP reiniciável. O valor de deslocamento é o deslocamento de byte no arquivo de despejo onde os dados ACL (passe V) começam e são retornados no final de um backup. Para que uma operação de restauração de acesso direto restaure corretamente os dados de backup, o valor ACL_START deve ser passado para a operação de restauração quando ela for iniciada. Uma operação de backup NDMP reiniciável usa o valor ACL_START para se comunicar com o aplicativo de backup onde a parte não reiniciável do fluxo de backup começa.

Variável de ambiente	Valores válidos	Padrão	Descrição
DATA_BASE	`0`, `-1`, ou `DUMP_DATE` valor	`-1`	Especifica a data de início para backups incrementais. Quando definido como `-1`, o especificador incremental BASE_DATE é desativado. Quando definido como `0` em um backup de nível 0, backups incrementais são ativados. Após o backup inicial, o valor da variável DUMP_DATE do backup incremental anterior é atribuído à variável BASE_DATE. Essas variáveis são uma alternativa aos backups incrementais baseados em NÍVEL/ATUALIZAÇÃO.
DIRETA	`Y` ou `N`	`N`	Especifica que uma restauração deve avançar rapidamente diretamente para o local na fita onde os dados do arquivo residem, em vez de digitalizar toda a fita. Para que a recuperação de acesso direto funcione, o aplicativo de backup deve fornecer informações de posicionamento. Se essa variável estiver definida como `Y`, o aplicativo de backup especificará os nomes de arquivo ou diretório e as informações de posicionamento.

Variável de ambiente	Valores válidos	Padrão	Descrição
NOME_DMP	`string`	`none`	Especifica o nome para um backup de várias subárvores. Esta variável é obrigatória para múltiplos backups de subárvore.
DUMP_DATE	`return_value`	`none`	Você não altera essa variável diretamente. Ele é criado pelo backup se a variável BASE_DATE for definida como um valor diferente `-1`de . A variável DUMP_DATE é derivada pela prependência do valor de nível de 32 bits para um valor de tempo de 32 bits calculado pelo software dump. O nível é incrementado a partir do último valor de nível passado para a variável BASE_DATE. O valor resultante é usado como o valor BASE_DATE em um backup incremental subsequente.

Variável de ambiente	Valores válidos	Padrão	Descrição
ENHANCED_DAR_ENABLED (MELHORADO_DAR_ATIVADO	`Y` ou `N`	`N`	Especifica se a funcionalidade DAR aprimorada está ativada. A FUNCIONALIDADE DAR aprimorada suporta DAR de diretório e DAR de arquivos com fluxos NT. Ele fornece melhorias de desempenho. DAR aprimorado durante a restauração só é possível se as seguintes condições forem atendidas: • ONTAP suporta DAR melhorado. • O histórico do ficheiro está ativado durante a cópia de segurança. • A `ndmpd.offset_map.enable` opção está definida como `on`. • ENHANCED_DAR_ENABLED variável é definida como `Y` durante a restauração.

Variável de ambiente	Valores válidos	Padrão	Descrição
EXCLUIR	`pattern_string`	`none`	Especifica arquivos ou diretórios excluídos ao fazer backup de dados. A lista Excluir é uma lista separada por vírgulas de nomes de arquivo ou diretório. Se o nome de um arquivo ou diretório corresponder a um dos nomes na lista, ele será excluído do backup. As seguintes regras se aplicam ao especificar nomes na lista Excluir: • O nome exato do arquivo ou diretório deve ser usado. • O asterisco (*), um caractere curinga, deve ser o primeiro ou o último caractere da cadeia de carateres. Cada string pode ter até dois asteriscos. • Uma vírgula em um nome de arquivo ou diretório deve ser precedida por uma barra invertida. • A lista Excluir pode conter até 32 nomes. Os arquivos ou diretórios especificados para serem excluídos para backup não serão excluídos se você definir Non_QUOTA_TREE como `Y` simultaneamente.

Variável de ambiente	Valores válidos	Padrão	Descrição
EXTRAIR	`Y`, `N`, ou `E`	`N`	Especifica que subárvores de um conjunto de dados de backup devem ser restauradas. O aplicativo de backup especifica os nomes das subárvores a serem extraídas. Se um arquivo especificado corresponder a um diretório cujo conteúdo foi feito backup, o diretório é extraído recursivamente. Para renomear um arquivo, diretório ou qtree durante a restauração sem usar DAR, você deve definir a variável de ambiente EXTRAIR como `E`.
EXTRACT_ACL	`Y` ou `N`	`Y`	Especifica que as ACLs do arquivo de backup são restauradas em uma operação de restauração. O padrão é restaurar ACLs ao restaurar dados, exceto para DARS.

Variável de ambiente	Valores válidos	Padrão	Descrição
FORÇA	`Y` ou `N`	`N`	Determina se a operação de restauração deve verificar se há espaço de volume e disponibilidade de inode no volume de destino. Definir essa variável para `Y` fazer com que a operação de restauração pule as verificações de espaço de volume e disponibilidade de inode no caminho de destino. Se não houver espaço de volume suficiente ou inodes disponíveis no volume de destino, a operação de restauração recupera a quantidade de dados permitidos pelo espaço de volume de destino e pela disponibilidade de inodes. A operação de restauração pára quando o espaço de volume ou inodes não estão disponíveis.

Variável de ambiente	Valores válidos	Padrão	Descrição
HIST	`Y` ou `N`	`N`	Especifica que as informações do histórico de arquivos são enviadas para o aplicativo de backup. A maioria dos aplicativos de backup comerciais define a variável HIST como `Y`. Se quiser aumentar a velocidade de uma operação de backup ou solucionar um problema com a coleção de histórico de arquivos, defina essa variável como `N`. Não deve definir a variável HIST para `Y` se a aplicação de cópia de segurança não suportar o histórico de ficheiros.

Variável de ambiente	Valores válidos	Padrão	Descrição
IGNORE_CTIME	`Y` ou `N`	`N`	Especifica que o backup de um arquivo não é incrementalmente feito se somente seu valor ctime tiver sido alterado desde o backup incremental anterior. Alguns aplicativos, como software de verificação de vírus, alteram o valor ctime de um arquivo dentro do inode, mesmo que o arquivo ou seus atributos não tenham sido alterados. Como resultado, um backup incremental pode fazer backup de arquivos que não foram alterados. A `IGNORE_CTIME` variável deve ser especificada somente se backups incrementais estiverem tomando uma quantidade inaceitável de tempo ou espaço porque o valor ctime foi modificado. O `NDMP dump` comando define `IGNORE_CTIME` como `false` por padrão. Definir para que isso `true` possa resultar na seguinte perda de dados: 1. Se `IGNORE_CTIME` estiver definido como verdadeiro com

Variável de ambiente	Valores válidos	Padrão	Descrição
IGNORE_QTREES	`Y` ou `N`	`N`	Especifica que a operação de restauração não restaura informações de qtree de qtrees de backup.
NÍVEL	`0-31`	`0`	Especifica o nível de backup. O nível 0 copia todo o conjunto de dados. Níveis de backup incremental, especificados por valores acima de 0, copie todos os arquivos (novos ou modificados) desde o último backup incremental. Por exemplo, um nível 1 faz backup de arquivos novos ou modificados desde o backup de nível 0, um nível 2 faz backup de arquivos novos ou modificados desde o backup de nível 1 e assim por diante.
LISTA	`Y` ou `N`	`N`	Lista os nomes dos arquivos de backup e os números de inode sem realmente restaurar os dados.
LIST_QTREES	`Y` ou `N`	`N`	Lista os qtrees de backup sem realmente restaurar os dados.

exclusão de arquivos, que são movidos através de qtrees na fonte durante a restauração increm

Variável de ambiente	Valores válidos	Padrão	Descrição
MULTI_SUBTREE_ NOMES	`string`	`none`	Especifica que o backup é um backup de várias subárvores. Várias subárvores são especificadas na cadeia de carateres, que é uma lista de nomes de subárvores separada por uma nova linha. As subárvores são especificadas por nomes de caminho relativos ao seu diretório raiz comum, que deve ser especificado como o último elemento da lista. Se você usar essa variável, você também deve usar a variável DMP_NAME.
NDMP_UNICODE_ FH	`Y` ou `N`	`N`	Especifica que um nome Unicode é incluído além do nome NFS do arquivo nas informações do histórico do arquivo. Essa opção não é usada pela maioria dos aplicativos de backup e não deve ser definida a menos que o aplicativo de backup seja projetado para receber esses nomes de arquivo adicionais. A variável HIST também deve ser definida.
NO_ACLS	`Y` ou `N`	`N`	Especifica que as ACLs não devem ser copiadas ao fazer backup de dados.

Variável de ambiente	Valores válidos	Padrão	Descrição
NON_QUOTA_TREE	`Y` ou `N`	`N`	Especifica que os arquivos e diretórios no qtrees devem ser ignorados ao fazer backup de dados. Quando definido como `Y`, os itens no qtrees no conjunto de dados especificado pela variável SISTEMA DE ARQUIVOS não são copiados. Esta variável tem um efeito somente se a variável FILESYSTEM especificar um volume inteiro. A variável non_QUOTA_TREE só funciona em um backup de nível 0 e não funciona se a variável MULTI_SUBTREE_NAMES for especificada. Os arquivos ou diretórios especificados para serem excluídos para backup não serão excluídos se você definir Non_QUOTA_TREE como `Y` simultaneamente.
NOWRITE	`Y` ou `N`	`N`	Especifica que a operação de restauração não deve gravar dados no disco. Esta variável é usada para depuração.

Variável de ambiente	Valores válidos	Padrão	Descrição
RECURSIVA	`Y` ou `N`	`Y`	Especifica que as entradas de diretório durante uma restauração DAR serão expandidas. As variáveis de ambiente DIRECT e ENHANCED_DAR_ENABLED também devem estar ativadas (definidas para `Y`). Se a variável RECURSIVA estiver desativada (definida como `N`), somente as permissões e ACLs de todos os diretórios no caminho de origem original serão restauradas a partir da fita, não do conteúdo dos diretórios. Se a variável RECURSIVA estiver definida como `N` ou a variável RECOVER_full_PATHS estiver definida como `Y`, o caminho de recuperação deve terminar com o caminho original.

Variável de ambiente	Valores válidos	Padrão	Descrição
RECUPERAR_FULL_PATHS	`Y` ou `N`	`N`	Especifica que o caminho de recuperação completo terá suas permissões e ACLs restauradas após o DAR. DIRECT e ENHANCED_DAR_ENABLED também devem ser ativados (definidos como `Y`). Se RECOVER_full_PATHS estiver definido como `Y`, o caminho de recuperação deve terminar com o caminho original. Se os diretórios já existirem no volume de destino, suas permissões e ACLs não serão restaurados da fita.
ATUALIZAÇÃO	`Y` ou `N`	`Y`	Atualiza as informações de metadados para habilitar o backup incremental baseado em NÍVEL.

Variáveis de ambiente suportadas para SMTape

de erro.

Por exemplo, os seguintes são caminhos de recuperação válidos porque todos os caminhos de recuperação estão dentro `foo/dir1/deepdir/myfile`de :

- `/foo`
- `/foo/dir`
- `/foo/dir1/deepdir`
- `/foo/dir1/deepdir/myfile`

Os seguintes são caminhos de recuperação inválidos:

- `/foo`

  `/foo/dir`

  `/foo/dir1/myfile`

-
- /foo/dir2
- /foo/dir2/myfile

Variável de ambiente	Valores válidos	Padrão	Descrição
DATA_BASE	`DUMP_DATE`	`-1`	Especifica a data de início para backups incrementais. `BASE_DATE` É uma representação de cadeia de carateres dos identificadores Snapshot de referência. Usando a `BASE_DATE` cadeia de carateres, o SMTape localiza a cópia Snapshot de referência. `BASE_DATE` não é necessário para backups de linha de base. Para um backup incremental, o valor da `DUMP_DATE` variável da linha de base anterior ou backup incremental é atribuído à `BASE_DATE` variável. O aplicativo de backup atribui o `DUMP_DATE` valor de uma linha de base ou backup incremental SMTape anterior.

Variável de ambiente	Valores válidos	Padrão	Descrição
DUMP_DATE	`return_value`	`none`	No final de um backup SMTape, DUMP_DATE contém um identificador de cadeia de carateres que identifica a cópia Snapshot usada para esse backup. Esta cópia Snapshot pode ser usada como cópia Snapshot de referência para um backup incremental subsequente. O valor resultante de DUMP_DATE é usado como o valor BASE_DATE para backups incrementais subsequentes.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifica a sequência de backups incrementais associados ao backup de linha de base. O ID do conjunto de cópias de segurança é um ID exclusivo de 128 bits que é gerado durante uma cópia de segurança de linha de base. O aplicativo de backup atribui esse ID como entrada à `SMTAPE_BACKUP_SET_ID` variável durante um backup incremental.

Variável de ambiente	Valores válidos	Padrão	Descrição
SMTAPE_SNAPSHOT_NAME	Qualquer cópia Snapshot válida disponível no volume	`Invalid`	Quando a variável SMTAPE_SNAPSHOT_NAME está definida como uma cópia Snapshot, essa cópia Snapshot e suas cópias Snapshot mais antigas são feitas backup em fita. Para backup incremental, essa variável especifica a cópia Snapshot incremental. A variável BASE_DATE fornece a cópia Snapshot da linha de base.
SMTAPE_DELETE_SNAPSHOT	`Y` ou `N`	`N`	Para uma cópia Snapshot criada automaticamente pelo SMTape, quando a variável SMTAPE_DELETE_SNAPSHOT estiver definida como `Y`, depois que a operação de backup estiver concluída, o SMTape exclui essa cópia Snapshot. No entanto, uma cópia Snapshot criada pelo aplicativo de backup não será excluída.
SMTAPE_BREAK_MIRROR	`Y` ou `N`	`N`	Quando a variável SMTAPE_BREAK_MIRROR é definida como `Y`, o volume do tipo `DP` é alterado para um `RW` volume após uma restauração bem-sucedida.

Topologias comuns de backup de fita NDMP

O NDMP dá suporte a várias topologias e configurações entre aplicativos de backup e sistemas de storage ou outros servidores NDMP que fornecem dados (sistemas de arquivos) e serviços de fita.

Sistema de storage para fita local

Na configuração mais simples, um aplicativo de backup faz backup dos dados de um sistema de storage para um subsistema de fita conetado ao sistema de storage. A conexão de controle NDMP existe através do limite da rede. A conexão de dados NDMP que existe no sistema de storage entre os serviços de dados e fita é chamada de configuração local NDMP.

Sistema de storage para fita anexado a outro sistema de storage

Um aplicativo de backup também pode fazer backup de dados de um sistema de armazenamento para uma biblioteca de fitas (um trocador de médio com uma ou mais unidades de fita) conetada a outro sistema de armazenamento. Neste caso, a conexão de dados NDMP entre os serviços de dados e fita é fornecida por uma conexão de rede TCP ou TCP/IPv6. Isso é chamado de uma configuração de sistema de storage três vias NDMP para o sistema de storage.

Biblioteca de fitas conetada ao sistema de storage à rede

As bibliotecas de fitas habilitadas para NDMP fornecem uma variação da configuração de três vias. Nesse caso, a biblioteca de fitas se coneta diretamente à rede TCP/IP e se comunica com o aplicativo de backup e o sistema de armazenamento por meio de um servidor NDMP interno.

Sistema de storage para servidor de dados para fita ou servidor para sistema de storage para fita

O NDMP também dá suporte a configurações de três vias de sistema de storage para servidor de dados e servidor para storage, embora essas variantes sejam menos amplamente implantadas. O sistema de armazenamento para servidor permite o backup de dados do sistema de armazenamento em uma biblioteca de fitas conetada ao host do aplicativo de backup ou a outro sistema de servidor de dados. A configuração do sistema de servidor para armazenamento permite que os dados do servidor sejam copiados para uma biblioteca de fitas conetada ao sistema de armazenamento.

Métodos de autenticação NDMP compatíveis

Você pode especificar um método de autenticação para permitir solicitações de conexão NDMP. O ONTAP oferece suporte a dois métodos para autenticar o acesso NDMP a um sistema de storage: Texto simples e desafio.

No modo NDMP com escopo de nó, desafio e texto sem formatação são ativados por padrão. No entanto, você não pode desativar o desafio. Você pode ativar e desativar texto sem formatação. No método de autenticação em texto simples, a senha de login é transmitida como texto não criptografado.

No modo NDMP com escopo de máquina virtual de storage (SVM), por padrão o método de autenticação é um desafio. Ao contrário do modo NDMP com escopo de nó, neste modo você pode ativar e desativar métodos de autenticação de texto simples e desafio.

Informações relacionadas

Autenticação de usuário em um modo NDMP com escopo de nó

Autenticação de usuário no modo NDMP com escopo SVM

Extensões NDMP suportadas por ONTAP

O NDMP v4 fornece um mecanismo para criar extensões de protocolo NDMP v4 sem modificar o protocolo principal do NDMP v4. Você deve estar ciente das extensões NDMP v4 que são suportadas pelo ONTAP.

As seguintes extensões NDMP v4 são suportadas pelo ONTAP:

- Backup ciente de cluster (CAB)

  Essa extensão só é suportada no modo NDMP com escopo SVM.

- Extensão de endereço de conexão (CAE) para suporte a IPv6
- Classe de extensão 0x2050

  Essa extensão suporta operações de backup reiniciáveis e extensões de gerenciamento de Snapshot.

  A `NDMP_SNAP_RECOVER` mensagem, que faz parte das Extensões de Gerenciamento de Snapshot, é usada para iniciar uma operação de recuperação e transferir os dados recuperados de uma cópia Snapshot local para um local do sistema de arquivos local. No ONTAP, esta mensagem permite a recuperação de volumes e arquivos regulares apenas.

  ```
  `NDMP_SNAP_DIR_LIST`A mensagem permite que você navegue pelas cópias Snapshot de um volume. Se uma operação sem interrupções ocorrer enquanto uma operação de navegação estiver em andamento, o aplicativo de backup deverá reiniciar a operação de navegação.
  ```

Extensão de backup NDMP restartable para um despejo suportado pelo ONTAP

Você pode usar a funcionalidade de extensão de backup reiniciável NDMP (RBE) para reiniciar um backup a partir de um ponto de verificação conhecido no fluxo de dados antes da falha.

O que é a funcionalidade DAR melhorada

Você pode usar a funcionalidade avançada de recuperação de acesso direto (DAR) para DAR de diretório e DAR de arquivos e fluxos NT. Por padrão, a funcionalidade DAR aprimorada está ativada.

A ativação da FUNCIONALIDADE DAR aprimorada pode afetar o desempenho do backup porque um mapa de deslocamento precisa ser criado e gravado em fita. Você pode ativar ou desativar O DAR aprimorado nos modos NDMP com escopo de nó e máquina virtual de armazenamento (SVM).

Limites de escalabilidade para sessões NDMP

Você deve estar ciente do número máximo de sessões NDMP que podem ser estabelecidas simultaneamente em sistemas de armazenamento de diferentes capacidades de memória do sistema. Este número máximo depende da memória do sistema de um sistema de armazenamento.

Os limites mencionados na tabela a seguir são para o servidor NDMP. Os limites mencionados na seção "limites de escalabilidade para sessões de backup e restauração de despejo" são para a sessão de despejo e restauração.

Limites de escalabilidade para sessões de backup e restauração de despejo

Memória do sistema de um sistema de armazenamento	Número máximo de sessões NDMP
Menos de 16 GB	8
Maior ou igual a 16 GB, mas inferior a 24 GB	20
Maior ou igual a 24 GB	36

Você pode obter a memória do sistema do seu sistema de armazenamento usando o `sysconfig -a` comando (disponível através do nodeshell). Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Sobre o NDMP para volumes FlexGroup

A partir do ONTAP 9.7, o NDMP é compatível com volumes FlexGroup.

A partir do ONTAP 9.7, o comando ndmpcopy é suportado para transferência de dados entre volumes FlexVol e FlexGroup.

Se você reverter do ONTAP 9.7 para uma versão anterior, as informações de transferência incremental das transferências anteriores não serão mantidas e, portanto, você deverá executar uma cópia de linha de base após reverter.

A partir do ONTAP 9.8, os seguintes recursos NDMP são compatíveis com volumes FlexGroup:

- A mensagem NDMP_snap_RECOVER na classe de extensão 0x2050 pode ser usada para recuperar arquivos individuais em um volume FlexGroup.
- A extensão de backup reiniciável (RBE) NDMP é compatível com volumes FlexGroup.
- As variáveis de ambiente EXCLUEM e MULTI_SUBTREE_NAMES são suportadas para volumes FlexGroup.

Sobre o NDMP com SnapLock volumes

A criação de várias cópias de dados regulamentados proporciona cenários de recuperação redundantes. Com o uso de despejo e restauração NDMP, é possível preservar as características WORM (write once, read many) dos arquivos de origem em um volume SnapLock.

Os atributos DO WORM nos arquivos em um volume SnapLock são preservados ao fazer backup, restaurar e copiar dados; no entanto, atributos WORM são aplicados apenas ao restaurar para um volume SnapLock. Se um backup de um volume SnapLock for restaurado para um volume diferente de um volume SnapLock, os atributos WORM serão preservados, mas serão ignorados e não serão aplicados pelo ONTAP.

Gerenciar o modo NDMP com escopo de nó para volumes FlexVol

Gerencie o modo NDMP com escopo de nó para visão geral do FlexVol volumes

Você pode gerenciar NDMP no nível do nó usando opções e comandos NDMP. Você pode modificar as opções NDMP usando o `options` comando. Você deve usar credenciais específicas do NDMP para acessar um sistema de storage para executar operações de backup e restauração em fita.

Para obter mais informações sobre o `options` comando, consulte as páginas de manual.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo de nó

Qual é o modo NDMP com escopo de nó

Comandos para gerenciar o modo NDMP com escopo de nó

Você pode usar os `system services ndmp` comandos para gerenciar NDMP em um nível de nó. Alguns desses comandos são obsoletos e serão removidos em uma futura versão principal.

Você pode usar os seguintes comandos NDMP somente no nível avançado de privilégio:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Se você quiser…	Use este comando…
Ativar o serviço NDMP	`system services ndmp on*`
Desativar o serviço NDMP	`system services ndmp off*`
Apresentar a configuração NDMP	`system services ndmp show*`
Modificar a configuração NDMP	`system services ndmp modify*`
Exibir a versão padrão do NDMP	`system services ndmp version*`
Exibir a configuração do serviço NDMP	`system services ndmp service show`
Modificar a configuração do serviço NDMP	`system services ndmp service modify`
Exibir todas as sessões NDMP	`system services ndmp status`

Se você quiser…	Use este comando…
Exibir informações detalhadas sobre todas as sessões NDMP	`system services ndmp probe`
Termine a sessão NDMP especificada	`system services ndmp kill`
Encerrar todas as sessões NDMP	`system services ndmp kill-all`
Altere a senha NDMP	`system services ndmp password*`
Ative o modo NDMP com escopo de nó	`system services ndmp node-scope-mode on*`
Desative o modo NDMP com escopo de nó	`system services ndmp node-scope-mode off*`
Exibir o status do modo NDMP com escopo do nó	`system services ndmp node-scope-mode status*`
Encerrar com força todas as sessões NDMP	`system services ndmp service terminate`
Inicie o daemon de serviço NDMP	`system services ndmp service start`
Pare o daemon de serviço NDMP	`system services ndmp service stop`
Inicie o registo para a sessão NDMP especificada	`system services ndmp log start*`
Parar o registo para a sessão NDMP especificada	`system services ndmp log stop*`

- Esses comandos são obsoletos e serão removidos em uma futura versão principal.

Para obter mais informações sobre esses comandos, consulte as páginas de manual dos `system services ndmp` comandos.

Autenticação de usuário em um modo NDMP com escopo de nó

No modo NDMP com escopo de nó, você deve usar credenciais específicas do NDMP para acessar um sistema de storage para executar operações de backup e restauração de fita.

O ID de usuário padrão é "root". Antes de usar o NDMP em um nó, você deve garantir que você altere a senha padrão do NDMP associada ao usuário NDMP. Você também pode alterar o ID de usuário NDMP padrão.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo de nó

Gerenciar o modo NDMP com escopo SVM para volumes FlexVol

Gerenciar o modo NDMP com escopo SVM para visão geral do FlexVol volumes

Você pode gerenciar NDMP por SVM usando as opções e comandos NDMP. Você pode modificar as opções NDMP usando o `vserver services ndmp modify` comando. No modo NDMP com escopo SVM, a autenticação do usuário é integrada ao mecanismo de controle de acesso baseado em funções.

Você pode adicionar NDMP na lista de protocolos permitidos ou não permitidos usando o `vserver modify` comando. Por padrão, NDMP está na lista de protocolos permitidos. Se NDMP for adicionado à lista de protocolos não permitidos, as sessões NDMP não poderão ser estabelecidas.

Você pode controlar o tipo de LIF no qual uma conexão de dados NDMP é estabelecida usando a `-preferred-interface-role` opção. Durante um estabelecimento de conexão de dados NDMP, o NDMP escolhe um endereço IP que pertence ao tipo LIF, conforme especificado por essa opção. Se os endereços IP não pertencem a nenhum desses tipos de LIF, então a conexão de dados NDMP não pode ser estabelecida. Para obter mais informações sobre a `-preferred-interface-role` opção, consulte as páginas de manual.

Para obter mais informações sobre o `vserver services ndmp modify` comando, consulte as páginas de manual.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo SVM

O que a extensão Cluster Aware Backup faz

Qual é o modo NDMP com escopo SVM

"Administração do sistema"

Comandos para gerenciar o modo NDMP com escopo SVM

Você pode usar os `vserver services ndmp` comandos para gerenciar NDMP em cada máquina virtual de storage (SVM, anteriormente conhecido como SVM).

Se você quiser…	Use este comando…
Ativar o serviço NDMP	`vserver services ndmp on` O serviço NDMP deve estar sempre habilitado em todos os nós em um cluster. Você pode ativar o serviço NDMP em um nó usando o `system services ndmp on` comando. Por padrão, o serviço NDMP é sempre ativado em um nó.
Desativar o serviço NDMP	`vserver services ndmp off`

Se você quiser…	Use este comando…
Apresentar a configuração NDMP	`vserver services ndmp show`
Modificar a configuração NDMP	`vserver services ndmp modify`
Exibir a versão padrão do NDMP	`vserver services ndmp version`
Exibir todas as sessões NDMP	`vserver services ndmp status`
Exibir informações detalhadas sobre todas as sessões NDMP	`vserver services ndmp probe`
Encerrar uma sessão NDMP especificada	`vserver services ndmp kill`
Encerrar todas as sessões NDMP	`vserver services ndmp kill-all`
Gerar a senha NDMP	`vserver services ndmp generate-password`
Exibir status do ramal NDMP	`vserver services ndmp extensions show` Este comando está disponível no nível de privilégio avançado.
Modificar (ativar ou desativar) o estado da extensão NDMP	`vserver services ndmp extensions modify` Este comando está disponível no nível de privilégio avançado.
Inicie o registo para a sessão NDMP especificada	`vserver services ndmp log start` Este comando está disponível no nível de privilégio avançado.
Parar o registo para a sessão NDMP especificada	`vserver services ndmp log stop` Este comando está disponível no nível de privilégio avançado.

Para obter mais informações sobre esses comandos, consulte as páginas de manual dos `vserver services ndmp` comandos.

O que a extensão Cluster Aware Backup faz

O CAB (Cluster Aware Backup) é uma extensão de protocolo NDMP v4. Essa extensão permite que o servidor NDMP estabeleça uma conexão de dados em um nó que possua um volume. Isso também permite que o aplicativo de backup determine se os volumes e

dispositivos de fita estão localizados no mesmo nó em um cluster.

Para permitir que o servidor NDMP identifique o nó que possui um volume e estabeleça uma conexão de dados em tal nó, o aplicativo de backup deve suportar a EXTENSÃO CAB. A extensão CAB requer que o aplicativo de backup informe o servidor NDMP sobre o volume a ser feito backup ou restaurado antes de estabelecer a conexão de dados. Isso permite que o servidor NDMP determine o nó que hospeda o volume e estabeleça adequadamente a conexão de dados.

Com a EXTENSÃO CAB suportada pelo aplicativo de backup, o servidor NDMP fornece informações de afinidade sobre volumes e dispositivos de fita. Usando essas informações de afinidade, o aplicativo de backup pode executar um backup local em vez de um backup de três vias se um volume e um dispositivo de fita estiverem localizados no mesmo nó em um cluster.

Disponibilidade de volumes e dispositivos de fita para backup e restauração em diferentes tipos de LIF

Você pode configurar um aplicativo de backup para estabelecer uma conexão de controle NDMP em qualquer um dos tipos de LIF em um cluster. No modo NDMP com escopo de máquina virtual de armazenamento (SVM), você pode determinar a disponibilidade de volumes e dispositivos de fita para operações de backup e restauração, dependendo desses tipos de LIF e do status da extensão DA CABINE.

As tabelas a seguir mostram a disponibilidade de volumes e dispositivos de fita para tipos de LIF de conexão de controle NDMP e o status da EXTENSÃO DA CABINE:

Disponibilidade de volumes e dispositivos de fita quando a EXTENSÃO CAB não é suportada pelo aplicativo de backup

Tipo de LIF de conexão de controle NDMP	Volumes disponíveis para backup ou restauração	Dispositivos de fita disponíveis para backup ou restauração
LIF de gerenciamento de nós	Todos os volumes hospedados por um nó	Dispositivos de fita conetados ao nó que hospeda o LIF de gerenciamento de nós
LIF de dados	Somente volumes pertencentes ao SVM hospedados por um nó que hospeda o data LIF	Nenhum
LIF de gerenciamento de clusters	Todos os volumes hospedados por um nó que hospeda o LIF de gerenciamento de cluster	Nenhum
LIF entre clusters	Todos os volumes hospedados por um nó que hospeda o LIF entre clusters	Dispositivos de fita conetados ao nó que hospeda o LIF entre clusters

Disponibilidade de volumes e dispositivos de fita quando a EXTENSÃO CAB é suportada pelo aplicativo de backup

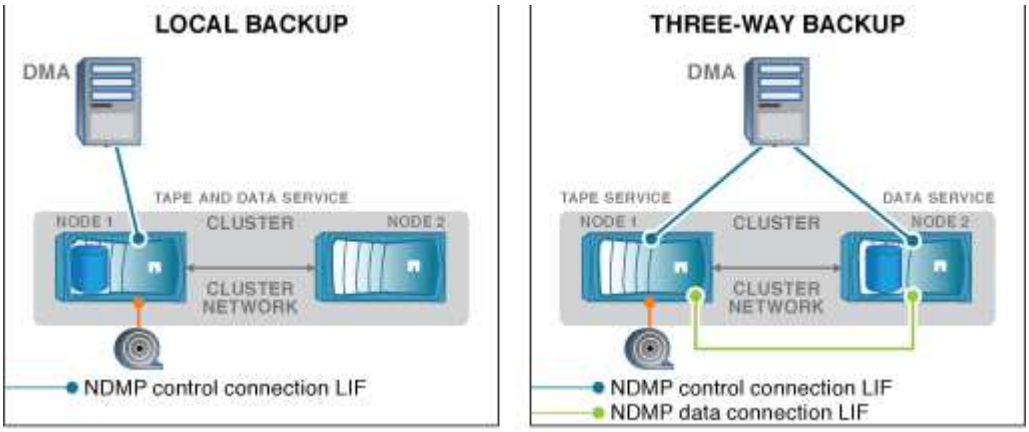
Tipo de LIF de conexão de controle NDMP	Volumes disponíveis para backup ou restauração	Dispositivos de fita disponíveis para backup ou restauração
LIF de gerenciamento de nós	Todos os volumes hospedados por um nó	Dispositivos de fita conetados ao nó que hospeda o LIF de gerenciamento de nós
LIF de dados	Todos os volumes pertencentes ao SVM que hospeda o data LIF	Nenhum
LIF de gerenciamento de clusters	Todos os volumes no cluster	Todos os dispositivos de fita no cluster
LIF entre clusters	Todos os volumes no cluster	Todos os dispositivos de fita no cluster

Que informação de afinidade é

Com o aplicativo de backup ciente DA CAB, o servidor NDMP fornece informações de localização exclusivas sobre volumes e dispositivos de fita. Usando essas informações de afinidade, o aplicativo de backup pode executar um backup local em vez de um backup de três vias se um volume e um dispositivo de fita compartilharem a mesma afinidade.

Se a conexão de controle NDMP for estabelecida em um LIF de gerenciamento de nós, LIF de gerenciamento de cluster ou LIF, o aplicativo de backup poderá usar as informações de afinidade para determinar se um dispositivo de volume e fita está localizado no mesmo nó e, em seguida, executar uma operação de backup ou restauração local ou de três vias. Se a conexão de controle NDMP for estabelecida em um LIF de dados, o aplicativo de backup sempre executará um backup de três vias.

Backup NDMP local e backup NDMP de três vias



Usando as informações de afinidade sobre volumes e dispositivos de fita, o DMA (aplicativo de backup) executa um backup NDMP local no volume e dispositivo de fita localizado no nó 1 no cluster. Se o volume se mover do nó 1 para o nó 2, as informações de afinidade sobre o volume e o dispositivo de fita serão alteradas. Assim, para um backup subsequente, o DMA executa uma operação de backup NDMP de três vias. Isso garante a continuidade da política de backup para o volume, independentemente do nó para o qual o volume é movido.

Informações relacionadas

O que a extensão Cluster Aware Backup faz

O servidor NDMP oferece suporte a conexões de controle seguras no modo com escopo SVM

Uma conexão de controle seguro pode ser estabelecida entre o aplicativo de gerenciamento de dados (DMA) e o servidor NDMP usando soquetes seguros (SSL/TLS) como mecanismo de comunicação. Esta comunicação SSL é baseada nos certificados do servidor. O servidor NDMP escuta na porta 30000 (atribuída pela IANA para o serviço "'ndmps").

Depois de estabelecer a conexão do cliente nesta porta, o handshake SSL padrão segue onde o servidor apresenta o certificado ao cliente. Quando o cliente aceita o certificado, o handshake SSL está concluído. Depois que esse processo estiver concluído, toda a comunicação entre o cliente e o servidor é criptografada. O fluxo de trabalho do protocolo NDMP permanece exatamente como antes. A conexão NDMP segura requer apenas autenticação de certificado do lado do servidor. Um DMA pode optar por estabelecer uma conexão conetando-se ao serviço NDMP seguro ou ao serviço NDMP padrão.

Por padrão, o serviço NDMP seguro é desativado para uma máquina virtual de storage (SVM). Você pode ativar ou desativar o serviço NDMP seguro em um determinado SVM usando o `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` comando.

Tipos de conexão de dados NDMP

No modo NDMP com escopo de máquina virtual de armazenamento (SVM), os tipos de conexão de dados NDMP suportados dependem do tipo de conexão LIF de controle NDMP e do status da extensão DA CABINE. Este tipo de conexão de dados NDMP indica se você pode executar uma operação de backup ou restauração local ou de três vias NDMP.

Você pode executar uma operação de backup ou restauração NDMP de três vias em uma rede TCP ou TCP/IPv6. As tabelas a seguir mostram os tipos de conexão de dados NDMP com base no tipo de LIF de conexão de controle NDMP e no status da EXTENSÃO DA CABINE.

Tipo de conexão de dados NDMP quando a extensão CAB é suportada pelo aplicativo de backup

Tipo de LIF de conexão de controle NDMP	Tipo de conexão de dados NDMP
LIF de gerenciamento de nós	LOCAL, TCP, TCP/IPV6
LIF de dados	TCP, TCP/IPv6
LIF de gerenciamento de clusters	LOCAL, TCP, TCP/IPV6
LIF entre clusters	LOCAL, TCP, TCP/IPV6

Tipo de conexão de dados NDMP quando a EXTENSÃO CAB não é suportada pelo aplicativo de backup

Tipo de LIF de conexão de controle NDMP	Tipo de conexão de dados NDMP
LIF de gerenciamento de nós	LOCAL, TCP, TCP/IPV6
LIF de dados	TCP, TCP/IPv6
LIF de gerenciamento de clusters	TCP, TCP/IPv6
LIF entre clusters	LOCAL, TCP, TCP/IPV6

Informações relacionadas

O que a extensão Cluster Aware Backup faz

"Gerenciamento de rede"

Autenticação de usuário no modo NDMP com escopo SVM

No modo NDMP com escopo de máquina virtual de storage (SVM), a autenticação de usuário NDMP é integrada ao controle de acesso baseado em funções. No contexto SVM, o usuário NDMP deve ter a função "vsadmin" ou "vsadmin-backup". Em um contexto de cluster, o usuário NDMP deve ter a função "'admin'" ou "'backup'".

Além dessas funções pré-definidas, uma conta de usuário associada a uma função personalizada também pode ser usada para autenticação NDMP, desde que a função personalizada tenha a pasta "'vserver services ndmp" em seu diretório de comando e o nível de acesso da pasta não seja "'nenhum'". Nesse modo, você deve gerar uma senha NDMP para uma determinada conta de usuário, que é criada por meio do controle de acesso baseado em função. Os usuários de cluster em uma função de administrador ou backup podem acessar um LIF de gerenciamento de nós, um LIF de gerenciamento de clusters ou um LIF entre clusters. Os usuários em uma função vsadmin-backup ou vsadmin podem acessar apenas o LIF de dados para esse SVM. Portanto, dependendo da função de um usuário, a disponibilidade de volumes e dispositivos de fita para operações de backup e restauração varia.

Este modo também suporta autenticação de utilizador para utilizadores NIS e LDAP. Portanto, os usuários NIS e LDAP podem acessar vários SVMs com um ID de usuário e senha comuns. No entanto, a autenticação NDMP não suporta usuários do ative Directory.

Nesse modo, uma conta de usuário deve estar associada ao aplicativo SSH e ao método de autenticação ""Senha de usuário"".

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo SVM

"Administração do sistema"

Gerar uma senha específica do NDMP para usuários NDMP

No modo NDMP com escopo de máquina virtual de armazenamento (SVM), você deve gerar uma senha para um ID de usuário específico. A senha gerada é baseada na senha de login real para o usuário NDMP. Se a senha de login real mudar, você deve gerar a senha específica do NDMP novamente.

Passos

1. Use o `vserver services ndmp generate-password` comando para gerar uma senha específica do NDMP.

   Você pode usar essa senha em qualquer operação NDMP atual ou futura que exija a entrada de senha.

   > A partir do contexto de máquina virtual de storage (SVM, anteriormente conhecido como SVM), você pode gerar senhas NDMP para usuários pertencentes apenas a esse SVM.

   O exemplo a seguir mostra como gerar uma senha específica do NDMP para um ID de usuário user1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. Se alterar a palavra-passe para a conta normal do sistema de armazenamento, repita este procedimento para obter a nova palavra-passe específica do NDMP.

Como as operações de backup e restauração em fita são afetadas durante a recuperação de desastres na configuração do MetroCluster

É possível executar operações de backup em fita e restaurar simultaneamente durante a recuperação de desastres em uma configuração do MetroCluster. Você precisa entender como essas operações são afetadas durante a recuperação de desastres.

Se as operações de backup e restauração em fita forem executadas em um volume de SVM em uma relação de recuperação de desastres, você poderá continuar executando backup em fita incremental e restaurar as operações após um switchover e um switchback.

Sobre o motor de descarga para volumes FlexVol

Sobre o motor de descarga para volumes FlexVol

O dump é uma solução de backup e recuperação baseada em cópia Snapshot da ONTAP que ajuda você a fazer backup de arquivos e diretórios de uma cópia Snapshot para um dispositivo de fita e restaurar os dados de backup para um sistema de storage.

Você pode fazer backup dos dados do sistema de arquivos, como diretórios, arquivos e suas configurações de segurança associadas, em um dispositivo de fita usando o backup de despejo. Você pode fazer backup de um volume inteiro, de uma qtree inteiro ou de uma subárvore que não seja um volume inteiro nem uma qtree inteiro.

Você pode executar um backup ou restauração de despejo usando aplicativos de backup compatíveis com NDMP.

Ao executar um backup de despejo, você pode especificar a cópia Snapshot a ser usada para um backup. Se você não especificar uma cópia Snapshot para o backup, o mecanismo de despejo criará uma cópia Snapshot

para o backup. Depois que a operação de backup for concluída, o mecanismo de despejo excluirá essa cópia Snapshot.

Você pode executar backups de nível 0, incrementais ou diferenciais na fita usando o mecanismo de despejo.

> Depois de reverter para uma versão anterior ao Data ONTAP 8.3, você deve executar uma operação de backup de linha de base antes de executar uma operação de backup incremental.

Informações relacionadas

"Atualize, reverta ou downgrade"

Como funciona um backup de despejo

Um backup de despejo grava dados do sistema de arquivos do disco para a fita usando um processo predefinido. Você pode fazer backup de um volume, uma qtree ou uma subárvore que não seja um volume inteiro nem uma qtree inteiro.

A tabela a seguir descreve o processo que o ONTAP usa para fazer backup do objeto indicado pelo caminho de despejo:

Fase	Ação
1	Para backups de volumes inferiores a completos ou de qtree, o ONTAP percorre diretórios para identificar os arquivos a serem copiados. Se você estiver fazendo backup de um volume ou qtree inteiro, o ONTAP combina esse estágio com o Estágio 2.
2	Para um backup de volume completo ou de qtree completo, o ONTAP identifica os diretórios nos volumes ou qtrees a serem copiados.
3	O ONTAP grava os diretórios em fita.
4	O ONTAP grava os arquivos em fita.
5	O ONTAP grava as informações da ACL (se aplicável) na fita.

O backup de despejo usa uma cópia Snapshot de seus dados para o backup. Portanto, você não precisa colocar o volume off-line antes de iniciar o backup.

O backup de despejo nomeia cada cópia Snapshot que ele cria como `snapshot_for_backup.n`, onde `n` é um número inteiro começando em 0. Cada vez que o backup de despejo cria uma cópia Snapshot, ele aumenta o número inteiro em 1. O número inteiro é redefinido para 0 após o sistema de armazenamento ser reiniciado. Depois que a operação de backup for concluída, o mecanismo de despejo excluirá essa cópia Snapshot.

Quando o ONTAP executa vários backups de despejo simultaneamente, o mecanismo de despejo cria várias cópias Snapshot. Por exemplo, se o ONTAP estiver executando dois backups de despejo simultaneamente, você encontrará as seguintes cópias Snapshot nos volumes a partir dos quais os dados estão sendo copiados: `snapshot_for_backup.0` E `snapshot_for_backup.1`.

Quando você está fazendo backup de uma cópia Snapshot, o mecanismo de despejo não cria uma cópia Snapshot adicional.

Tipos de dados que o motor de descarga faz backup

O mecanismo de despejo permite que você faça backup de dados em fita para proteger contra desastres ou interrupções no controlador. Além de fazer backup de objetos de dados, como arquivos, diretórios, qtrees ou volumes inteiros, o mecanismo de despejo pode fazer backup de muitos tipos de informações sobre cada arquivo. Conhecer os tipos de dados que o mecanismo de despejo pode fazer backup e as restrições a serem levadas em consideração podem ajudá-lo a Planejar sua abordagem para a recuperação de desastres.

Além de fazer backup de dados em arquivos, o mecanismo de despejo pode fazer backup das seguintes informações sobre cada arquivo, conforme aplicável:

- UNIX GID, proprietário UID e permissões de arquivo
- Tempo de acesso, criação e modificação do UNIX
- Tipo de ficheiro
- Tamanho do ficheiro
- Nome DOS, atributos dos e tempo de criação
- Listas de controle de acesso (ACLs) com 1.024 entradas de controle de acesso (ACEs)
- Informações de Qtree
- Caminhos de junção

Os caminhos de junção são copiados como links simbólicos.

- Clones de LUN e LUN

  Você pode fazer backup de um objeto LUN inteiro; no entanto, não é possível fazer backup de um único arquivo dentro do objeto LUN. Da mesma forma, você pode restaurar um objeto LUN inteiro, mas não um único arquivo dentro do LUN.

  O mecanismo de despejo faz backup de clones de LUN como LUNs independentes.

- Arquivos alinhados à VM

  O backup de arquivos alinhados à VM não é suportado em versões anteriores ao Data ONTAP 8.1,2.

Quando um clone de LUN com backup de snapshot é transferido do Data ONTAP operando no modo 7 para o ONTAP, ele se torna um LUN inconsistente. O motor de descarga não faz backup de LUNs inconsistentes.

Quando você restaura dados para um volume, a e/S do cliente é restrita nos LUNs sendo restaurados. A restrição LUN é removida apenas quando a operação de restauração de despejo estiver concluída. Da mesma forma, durante uma operação de restauração de um único arquivo ou LUN do SnapMirror, a e/S do cliente é restrita em arquivos e LUNs sendo restaurados. Esta restrição é removida apenas quando a operação de restauração de um único arquivo ou LUN estiver concluída. Se um backup de despejo for executado em um

volume no qual uma restauração de despejo ou uma operação de restauração de arquivo único SnapMirror ou LUN está sendo executada, os arquivos ou LUNs que têm restrição de e/S cliente não serão incluídos no backup. Esses arquivos ou LUNs são incluídos em uma operação de backup subsequente se a restrição de e/S do cliente for removida.

> Um LUN em execução no Data ONTAP 8.3 que é feito backup em fita pode ser restaurado apenas para 8,3 e versões posteriores e não para uma versão anterior. Se o LUN for restaurado para uma versão anterior, o LUN será restaurado como um arquivo.

Quando você faz backup de um volume secundário do SnapVault ou de um destino do volume SnapMirror em fita, apenas os dados do volume são copiados. Não é feito backup dos metadados associados. Portanto, quando você tenta restaurar o volume, apenas os dados nesse volume são restaurados. As informações sobre as relações SnapMirror de volume não estão disponíveis no backup e, portanto, não são restauradas.

Se você despejar um arquivo que tenha apenas permissões do Windows NT e restaurá-lo para uma qtree ou volume de estilo UNIX, o arquivo obtém as permissões UNIX padrão para essa qtree ou volume.

Se você despejar um arquivo que tenha apenas permissões UNIX e restaurá-lo para uma qtree ou volume no estilo NTFS, o arquivo obtém as permissões padrão do Windows para essa qtree ou volume.

Outros despejos e restaurações preservam permissões.

Você pode fazer backup de arquivos alinhados à VM e da `vm-align-sector` opção. Para obter mais informações sobre arquivos alinhados à VM, "Gerenciamento de storage lógico"consulte .

Que cadeias de incremento são

Uma cadeia de incremento é uma série de backups incrementais do mesmo caminho. Como você pode especificar qualquer nível de backup a qualquer momento, você deve entender cadeias de incremento para poder executar backups e restaurações de forma eficaz. Você pode executar 31 níveis de operações de backup incrementais.

Existem dois tipos de cadeias de incremento:

- Uma cadeia de incremento consecutiva, que é uma sequência de backups incrementais que começa com o nível 0 e é aumentada em 1 em cada backup subsequente.
- Uma cadeia de incremento não consecutiva, onde backups incrementais saltam níveis ou têm níveis que estão fora de sequência, como 0, 2, 3, 1, 4 ou mais comumente 0, 1, 2, 1 ou 0, 1, 2, 1, 1.

Os backups incrementais são baseados no backup de nível mais recente. Por exemplo, a sequência dos níveis de backup 0, 2, 3, 1, 4 fornece duas cadeias de incremento: 0, 2, 3 e 0, 1, 4. A tabela a seguir explica as bases dos backups incrementais:

Ordem de cópia de segurança	Nível de incremento	Cadeia de incremento	Base	Cópia de segurança dos ficheiros
1	0	Ambos	Arquivos no sistema de armazenamento	Todos os arquivos no caminho de backup

Ordem de cópia de segurança	Nível de incremento	Cadeia de incremento	Base	Cópia de segurança dos ficheiros
2	2	0, 2, 3	Backup de nível 0	Arquivos no caminho de backup criados desde o backup de nível 0
3	3	0, 2, 3	Backup de nível 2	Arquivos no caminho de backup criados desde o backup de nível 2
4	1	0, 1, 4	Backup de nível 0, porque este é o nível mais recente que é menor do que o backup de nível 1	Arquivos no caminho de backup criados desde o backup de nível 0, incluindo arquivos que estão nos backups de nível 2 e nível 3
5	4	0, 1, 4	O backup de nível 1, por ser um nível mais baixo e mais recente que os backups de nível 0, nível 2 ou nível 3	Arquivos criados desde o backup de nível 1

Qual é o fator de bloqueio

Um bloco de fita é de 1.024 bytes de dados. Durante um backup ou restauração de fita, você pode especificar o número de blocos de fita transferidos em cada operação de leitura/gravação. Esse número é chamado de *fator de bloqueio*.

Você pode usar um fator de bloqueio de 4 a 256. Se você pretende restaurar um backup para um sistema diferente do sistema que fez o backup, o sistema de restauração deve suportar o fator de bloqueio usado para o backup. Por exemplo, se você usar um fator de bloqueio de 128, o sistema no qual você restaura esse backup deve suportar um fator de bloqueio de 128.

Durante um backup NDMP, o MOVER_RECORD_SIZE determina o fator de bloqueio. O ONTAP permite um valor máximo de 256 KB para MOVER_RECORD_size.

Quando reiniciar um backup de despejo

Um backup de despejo às vezes não termina devido a erros internos ou externos, como erros de gravação de fita, interrupções de energia, interrupções acidentais de usuário ou inconsistência interna no sistema de armazenamento. Se o backup falhar por um desses motivos, você poderá reiniciá-lo.

Você pode optar por interromper e reiniciar um backup para evitar períodos de tráfego intenso no sistema de armazenamento ou para evitar a concorrência por outros recursos limitados no sistema de armazenamento, como uma unidade de fita. Você pode interromper um backup longo e reiniciá-lo mais tarde se uma restauração (ou backup) mais urgente exigir a mesma unidade de fita. Os backups reiniciáveis persistem nas reinicializações. Você pode reiniciar um backup abortado para fita somente se as seguintes condições forem verdadeiras:

- A cópia de segurança abortada está na fase IV
- Todas as cópias Snapshot associadas que foram bloqueadas pelo comando dump estão disponíveis.
- O histórico do ficheiro tem de estar ativado.

Quando essa operação de despejo é abortada e deixada em um estado reiniciável, as cópias Snapshot associadas são bloqueadas. Essas cópias Snapshot são liberadas após o contexto de backup ser excluído. Pode visualizar a lista de contextos de cópia de segurança utilizando o `vserver services ndmp restartable backup show` comando.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Como funciona uma restauração de despejo

Uma restauração de despejo grava dados do sistema de arquivos da fita para o disco usando um processo predefinido.

O processo na tabela a seguir mostra como a restauração de despejo funciona:

Fase	Ação
1	O ONTAP cataloga os arquivos que precisam ser extraídos da fita.
2	O ONTAP cria diretórios e arquivos vazios.
3	O ONTAP lê um arquivo da fita, grava-o no disco e define as permissões (incluindo ACLs) nele.
4	O ONTAP repete os estágios 2 e 3 até que todos os arquivos especificados sejam copiados da fita.

Tipos de dados que o motor de descarga restaura

Quando ocorre um desastre ou uma interrupção do controlador, o mecanismo de despejo fornece vários métodos para recuperar todos os dados que você fez backup, de arquivos únicos, para atributos de arquivo, para diretórios inteiros. Conhecer os tipos de dados que o mecanismo de despejo pode restaurar e quando usar qual método de recuperação pode ajudar a minimizar o tempo de inatividade.

Você pode restaurar dados para um LUN on-line mapeado. No entanto, os aplicativos host não podem acessar esse LUN até que a operação de restauração esteja concluída. Após a conclusão da operação de restauração, o cache do host dos dados LUN deve ser lavado para fornecer coerência com os dados restaurados.

O motor de descarga pode recuperar os seguintes dados:

- Conteúdo de arquivos e diretórios
- Permissões de arquivo UNIX
- ACLs

  Se você restaurar um arquivo que tenha apenas permissões de arquivo UNIX para uma qtree ou volume NTFS, o arquivo não tem ACLs do Windows NT. O sistema de armazenamento usa apenas as permissões de arquivo UNIX neste arquivo até que você crie uma ACL do Windows NT nele.

  > Se você restaurar ACLs de backup de sistemas de armazenamento que executam o Data ONTAP 8.2 para sistemas de armazenamento que executam o Data ONTAP 8.1.x e anteriores que tenham um limite ACE inferior a 1.024, uma ACL padrão será restaurada.

- Informações de Qtree

  As informações de Qtree são usadas somente se uma qtree for restaurada para a raiz de um volume. As informações de Qtree não são usadas se uma qtree for restaurada para um diretório inferior, como

`/vs1/vol1/subdir/lowerdir` , e deixar de ser uma qtree.

- Todos os outros atributos de arquivo e diretório
- Fluxos do Windows NT
- LUNs
  - Um LUN deve ser restaurado para um nível de volume ou um nível de qtree para que ele permaneça como um LUN.

    Se for restaurado para um diretório, ele será restaurado como um arquivo porque não contém metadados válidos.

  - Um LUN de 7 modos é restaurado como LUN em um volume ONTAP.
- Um volume do modo 7D pode ser restaurado para um volume ONTAP.
- Os arquivos alinhados à VM restaurados para um volume de destino herdam as propriedades de alinhamento da VM do volume de destino.
- O volume de destino para uma operação de restauração pode ter arquivos com bloqueios obrigatórios ou de aconselhamento.

  Ao executar a operação de restauração para um volume de destino, o motor de descarga ignora esses bloqueios.

Considerações antes de restaurar dados

Você pode restaurar os dados de backup para o caminho original ou para um destino diferente. Se estiver a restaurar dados de cópia de segurança para um destino diferente, tem de preparar o destino para a operação de restauro.

Antes de restaurar dados para o caminho original ou para um destino diferente, você deve ter as seguintes informações e atender aos seguintes requisitos:

- O nível da restauração
- O caminho para o qual você está restaurando os dados
- O fator de bloqueio usado durante o backup
- Se você estiver fazendo uma restauração incremental, todas as fitas devem estar na cadeia de backup
- Uma unidade de fita disponível e compatível com a fita a ser restaurada

Antes de restaurar dados para um destino diferente, você deve executar as seguintes operações:

- Se você estiver restaurando um volume, você deve criar um novo volume.
- Se você estiver restaurando uma qtree ou um diretório, você deve renomear ou mover arquivos que provavelmente tenham os mesmos nomes que os arquivos que você está restaurando.

> No ONTAP 9, os nomes de qtree suportam o formato Unicode. As versões anteriores do ONTAP não suportam este formato. Se uma qtree com nomes Unicode no ONTAP 9 for copiada para uma versão anterior do ONTAP usando o `ndmpcopy` comando ou através da restauração de uma imagem de backup em uma fita, a qtree será restaurada como um diretório regular e não como uma qtree com formato Unicode.

Se um arquivo restaurado tiver o mesmo nome que um arquivo existente, o arquivo existente será substituído pelo arquivo restaurado. No entanto, os diretórios não são sobrescritos.

Para renomear um arquivo, diretório ou qtree durante a restauração sem usar DAR, você deve definir a variável de ambiente EXTRAIR como `E`.

Espaço necessário no sistema de armazenamento de destino

Você precisa de cerca de 100 MB mais espaço no sistema de armazenamento de destino do que a quantidade de dados a serem restaurados.

A operação de restauração verifica a disponibilidade de espaço de volume e inode no volume de destino quando a operação de restauração é iniciada. Definir a variável de ambiente FORÇAR para `Y` fazer com que a operação de restauração pule as verificações de espaço de volume e disponibilidade de inode no caminho de destino. Se não houver espaço de volume suficiente ou inodes disponíveis no volume de destino, a operação de restauração recupera a quantidade de dados permitidos pelo espaço de volume de destino e pela disponibilidade de inodes. A operação de restauração pára quando não há mais espaço de volume ou inodes restantes.

Limites de escalabilidade para sessões de backup e restauração de despejo

Você deve estar ciente do número máximo de sessões de backup e restauração de despejo que podem ser executadas simultaneamente em sistemas de armazenamento de diferentes capacidades de memória do sistema. Este número máximo depende da memória do sistema de um sistema de armazenamento.

Os limites mencionados na tabela a seguir são para o motor de descarga ou restauração. Os limites mencionados nos limites de escalabilidade para sessões NDMP são para o servidor NDMP, que são superiores aos limites do mecanismo.

Memória do sistema de um sistema de armazenamento	Número total de sessões de backup e restauração de despejo
Menos de 16 GB	4
Maior ou igual a 16 GB, mas inferior a 24 GB	16
Maior ou igual a 24 GB	32

Se você usar `ndmpcopy` o comando para copiar dados em sistemas de armazenamento, duas sessões NDMP serão estabelecidas, uma para backup de despejo e outra para restauração de despejo.

Você pode obter a memória do sistema do seu sistema de armazenamento usando o `sysconfig -a` comando (disponível através do nodeshell). Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Informações relacionadas

Limites de escalabilidade para sessões NDMP

Suporte de backup e restauração em fita entre o Data ONTAP operando no modo 7 e o ONTAP

Você pode restaurar dados de backup de um sistema de storage operando no modo 7 ou executando o ONTAP para um sistema de storage operando no modo 7 ou executando o ONTAP.

As seguintes operações de backup e restauração em fita são suportadas entre o Data ONTAP operando no modo 7 e o ONTAP:

- Fazer backup de um volume de 7 modos para uma unidade de fita conetada a um sistema de armazenamento executando o ONTAP
- Fazer backup de um volume ONTAP em uma unidade de fita conetada a um sistema de 7 modos
- Restaurar dados de backup de um volume de 7 modos a partir de uma unidade de fita conetada a um sistema de armazenamento executando o ONTAP
- Restaurar dados de backup de um volume ONTAP de uma unidade de fita conetada a um sistema de modo 7D.
- Restaurar um volume do modo 7D para um volume ONTAP

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Restaurar um volume ONTAP para um volume do modo 7D.

Um LUN ONTAP é restaurado como um arquivo regular em um volume de 7 modos.

Eliminar contextos reiniciáveis

Se você quiser iniciar um backup em vez de reiniciar um contexto, você pode excluir o contexto.

Sobre esta tarefa

Você pode excluir um contexto restartable usando o `vserver services ndmp restartable-backup delete` comando fornecendo o nome SVM e o ID de contexto.

Passos

1. Excluir um contexto restartable:

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context -id` *`context_identifier`*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Como o dump funciona em um volume secundário do SnapVault

Você pode executar operações de backup em fita em dados espelhados no volume secundário do SnapVault. Você pode fazer backup apenas dos dados espelhados no volume secundário do SnapVault para fita e não dos metadados da relação do SnapVault.

Quando você quebra a relação de espelhamento de proteção de dados (`snapmirror break`) ou quando ocorre uma ressincronização do SnapMirror, sempre é necessário executar um backup de linha de base.

Como o dump funciona com failover de armazenamento e operações ARL

Antes de executar operações de backup ou restauração de despejo, você deve entender como essas operações funcionam com operações de failover de storage (takeover e giveback) ou realocação de agregados (ARL). A `-override-vetoes` opção determina o comportamento do mecanismo de descarga durante uma operação de failover de armazenamento ou ARL.

Quando uma operação de backup ou restauração de despejo está em execução e a `-override-vetoes` opção está definida como `false`, uma operação de failover de armazenamento iniciado pelo usuário ou ARL é interrompida. No entanto, se a `-override-vetoes` opção estiver definida como `true`, a operação de failover de armazenamento ou ARL será continuada e a operação de backup ou restauração de despejo será cancelada. Quando um failover de armazenamento ou operação ARL é iniciado automaticamente pelo sistema de armazenamento, uma operação de backup ou restauração de despejo ativo é sempre abortada. Não é possível reiniciar as operações de backup de despejo e restauração mesmo após a conclusão das

operações de failover de armazenamento ou ARL.

Operações de descarga quando a extensão DA CABINA é suportada

Se o aplicativo de backup suportar a EXTENSÃO CAB, você poderá continuar executando operações de backup e restauração de despejo incremental sem reconfigurar políticas de backup após um failover de armazenamento ou operação ARL.

Operações de descarga quando a extensão DA CABINA não é suportada

Se o aplicativo de backup não suportar a EXTENSÃO CAB, você poderá continuar executando operações de backup e restauração de despejo incremental se você migrar o LIF configurado na política de backup para o nó que hospeda o agregado de destino. Caso contrário, após a operação de failover de armazenamento e ARL, você deve executar um backup de linha de base antes de executar a operação de backup incremental.

Para operações de failover de storage, o LIF configurado na política de backup deve ser migrado para o nó do parceiro.

Informações relacionadas

"Alta disponibilidade"

Como o dump funciona com a movimentação de volume

As operações de backup e restauração em fita e a movimentação de volume podem ser executadas em paralelo até que a fase final de transição seja tentada pelo sistema de storage. Após essa fase, novas operações de backup e restauração de fita não são permitidas no volume que está sendo movido. No entanto, as operações atuais continuam a ser executadas até a conclusão.

A tabela a seguir descreve o comportamento das operações de backup e restauração de fita após a operação de movimentação de volume:

Se você estiver executando operações de backup e restauração de fita na…	Então…
Modo NDMP com escopo de máquina virtual de storage (SVM) quando a EXTENSÃO CAB é suportada pelo aplicativo de backup	Você pode continuar executando operações incrementais de backup em fita e restauração em volumes somente leitura/gravação e leitura sem reconfigurar políticas de backup.
Modo NDMP com escopo SVM quando a EXTENSÃO CAB não é suportada pelo aplicativo de backup	Você pode continuar executando operações incrementais de backup em fita e restauração em volumes somente leitura/gravação e leitura se migrar o LIF configurado na política de backup para o nó que hospeda o agregado de destino. Caso contrário, após a movimentação do volume, você deve executar um backup de linha de base antes de executar a operação de backup incremental.

Quando ocorre uma movimentação de volume, se o volume pertencente a uma SVM diferente no nó de destino tiver o mesmo nome do volume movido, então você não poderá executar operações de backup incrementais do volume movido.

Como o dump funciona quando um FlexVol volume está cheio

Antes de executar uma operação de backup de despejo incremental, você deve garantir que há espaço livre suficiente no FlexVol volume.

Se a operação falhar, você precisará aumentar o espaço livre no volume Flex vol aumentando seu tamanho ou excluindo as cópias Snapshot. Em seguida, execute novamente a operação de backup incremental.

Como o dump funciona quando o tipo de acesso ao volume muda

Quando um volume de destino do SnapMirror ou um volume secundário do SnapVault mudar de estado de leitura/gravação para somente leitura ou de somente leitura para leitura/gravação, você deve executar uma operação de backup ou restauração de fita de linha de base.

O destino do SnapMirror e os volumes secundários do SnapVault são volumes somente leitura. Se você executar operações de backup e restauração em fita nesses volumes, será necessário executar uma operação de backup ou restauração de linha de base sempre que o volume mudar de estado de somente leitura para leitura/gravação ou de leitura/gravação para somente leitura.

Como o dump funciona com um único arquivo SnapMirror ou restauração LUN

Antes de executar operações de backup de despejo ou restauração em um volume para o qual um único arquivo ou LUN é restaurado usando a tecnologia SnapMirror, você deve entender como as operações de despejo funcionam com um único arquivo ou operação de restauração LUN.

Durante uma operação de restauração de um único arquivo ou LUN do SnapMirror, a e/S do cliente é restrita no arquivo ou LUN que está sendo restaurado. Quando a operação de restauração de um único arquivo ou LUN terminar, a restrição de e/S no arquivo ou LUN é removida. Se um backup de despejo for executado em um volume para o qual um único arquivo ou LUN é restaurado, o arquivo ou LUN que tem restrição de e/S cliente não será incluído no backup de despejo. Em uma operação de backup subsequente, esse arquivo ou LUN é feito backup em fita após a restrição de e/S ser removida.

Não é possível executar uma restauração de despejo e uma operação de restauração de arquivo único SnapMirror ou LUN simultaneamente no mesmo volume.

Como as operações de backup e restauração de despejo são afetadas nas configurações do MetroCluster

Antes de executar operações de backup e restauração de despejo em uma configuração do MetroCluster, você deve entender como as operações de despejo são afetadas quando ocorre uma operação de switchover ou switchback.

Operação de backup ou restauração de despejo seguida de switchover

Considere dois clusters: Cluster 1 e cluster 2. Durante uma operação de backup de despejo ou restauração no

cluster 1, se um switchover for iniciado do cluster 1 para o cluster 2, ocorrerá o seguinte:

- Se o valor `override-vetoes` da opção for `false`, o switchover será abortado e a operação de backup ou restauração continua.
- Se o valor da opção for `true`, a operação de backup de despejo ou restauração é abortada e o switchover continua.

Operação de backup ou restauração de despejo seguida de switchback

Um switchover é executado do cluster 1 para o cluster 2 e uma operação de backup ou restauração de despejo é iniciada no cluster 2. A operação de despejo faz backup ou restaura um volume localizado no cluster 2. Neste ponto, se um switchback é iniciado do cluster 2 para o cluster 1, então ocorre o seguinte:

- Se o valor da `override-vetoes` opção for `false`, o switchback é cancelado e a operação de backup ou restauração continua.
- Se o valor da opção for `true`, a operação de backup ou restauração será abortada e o switchback continuará.

Operação de backup ou restauração de despejo iniciada durante um switchover ou switchback

Durante um switchover do cluster 1 para o cluster 2, se uma operação de backup de despejo ou restauração for iniciada no cluster 1, a operação de backup ou restauração falhará e o switchover continuará.

Durante um switchback do cluster 2 para o cluster 1, se uma operação de backup de despejo ou restauração for iniciada do cluster 2, a operação de backup ou restauração falhará e o switchback continuará.

Sobre o motor SMTape para volumes FlexVol

Sobre o motor SMTape para volumes FlexVol

O SMTape é uma solução de recuperação de desastres da ONTAP que faz backup de blocos de dados em fita. Você pode usar o SMTape para realizar backups de volume em fitas. No entanto, você não pode executar um backup no nível de qtree ou subárvore. O SMTape suporta backups de linha de base, diferenciais e incrementais. SMTape não requer uma licença.

Você pode executar uma operação de backup e restauração SMTape usando um aplicativo de backup compatível com NDMP. Você pode escolher SMTape para executar operações de backup e restauração somente no modo NDMP com escopo de máquina virtual de armazenamento (SVM).

> O processo de reversão não é suportado quando uma sessão de backup ou restauração do SMTape está em andamento. Você deve esperar até que a sessão termine ou você deve abortar a sessão NDMP.

Com o SMTape, você pode fazer backup de 255 cópias Snapshot. Para backups subsequentes de linha de base, incrementais ou diferenciais, você precisa excluir cópias Snapshot de backup mais antigas.

Antes de executar uma restauração de linha de base, o volume para o qual os dados estão sendo restaurados deve ser do tipo `DP` e esse volume deve estar no estado restrito. Após uma restauração bem-sucedida, esse volume é automaticamente online. É possível realizar restaurações incrementais ou diferenciais subsequentes nesse volume na ordem em que os backups foram executados.

Use cópias Snapshot durante o backup SMTape

Você deve entender como as cópias Snapshot são usadas durante um backup de linha de base do SMTape e um backup incremental. Há também considerações a ter em mente ao executar um backup usando SMTape.

Backup de linha de base

Durante a execução de um backup de linha de base, você pode especificar o nome da cópia Snapshot a ser feita em backup em fita. Se nenhuma cópia Snapshot for especificada, dependendo do tipo de acesso do volume (leitura/gravação ou somente leitura), uma cópia Snapshot será criada automaticamente ou as cópias Snapshot existentes serão usadas. Quando você especifica uma cópia Snapshot para o backup, todas as cópias Snapshot anteriores à cópia Snapshot especificada também são feitas backup em fita.

Se você não especificar uma cópia Snapshot para o backup, ocorrerá o seguinte:

- Para um volume de leitura/gravação, uma cópia Snapshot é criada automaticamente.

  O backup da cópia Snapshot recém-criada e de todas as cópias Snapshot mais antigas é feito em fita.

- Para um volume somente leitura, o backup de todas as cópias Snapshot, incluindo a cópia Snapshot mais recente, é feito em fita.

  Não é feito o backup de todas as novas cópias Snapshot criadas após o backup ser iniciado.

Backup incremental

Para operações de backup incrementais ou diferenciais do SMTape, os aplicativos de backup compatíveis com NDMP criam e gerenciam as cópias Snapshot.

Você sempre deve especificar uma cópia Snapshot durante a execução de uma operação de backup incremental. Para uma operação de backup incremental bem-sucedida, o backup da cópia Snapshot durante a operação de backup anterior (linha de base ou incremental) deve estar no volume a partir do qual o backup é executado. Para garantir que você use essa cópia Snapshot de backup, considere a política Snapshot atribuída a esse volume enquanto configura a política de backup.

Considerações sobre backups do SMTape em destinos do SnapMirror

- Uma relação de espelho de proteção de dados cria cópias Snapshot temporárias no volume de destino para replicação.

  Você não deve usar essas cópias Snapshot para backup SMTape.

- Se uma atualização do SnapMirror ocorrer em um volume de destino em um relacionamento de espelho de proteção de dados durante uma operação de backup do SMTape no mesmo volume, a cópia Snapshot que é backup do SMTape não deve ser excluída no volume de origem.

  Durante a operação de backup, o SMTape bloqueia a cópia Snapshot no volume de destino e, se a cópia Snapshot correspondente for excluída no volume de origem, a operação de atualização do SnapMirror subsequente falha.

- Você não deve usar essas cópias Snapshot durante o backup incremental.

Capacidades de SMTape

Os recursos do SMTape, como backup de cópias Snapshot, backups incrementais e diferenciais, preservação de recursos de deduplicação e compactação em volumes restaurados e semeadura em fita, ajudam a otimizar suas operações de backup e restauração em fita.

O SMTape oferece os seguintes recursos:

- Fornece uma solução de recuperação de desastres
- Permite backups incrementais e diferenciais
- Faz backup de cópias Snapshot
- Ativa o backup e a restauração de volumes deduplicados e preserva a deduplicação nos volumes restaurados
- Faz backup de volumes compatados e preserva a compactação nos volumes restaurados
- Ativa a semeadura da fita

O SMTape suporta o fator de bloqueio em múltiplos de 4 KB, na faixa de 4 KB a 256 KB.

Você pode restaurar os dados para volumes criados apenas em duas versões consecutivas do ONTAP.

Recursos não suportados no SMTape

O SMTape não suporta backups reiniciáveis e verificação de arquivos de backup.

Limites de escalabilidade para sessões de backup e restauração SMTape

Ao executar operações de backup e restauração SMTape através de NDMP ou CLI (tape seeding), você deve estar ciente do número máximo de sessões de backup e restauração SMTape que podem ser executadas simultaneamente em sistemas de armazenamento com diferentes capacidades de memória do sistema. Este número máximo depende da memória do sistema de um sistema de armazenamento.

Os limites de escalabilidade das sessões de backup e restauração SMTape são diferentes dos limites de sessão NDMP e dos limites de sessão de despejo.

Memória do sistema do sistema de armazenamento	Número total de sessões de backup e restauração SMTape
Menos de 16 GB	6
Maior ou igual a 16 GB, mas inferior a 24 GB	16
Maior ou igual a 24 GB	32

Você pode obter a memória do sistema do seu sistema de armazenamento usando o `sysconfig -a`

comando (disponível através do nodeshell). Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Informações relacionadas

Limites de escalabilidade para sessões NDMP

Limites de escalabilidade para sessões de backup e restauração de despejo

O que é a semeadura da fita

A semeadura de fita é uma funcionalidade SMTape que ajuda você a inicializar um FlexVol volume de destino em uma relação de espelho de proteção de dados.

A semeadura de fita permite estabelecer uma relação de espelho de proteção de dados entre um sistema de origem e um sistema de destino através de uma conexão de baixa largura de banda.

O espelhamento incremental das cópias Snapshot da origem para o destino é viável em uma conexão com baixa largura de banda. No entanto, um espelhamento inicial da cópia Snapshot de base leva muito tempo em uma conexão de baixa largura de banda. Nesses casos, você pode executar um backup SMTape do volume de origem para uma fita e usar a fita para transferir a cópia Snapshot de base inicial para o destino. Em seguida, você pode configurar atualizações incrementais de SnapMirror para o sistema de destino usando a conexão de baixa largura de banda.

Como o SMTape funciona com failover de armazenamento e operações ARL

Antes de executar operações de backup ou restauração do SMTape, você deve entender como essas operações funcionam com operações de failover de armazenamento (aquisição e giveback) ou realocação agregada (ARL). A `-override-vetoes` opção determina o comportamento do mecanismo SMTape durante um failover de armazenamento ou operação ARL.

Quando uma operação de backup ou restauração do SMTape estiver em execução e a `-override-vetoes` opção estiver definida como `false`, um failover de armazenamento iniciado pelo usuário ou operação ARL será interrompido e a operação de backup ou restauração será concluída. Se o aplicativo de backup suportar a EXTENSÃO CAB, você pode continuar executando operações incrementais de backup e restauração de SMTape sem reconfigurar políticas de backup. No entanto, se a `-override-vetoes` opção estiver definida como `true`, a operação de failover de armazenamento ou ARL será continuada e a operação de backup ou restauração SMTape será cancelada.

Informações relacionadas

"Gerenciamento de rede"

"Alta disponibilidade"

Como o SMTape funciona com a movimentação de volume

Operações de backup e operações de movimentação de volume do SMTape podem ser executadas em paralelo até que o sistema de armazenamento tente a fase final de transição. Após essa fase, as novas operações de backup SMTape não podem ser executadas no volume que está sendo movido. No entanto, as operações atuais continuam a ser executadas até a conclusão.

Antes de iniciar a fase de transição para um volume, a operação de movimentação de volume verifica as operações ativas de backup SMTape no mesmo volume. Se houver operações de backup ativas do SMTape, a operação de movimentação de volume passa para um estado de transição diferido e permite que as operações de backup do SMTape sejam concluídas. Depois que essas operações de backup forem concluídas, você deverá reiniciar manualmente a operação de movimentação de volume.

Se o aplicativo de backup suportar a EXTENSÃO CAB, você poderá continuar executando operações incrementais de backup em fita e restauração em volumes somente leitura/gravação e leitura sem reconfigurar políticas de backup.

As operações de restauração de linha de base e movimentação de volume não podem ser executadas simultaneamente; no entanto, a restauração incremental pode ser executada em paralelo com as operações de movimentação de volume, com o comportamento semelhante ao das operações de backup SMTape durante operações de movimentação de volume.

Como o SMTape funciona com operações de rehost de volume

As operações do SMTape não podem começar quando uma operação de rehost de volume está em andamento em um volume. Quando um volume está envolvido em uma operação de rehost de volume, as sessões de SMTape não devem ser iniciadas nesse volume.

Se qualquer operação de rehost de volume estiver em andamento, o backup ou restauração do SMTape falhará. Se um backup ou restauração do SMTape estiver em andamento, as operações de rehost de volume falharão com uma mensagem de erro apropriada. Essa condição se aplica a operações de backup ou restauração baseadas em NDMP e CLI.

Como a política de backup NDMP é afetada durante o ADB

Quando o balanceador de dados automático (ADB) está habilitado, o balanceador analisa as estatísticas de uso de agregados para identificar o agregado que excedeu a porcentagem de uso de alto limite configurada.

Depois de identificar o agregado que excedeu o limite, o balanceador identifica um volume que pode ser movido para agregados residentes em outro nó no cluster e tenta movê-lo. Essa situação afeta a política de backup configurada para esse volume porque se o aplicativo de gerenciamento de dados (DMA) não estiver ciente DA CAB, o usuário terá que reconfigurar a política de backup e executar a operação de backup da linha de base.

> Se o DMA estiver ciente DA CAB e a política de backup tiver sido configurada usando uma interface específica, o ADB não será afetado.

Como as operações de backup e restauração do SMTape são afetadas nas configurações do MetroCluster

Antes de executar operações de backup e restauração do SMTape em uma configuração do MetroCluster, você deve entender como as operações do SMTape são afetadas quando ocorre uma operação de comutação ou switchback.

Operação de backup ou restauração SMTape seguida de switchover

Considere dois clusters: Cluster 1 e cluster 2. Durante uma operação de backup ou restauração do SMTape no cluster 1, se um switchover for iniciado do cluster 1 para o cluster 2, ocorrerá o seguinte:

- Se o valor `-override-vetoes` da opção for `false`, o processo de comutação é abortado e a operação de backup ou restauração continua.
- Se o valor da opção for `true`, a operação de backup ou restauração do SMTape será abortada e o processo de comutação continuará.

Operação de backup ou restauração SMTape seguida de switchback

Um switchover é executado do cluster 1 para o cluster 2 e uma operação de backup ou restauração SMTape é iniciada no cluster 2. A operação SMTape faz backup ou restaura um volume localizado no cluster 2. Neste ponto, se um switchback é iniciado do cluster 2 para o cluster 1, então ocorre o seguinte:

- Se o valor da `-override-vetoes` opção for `false`, o processo de switchback será abortado e a operação de backup ou restauração continuará.
- Se o valor da opção for `true`, a operação de backup ou restauração será abortada e o processo de switchback continuará.

Operação de backup ou restauração SMTape iniciada durante um switchover ou switchback

Durante um processo de comutação do cluster 1 para o cluster 2, se uma operação de backup ou restauração do SMTape for iniciada no cluster 1, a operação de backup ou restauração falhará e o switchover continuará.

Durante um processo de switchback do cluster 2 para o cluster 1, se uma operação de backup ou restauração do SMTape for iniciada a partir do cluster 2, a operação de backup ou restauração falhará e o switchback continuará.

Monitore as operações de backup e restauração em fita para volumes FlexVol

Monitore as operações de backup e restauração em fita para uma visão geral do FlexVol volumes

Você pode exibir os arquivos de log de eventos para monitorar as operações de backup e restauração de fita. O ONTAP Registra automaticamente eventos significativos de backup e restauração e o momento em que eles ocorrem em um arquivo de log chamado `backup` no diretório do controlador `/etc/log/`. Por predefinição, o registo de eventos está definido para `on`.

Talvez você queira exibir arquivos de log de eventos pelos seguintes motivos:

- Verificar se um backup noturno foi bem-sucedido
- Coleta de estatísticas sobre operações de backup
- Para usar as informações em arquivos de log de eventos anteriores para ajudar a diagnosticar problemas com operações de backup e restauração

Uma vez por semana, os arquivos de log de eventos são girados. O `/etc/log/backup` ficheiro é renomeado para `/etc/log/backup.0`, o `/etc/log/backup.0` ficheiro é renomeado para `/etc/log/backup.1`, e assim por diante. O sistema salva os arquivos de log por até seis semanas; portanto, você pode ter até sete arquivos de mensagem (`/etc/log/backup.[0-5]`e o arquivo atual `/etc/log/backup`).

Acesse os arquivos de log de eventos

Você pode acessar os arquivos de log de eventos para operações de backup e restauração de fita `/etc/log/` no diretório usando o `rdfile` comando no nodeshell. Você pode exibir esses arquivos de log de eventos para monitorar operações de backup e restauração de fita.

Sobre esta tarefa

Com configurações adicionais, como uma função de controle de acesso com acesso ao `spi` serviço da Web ou uma conta de usuário configurada com o `http` método de acesso, você também pode usar um navegador da Web para acessar esses arquivos de log.

Passos

1. Para acessar o nodeshell, digite o seguinte comando:

   `node run -node node_name`

   `node_name` é o nome do nó.

2. Para acessar os arquivos de log de eventos para operações de backup e restauração de fita, digite o seguinte comando:

   `rdfile /etc/log/backup`

Informações relacionadas

"Administração do sistema"

O que é o formato de mensagem de log de eventos de despejo e restauração

Descrição geral do formato de mensagem de registo de eventos

Para cada evento de despejo e restauração, uma mensagem é gravada no arquivo de log de backup.

O formato da mensagem de log de eventos de despejo e restauração é o seguinte:

`type timestamp identifier event (event_info)`

A lista a seguir descreve os campos no formato de mensagem de log de eventos:

- Cada mensagem de log começa com um dos indicadores de tipo descritos na tabela a seguir:

Tipo	Descrição
registo	A registar evento
dmp	Evento de despejo
rst	Restaurar evento

- `timestamp` mostra a data e a hora do evento.
- O `identifier` campo para um evento de despejo inclui o caminho de despejo e o ID exclusivo para o despejo. O `identifier` campo para um evento de restauração usa apenas o nome do caminho de destino de restauração como um identificador exclusivo. As mensagens de eventos relacionadas ao log não incluem um `identifier` campo.

Quais são os eventos de Registro

O campo evento de uma mensagem que começa com um log especifica o início de um log ou o fim de um log.

Ele contém um dos eventos mostrados na tabela a seguir:

Evento	Descrição
Start_Logging (Iniciar registo)	Indica o início do registo ou que o registo foi ligado novamente após ser desativado.
Stop_Logging (Parar registo)	Indica que o registo foi desativado.

Quais são os eventos de despejo

O campo evento para um evento de despejo contém um tipo de evento seguido de informações específicas do evento entre parênteses.

A tabela a seguir descreve os eventos, suas descrições e as informações de eventos relacionados que podem ser gravadas para uma operação de despejo:

Evento	Descrição	Informações sobre eventos
Iniciar	O despejo NDMP é iniciado	Nível de despejo e o tipo de despejo
Fim	Despejos concluídos com sucesso	Quantidade de dados processados
Abortar	A operação é cancelada	Quantidade de dados processados
Opções	As opções especificadas são listadas	Todas as opções e seus valores associados, incluindo opções NDMP
Tape_open (fita aberta)	A fita está aberta para leitura/gravação	O novo nome do dispositivo de fita
Tape_Close (Fechar fita)	A fita está fechada para leitura/gravação	O nome do dispositivo de fita

Evento	Descrição	Informações sobre eventos
Mudança de fase	Um despejo está entrando em uma nova fase de processamento	O nome da nova fase
Erro	Um despejo encontrou um evento inesperado	Mensagem de erro
Snapshot	Uma cópia Snapshot é criada ou localizada	O nome e a hora da cópia Snapshot
Base_dump	Foi localizada uma entrada de despejo base no metafile interno	O nível e o tempo do despejo base (apenas para despejos incrementais)

Quais são os eventos de restauração

O campo evento para um evento de restauração contém um tipo de evento seguido de informações específicas de eventos entre parênteses.

A tabela a seguir fornece informações sobre os eventos, suas descrições e as informações de eventos relacionados que podem ser gravadas para uma operação de restauração:

Evento	Descrição	Informações sobre eventos
Iniciar	A restauração NDMP é iniciada	Nível de restauração e tipo de restauração
Fim	Restaurações concluídas com êxito	Número de arquivos e quantidade de dados processados
Abortar	A operação é cancelada	Número de arquivos e quantidade de dados processados
Opções	As opções especificadas são listadas	Todas as opções e seus valores associados, incluindo opções NDMP
Tape_open (fita aberta)	A fita está aberta para leitura/gravação	O novo nome do dispositivo de fita
Tape_Close (Fechar fita)	A fita está fechada para leitura/gravação	O nome do dispositivo de fita
Mudança de fase	Restaurar está entrando em uma nova fase de processamento	O nome da nova fase

Evento	Descrição	Informações sobre eventos
Erro	Restaurar encontros com um evento inesperado	Mensagem de erro

Ativar ou desativar o registo de eventos

Pode ativar ou desativar o registo de eventos.

Passos

1. Para ativar ou desativar o log de eventos, digite o seguinte comando no clustershell:

   `options -option_name backup.log.enable -option-value {on | off}`

   `on` ativa o registo de eventos.

   `off` desativa o registo de eventos.

   O registo de eventos está ativado por predefinição.

Mensagens de erro para backup em fita e restauração de volumes FlexVol

Fazer backup e restaurar mensagens de erro

Limitação de recursos: nenhum tópico disponível

- **Mensagem**

  `Resource limitation: no available thread`

- **Causa**

  O número máximo de threads de e/S de fita locais ativos está atualmente em uso. Você pode ter um máximo de 16 unidades de fita locais ativas.

- **Ações corretivas**

  Aguarde que alguns trabalhos de fita sejam concluídos antes de iniciar um novo trabalho de backup ou restauração.

Reserva de fita preemptada

- **Mensagem**

  `Tape reservation preempted`

- **Causa**

  A unidade de fita está em uso por outra operação ou a fita foi fechada prematuramente.

- **Ações corretivas**

Certifique-se de que a unidade de fita não está em uso por outra operação e que o aplicativo DMA não cancelou o trabalho e tente novamente.

Não foi possível inicializar o suporte

- **Mensagem**

  ```
  Could not initialize media
  ```

- **Causa**

  Você pode receber esse erro por um dos seguintes motivos:

  - A unidade de fita usada para o backup está corrompida ou danificada.
  - A fita não contém o backup completo ou está corrompida.
  - O número máximo de threads de e/S de fita locais ativos está atualmente em uso.

    Você pode ter um máximo de 16 unidades de fita locais ativas.

- **Ações corretivas**
  - Se a unidade de fita estiver corrompida ou danificada, tente novamente a operação com uma unidade de fita válida.
  - Se a fita não contiver o backup completo ou estiver corrompida, não será possível executar a operação de restauração.
  - Se os recursos de fita não estiverem disponíveis, aguarde que alguns dos trabalhos de backup ou restauração sejam concluídos e tente novamente a operação.

Número máximo de despejos ou restaurações permitidos (limite máximo de sessão) em andamento

- **Mensagem**

  ```
  Maximum number of allowed dumps or restores (maximum session limit) in
  progress
  ```

- **Causa**

  O número máximo de trabalhos de cópia de segurança ou restauro já está em execução.

- **Ações corretivas**

  Tente novamente a operação depois que alguns dos trabalhos atualmente em execução tiverem sido concluídos.

Erro de Mídia na gravação da fita

- **Mensagem**

  ```
  Media error on tape write
  ```

- **Causa**

  A fita usada para o backup está corrompida.

- **Ações corretivas**

  Substitua a fita e tente novamente o trabalho de backup.

Falha na gravação em fita

- **Mensagem**

  ```
  Tape write failed
  ```

- **Causa**

  A fita usada para o backup está corrompida.

- **Ações corretivas**

  Substitua a fita e tente novamente o trabalho de backup.

Falha na gravação da fita - erro de Mídia encontrado na nova fita

- **Mensagem**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Causa**

  A fita usada para o backup está corrompida.

- **Ações corretivas**

  Substitua a fita e tente novamente o backup.

Falha na gravação da fita - a nova fita está quebrada ou protegida contra gravação

- **Mensagem**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Causa**

  A fita usada para o backup está corrompida ou protegida contra gravação.

- **Ações corretivas**

  Substitua a fita e tente novamente o backup.

Falha na gravação em fita - a nova fita já está no final do material

- **Mensagem**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Causa**

Não há espaço suficiente na fita para concluir o backup.

- **Ações corretivas**

  Substitua a fita e tente novamente o backup.

Erro de gravação da fita

- **Mensagem**

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- **Causa**

  A capacidade da fita é insuficiente para conter os dados de backup.

- **Ações corretivas**

  Use fitas com maior capacidade e tente novamente o trabalho de backup.

Erro de Mídia na leitura da fita

- **Mensagem**

  ```
  Media error on tape read
  ```

- **Causa**

  A fita a partir da qual os dados estão sendo restaurados está corrompida e pode não conter os dados completos de backup.

- **Ações corretivas**

  Se tiver certeza de que a fita tem o backup completo, tente novamente a operação de restauração. Se a fita não contiver o backup completo, não será possível executar a operação de restauração.

Erro de leitura da fita

- **Mensagem**

  ```
  Tape read error
  ```

- **Causa**

  A unidade de fita está danificada ou a fita não contém o backup completo.

- **Ações corretivas**

  Se a unidade de fita estiver danificada, use outra unidade de fita. Se a fita não contiver o backup completo, não será possível restaurar os dados.

Já no final da fita

- **Mensagem**

  ```
  Already at the end of tape
  ```

- **Causa**

  A fita não contém dados nem deve ser enrolada novamente.

- **Ações corretivas**

  Se a fita não contiver dados, use a fita que contém o backup e tente novamente o trabalho de restauração. Caso contrário, rebobine a fita e tente novamente o trabalho de restauração.

O tamanho do Registro da fita é muito pequeno. Tente um tamanho maior.

- **Mensagem**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Causa**

  O fator de bloqueio especificado para a operação de restauração é menor do que o fator de bloqueio usado durante o backup.

- **Ações corretivas**

  Use o mesmo fator de bloqueio especificado durante o backup.

O tamanho do Registro da fita deve ser block_size1 e não block_size2

- **Mensagem**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Causa**

  O fator de bloqueio especificado para a restauração local está incorreto.

- **Ações corretivas**

  Tente novamente o trabalho de restauração com `block_size1` o como fator de bloqueio.

O tamanho do Registro da fita deve estar no intervalo entre 4KB e 256KB

- **Mensagem**

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- **Causa**

  O fator de bloqueio especificado para a operação de backup ou restauração não está dentro do intervalo permitido.

- **Ações corretivas**

  Especifique um fator de bloqueio no intervalo de 4 KB a 256 KB.

Mensagens de erro NDMP

Erro de comunicação de rede

- **Mensagem**

  ```
  Network communication error
  ```

- **Causa**

  A comunicação com uma fita remota em uma conexão de três vias NDMP falhou.

- **Ações corretivas**

  Verifique a ligação de rede ao motor remoto.

Mensagem do soquete de leitura: Error_string

- **Mensagem**

  ```
  Message from Read Socket: error_string
  ```

- **Causa**

  Restaurar a comunicação da fita remota na conexão NDMP de 3 vias tem erros.

- **Ações corretivas**

  Verifique a ligação de rede ao motor remoto.

Mensagem de Write Dirnet: Error_string

- **Mensagem**

  ```
  Message from Write Dirnet: error_string
  ```

- **Causa**

  A comunicação de backup para uma fita remota em uma conexão de três vias NDMP tem um erro.

- **Ações corretivas**

  Verifique a ligação de rede ao motor remoto.

Tomada de leitura recebida EOF

- **Mensagem**

  ```
  Read Socket received EOF
  ```

- **Causa**

  A tentativa de se comunicar com uma fita remota em uma conexão de três vias NDMP chegou ao fim da marca File. Você pode estar tentando uma restauração de três vias a partir de uma imagem de backup com um tamanho de bloco maior.

- **Ações corretivas**

  Especifique o tamanho correto do bloco e tente novamente a operação de restauração.

ndmpd número de versão inválido: version_number "

- **Mensagem**

  `ndmpd invalid version number: version_number`

- **Causa**

  A versão NDMP especificada não é suportada pelo sistema de storage.

- **Ações corretivas**

  Especifique a versão 4 do NDMP.

Sessão ndmpd session_ID não ativa

- **Mensagem**

  `ndmpd session session_ID not active`

- **Causa**

  A sessão NDMP pode não existir.

- **Ações corretivas**

  Use o `ndmpd status` comando para exibir as sessões NDMP ativas.

Não foi possível obter vol Ref para volume volume_name

- **Mensagem**

  `Could not obtain vol ref for Volume vol_name`

- **Causa**

  Não foi possível obter a referência de volume porque o volume pode estar a ser utilizado por outras operações.

- **Ações corretivas**

  Tente novamente a operação mais tarde.

Tipo de conexão de dados ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] não suportado para conexões de controle ["IPv6"|"IPv4"]

- **Mensagem**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- **Causa**

  No modo NDMP com escopo de nó, a conexão de dados NDMP estabelecida deve ser do mesmo tipo de endereço de rede (IPv4 ou IPv6) que a conexão de controle NDMP.

- **Ações corretivas**

  Entre em Contato com o fornecedor do aplicativo de backup.

ESCUTA DE DADOS: Conexão de dados DA CABINE preparar erro de pré-condição

- **Mensagem**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Causa**

  A escuta de dados NDMP falha quando o aplicativo de backup negociou a extensão CAB com o servidor NDMP e há uma incompatibilidade no tipo de endereço de conexão de dados NDMP especificado entre as mensagens NDMP_CAB_DATA_CONN_PREPARE e NDMP_DATA_LISTEN.

- **Ações corretivas**

  Entre em Contato com o fornecedor do aplicativo de backup.

CONEXÃO DE DADOS: Conexão de dados DA CAB preparar erro de pré-condição

- **Mensagem**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Causa**

  A conexão de dados NDMP falha quando o aplicativo de backup negociou a extensão CAB com o servidor NDMP e há uma incompatibilidade no tipo de endereço de conexão de dados NDMP especificado entre as mensagens NDMP_CAB_DATA_CONN_PREPARE e NDMP_DATA_CONNECT.

- **Ações corretivas**

  Entre em Contato com o fornecedor do aplicativo de backup.

Erro:show failed: Não é possível obter a senha do usuário '<username>'

- **Mensagem**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Causa**

  Configuração incompleta da conta de usuário para NDMP

- **Ações corretivas**

  Certifique-se de que a conta de utilizador está associada ao método de acesso SSH e que o método de autenticação é a palavra-passe de utilizador.

Mensagens de erro de despejo

O volume de destino é somente leitura

- **Mensagem**

  ```
  Destination volume is read-only
  ```

- **Causa**

  O caminho para o qual a operação de restauração é tentada é somente leitura.

- **Ações corretivas**

  Tente restaurar os dados para um local diferente.

A qtree de destino é somente leitura

- **Mensagem**

  ```
  Destination qtree is read-only
  ```

- **Causa**

  A qtree para a qual a restauração é tentada é somente leitura.

- **Ações corretivas**

  Tente restaurar os dados para um local diferente.

Despejos temporariamente desativados no volume, tente novamente

- **Mensagem**

  ```
  Dumps temporarily disabled on volume, try again
  ```

- **Causa**

  Tentativa de backup de despejo NDMP em um volume de destino do SnapMirror que faz parte de `snapmirror break` uma operação ou de uma `snapmirror resync`.

- **Ações corretivas**

  Aguarde até que a `snapmirror break` operação ou `snapmirror resync` termine e, em seguida, efetue a operação de descarga.

Sempre que o estado de um volume de destino do SnapMirror mudar de leitura/gravação para somente leitura ou de somente leitura para leitura/gravação, você deve executar um backup de linha de base.

Rótulos NFS não reconhecidos

- **Mensagem**

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- **Causa**

  As etiquetas de segurança NFS são suportadas a partir do ONTAP 9.9,1 quando o NFSv4,2 está ativado. No entanto, as etiquetas de segurança NFS não são reconhecidas atualmente pelo mecanismo de despejo. Se ele encontrar quaisquer rótulos de segurança NFS nos arquivos, diretórios ou quaisquer arquivos especiais em qualquer formato de despejo, o despejo falhará.

- **Ações corretivas**

  Verifique se nenhum arquivo ou diretório tem rótulos de segurança NFS.

Não foram criados ficheiros

- **Mensagem**

  ```
  No files were created
  ```

- **Causa**

  Um DAR de diretório foi tentado sem habilitar a funcionalidade DAR aprimorada.

- **Ações corretivas**

  Ative a funcionalidade DAR melhorada e tente novamente DAR.

A restauração do arquivo <file name> falhou

- **Mensagem**

  ```
  Restore of the file file name failed
  ```

- **Causa**

  Quando um DAR (Direct Access Recovery) de um arquivo cujo nome de arquivo é o mesmo que o de um LUN no volume de destino é executado, o DAR falha.

- **Ações corretivas**

  Tente DAR novamente do arquivo.

Falha no truncamento para src inode <inode number>…

- **Mensagem**

  `Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.`

- **Causa**

  Inode de um arquivo é excluído quando o arquivo está sendo restaurado.

- **Ações corretivas**

  Aguarde até que a operação de restauração em um volume seja concluída antes de usar esse volume.

Não é possível bloquear um instantâneo necessário pelo despejo

- **Mensagem**

  `Unable to lock a snapshot needed by dump`

- **Causa**

  A cópia Snapshot especificada para o backup não está disponível.

- **Ações corretivas**

  Tente novamente o backup com uma cópia Snapshot diferente.

  Use o `snap list` comando para ver a lista de cópias Snapshot disponíveis.

Não foi possível localizar ficheiros bitmap

- **Mensagem**

  `Unable to locate bitmap files`

- **Causa**

  Os arquivos bitmap necessários para a operação de backup podem ter sido excluídos. Neste caso, o backup não pode ser reiniciado.

- **Ações corretivas**

  Efetue a cópia de segurança novamente.

O volume está temporariamente em um estado de transição

- **Mensagem**

  `Volume is temporarily in a transitional state`

- **Causa**

O volume que está a ser guardado está temporariamente num estado não montado.

- **Ações corretivas**

  Aguarde algum tempo e efetue a cópia de segurança novamente.

Mensagens de erro SMTape

Pedaços fora de ordem

- **Mensagem**

  ```
  Chunks out of order
  ```

- **Causa**

  As fitas de backup não estão sendo restauradas na sequência correta.

- **Ações corretivas**

  Repita a operação de restauração e carregue as fitas na sequência correta.

Formato de bloco não suportado

- **Mensagem**

  ```
  Chunk format not supported
  ```

- **Causa**

  A imagem de backup não é do SMTape.

- **Ações corretivas**

  Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha o backup do SMTape.

Falha ao alocar memória

- **Mensagem**

  ```
  Failed to allocate memory
  ```

- **Causa**

  O sistema ficou sem memória.

- **Ações corretivas**

  Tente novamente o trabalho mais tarde quando o sistema não estiver muito ocupado.

Falha ao obter buffer de dados

- **Mensagem**

  ```
  Failed to get data buffer
  ```

- **Causa**

  O sistema de armazenamento ficou sem buffers.

- **Ações corretivas**

  Aguarde até que algumas operações do sistema de armazenamento sejam concluídas e, em seguida, tente novamente o trabalho.

Falha ao encontrar instantâneo

- **Mensagem**

  ```
  Failed to find snapshot
  ```

- **Causa**

  A cópia Snapshot especificada para o backup não está disponível.

- **Ações corretivas**

  Verifique se a cópia Snapshot especificada está disponível. Caso contrário, tente novamente com a cópia Snapshot correta.

Falha ao criar instantâneo

- **Mensagem**

  ```
  Failed to create snapshot
  ```

- **Causa**

  O volume já contém o número máximo de cópias Snapshot.

- **Ações corretivas**

  Exclua algumas cópias Snapshot e tente novamente a operação de backup.

Falha ao bloquear instantâneo

- **Mensagem**

  ```
  Failed to lock snapshot
  ```

- **Causa**

  A cópia Snapshot está em uso ou foi excluída.

- **Ações corretivas**

  Se a cópia Snapshot estiver a ser utilizada por outra operação, aguarde que a operação termine e, em seguida, tente novamente a cópia de segurança. Se a cópia Snapshot tiver sido excluída, não será possível executar a cópia de segurança.

Falha ao eliminar instantâneo

- **Mensagem**

  `Failed to delete snapshot`

- **Causa**

  A cópia Snapshot automática não pôde ser excluída porque está em uso por outras operações.

- **Ações corretivas**

  Use o `snap` comando para determinar o status da cópia Snapshot. Se a cópia Snapshot não for necessária, exclua-a manualmente.

Falha ao obter instantâneo mais recente

- **Mensagem**

  `Failed to get latest snapshot`

- **Causa**

  A cópia Snapshot mais recente pode não existir porque o volume está sendo inicializado pelo SnapMirror.

- **Ações corretivas**

  Tente novamente após a inicialização estar concluída.

Falha ao carregar nova fita

- **Mensagem**

  `Failed to load new tape`

- **Causa**

  Erro na unidade de fita ou Mídia.

- **Ações corretivas**

  Substitua a fita e tente novamente a operação.

Falha ao inicializar a fita

- **Mensagem**

```
Failed to initialize tape
```

- **Causa**

  Você pode receber esta mensagem de erro por um dos seguintes motivos:

  - A imagem de backup não é do SMTape.
  - O fator de bloqueio da fita especificado está incorreto.
  - A fita está corrompida ou danificada.
  - A fita errada é carregada para restauração.

- **Ações corretivas**
  - Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha backup do SMTape.
  - Se o fator de bloqueio estiver incorreto, especifique o fator de bloqueio correto e tente novamente a operação.
  - Se a fita estiver corrompida, não será possível executar a operação de restauração.
  - Se a fita errada estiver carregada, tente novamente a operação com a fita correta.

Falha ao inicializar o fluxo de restauração

- **Mensagem**

```
Failed to initialize restore stream
```

- **Causa**

  Você pode receber esta mensagem de erro por um dos seguintes motivos:

  - A imagem de backup não é do SMTape.
  - O fator de bloqueio da fita especificado está incorreto.
  - A fita está corrompida ou danificada.
  - A fita errada é carregada para restauração.

- **Ações corretivas**
  - Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha o backup do SMTape.
  - Se o fator de bloqueio estiver incorreto, especifique o fator de bloqueio correto e tente novamente a operação.
  - Se a fita estiver corrompida, não será possível executar a operação de restauração.
  - Se a fita errada estiver carregada, tente novamente a operação com a fita correta.

Falha ao ler a imagem de cópia de segurança

- **Mensagem**

```
Failed to read backup image
```

- **Causa**

A fita está corrompida.

- **Ações corretivas**

  Se a fita estiver corrompida, não será possível executar a operação de restauração.

Cabeçalho da imagem ausente ou corrompido

- **Mensagem**

  ```
  Image header missing or corrupted
  ```

- **Causa**

  A fita não contém um backup SMTape válido.

- **Ações corretivas**

  Tente novamente com uma fita contendo um backup válido.

Asserção interna

- **Mensagem**

  ```
  Internal assertion
  ```

- **Causa**

  Existe um erro interno do SMTape.

- **Ações corretivas**

  Comunique o erro e envie o `etc/log/backup` ficheiro para o suporte técnico.

Número mágico da imagem de cópia de segurança inválido

- **Mensagem**

  ```
  Invalid backup image magic number
  ```

- **Causa**

  A imagem de backup não é do SMTape.

- **Ações corretivas**

  Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha o backup do SMTape.

Soma de verificação da imagem de cópia de segurança inválida

- **Mensagem**

```
Invalid backup image checksum
```

- **Causa**

  A fita está corrompida.

- **Ações corretivas**

  Se a fita estiver corrompida, não será possível executar a operação de restauração.

Fita de entrada inválida

- **Mensagem**

  ```
  Invalid input tape
  ```

- **Causa**

  A assinatura da imagem de backup não é válida no cabeçalho da fita. A fita possui dados corrompidos ou não contém uma imagem de backup válida.

- **Ações corretivas**

  Tente novamente o trabalho de restauro com uma imagem de cópia de segurança válida.

Caminho de volume inválido

- **Mensagem**

  ```
  Invalid volume path
  ```

- **Causa**

  O volume especificado para a operação de backup ou restauração não foi encontrado.

- **Ações corretivas**

  Tente novamente o trabalho com um caminho de volume e um nome de volume válidos.

Incompatibilidade na ID do conjunto de cópias de segurança

- **Mensagem**

  ```
  Mismatch in backup set ID
  ```

- **Causa**

  A fita carregada durante uma mudança de fita não faz parte do conjunto de backup.

- **Ações corretivas**

  Carregue a fita correta e tente novamente o trabalho.

Não correspondência no carimbo de hora de cópia de segurança

- **Mensagem**

  `Mismatch in backup time stamp`

- **Causa**

  A fita carregada durante uma mudança de fita não faz parte do conjunto de backup.

- **Ações corretivas**

  Use o `smtape restore -h` comando para verificar as informações do cabeçalho de uma fita.

Trabalho cancelado devido ao encerramento

- **Mensagem**

  `Job aborted due to shutdown`

- **Causa**

  O sistema de armazenamento está sendo reinicializado.

- **Ações corretivas**

  Tente novamente o trabalho depois que o sistema de armazenamento for reiniciado.

Trabalho cancelado devido a snapshot autodelete

- **Mensagem**

  `Job aborted due to Snapshot autodelete`

- **Causa**

  O volume não tem espaço suficiente e acionou a exclusão automática de cópias Snapshot.

- **Ações corretivas**

  Liberte espaço no volume e tente novamente o trabalho.

A fita está atualmente em uso por outras operações

- **Mensagem**

  `Tape is currently in use by other operations`

- **Causa**

  A unidade de fita está em uso por outro trabalho.

- **Ações corretivas**

Tente novamente a cópia de segurança após o trabalho atualmente ativo terminar.

Fitas fora de ordem

- **Mensagem**

  ```
  Tapes out of order
  ```

- **Causa**

  A primeira fita da sequência da fita para a operação de restauração não tem o cabeçalho da imagem.

- **Ações corretivas**

  Carregue a fita com o cabeçalho da imagem e tente novamente o trabalho.

Falha na transferência (cancelada devido à operação MetroCluster)

- **Mensagem**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Causa**

  A operação SMTape é abortada devido a uma operação de comutação ou comutação.

- **Ações corretivas**

  Execute a operação SMTape após o término da operação de comutação ou switchback.

Falha na transferência (interrupção iniciada ARL)

- **Mensagem**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Causa**

  Enquanto uma operação SMTape estiver em andamento se uma realocação agregada for iniciada, a operação SMTape será abortada.

- **Ações corretivas**

  Execute a operação SMTape após a conclusão da operação de realocação de agregados.

Falha na transferência (interrupção iniciada pelo CFO)

- **Mensagem**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Causa**

  A operação SMTape é abortada devido a uma operação de failover de armazenamento (aquisição e

giveback) de um agregado CFO.

- **Ações corretivas**

  Executar a operação SMTape após o failover de armazenamento do CFO agregado terminar.

Falha na transferência (cancelamento iniciado pelo SFO)

- **Mensagem**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Causa**

  A operação SMTape é abortada devido a uma operação de failover de armazenamento (aquisição e giveback).

- **Ações corretivas**

  Execute a operação SMTape após a conclusão da operação de failover de armazenamento (aquisição e giveback).

Agregado subjacente sob migração

- **Mensagem**

  ```
  Underlying aggregate under migration
  ```

- **Causa**

  Se uma operação SMTape for iniciada em um agregado que está sob migração (failover de armazenamento ou realocação agregada), a operação SMTape falhará.

- **Ações corretivas**

  Execute a operação SMTape depois que a migração agregada terminar.

O volume está atualmente em migração

- **Mensagem**

  ```
  Volume is currently under migration
  ```

- **Causa**

  A migração de volume e o backup SMTape não podem ser executados simultaneamente.

- **Ações corretivas**

  Tente novamente o trabalho de cópia de segurança após a conclusão da migração de volume.

Volume off-line

- **Mensagem**

  `Volume offline`

- **Causa**

  O volume que está sendo feito backup está offline.

- **Ações corretivas**

  Coloque o volume on-line e tente novamente o backup.

Volume não restrito

- **Mensagem**

  `Volume not restricted`

- **Causa**

  O volume de destino para o qual os dados estão sendo restaurados não é restrito.

- **Ações corretivas**

  Restrinja o volume e tente novamente a operação de restauração.

Configuração NDMP

Visão geral da configuração NDMP

Você pode configurar rapidamente um cluster ONTAP 9 para usar o Protocolo de gerenciamento de dados de rede (NDMP) para fazer backup de dados diretamente em fita usando um aplicativo de backup de terceiros.

Se o aplicativo de backup oferecer suporte ao Cluster Aware Backup (CAB), você poderá configurar o NDMP como *SVM-scoped* ou *node-scoped*:

- O escopo do SVM no nível do cluster (admin SVM) permite fazer backup de todos os volumes hospedados em diferentes nós do cluster. NDMP com escopo SVM é recomendado, sempre que possível.
- O NDMP com escopo de nó permite fazer backup de todos os volumes hospedados nesse nó.

Se o aplicativo de backup não suportar CAB, você deve usar NDMP com escopo de nó.

NDMP com escopo SVM e escopo de nó são mutuamente exclusivos; eles não podem ser configurados no mesmo cluster.

O NDMP com escopo de nó está obsoleto no ONTAP 9.

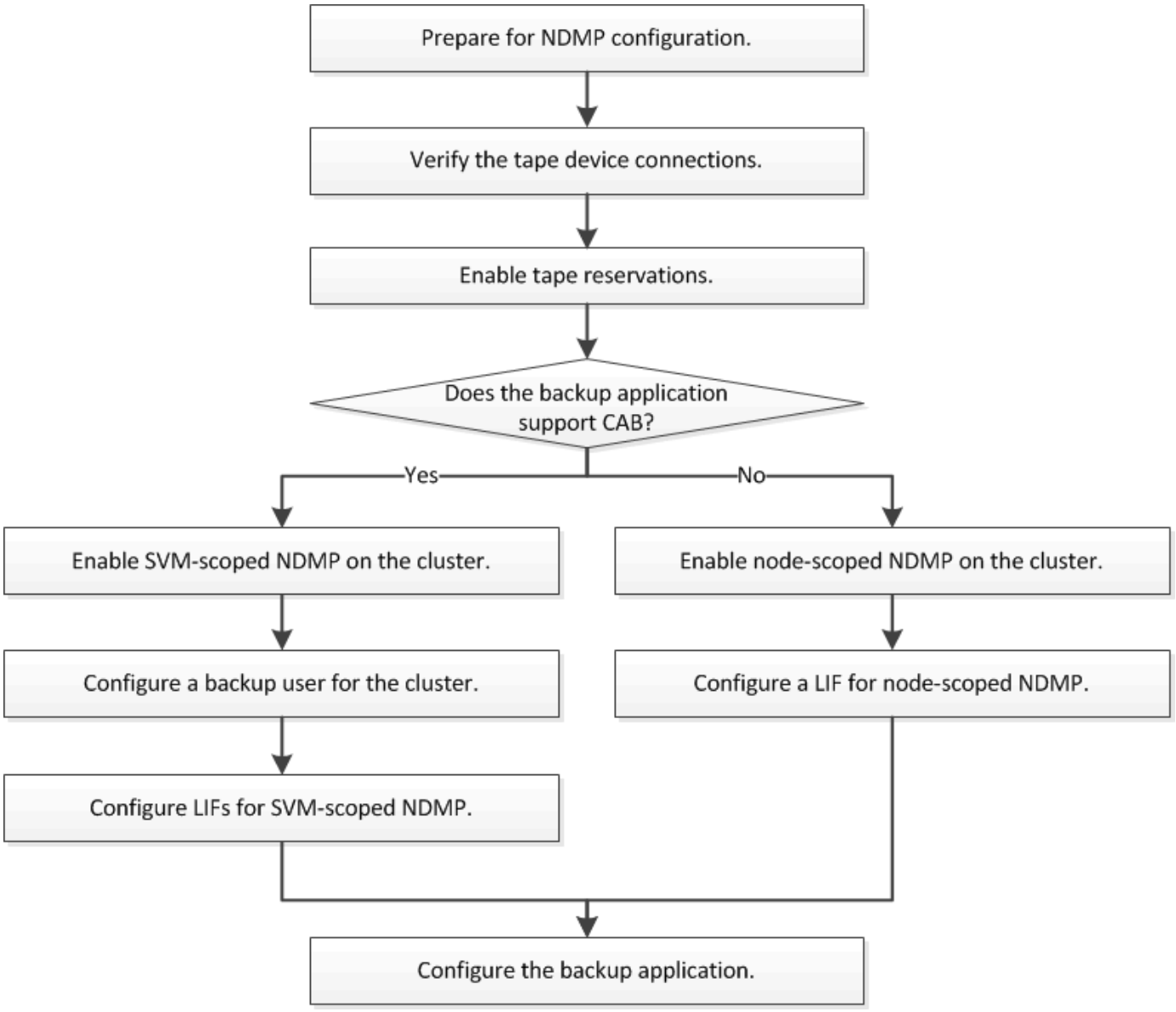
Saiba mais "Backup ciente de cluster (CAB)"sobre o .

Antes de configurar o NDMP, verifique o seguinte:

- Você tem um aplicativo de backup de terceiros (também chamado de aplicativo de gerenciamento de dados ou DMA).
- Você é um administrador de cluster.
- Dispositivos de fita e um servidor de Mídia opcional estão instalados.
- Os dispositivos de fita são conetados ao cluster por meio de um switch Fibre Channel (FC) ou conetados localmente.
- Pelo menos um dispositivo de fita tem um número de unidade lógica (LUN) de 0.

Fluxo de trabalho de configuração NDMP

A configuração do backup em fita no NDMP envolve a preparação para a configuração NDMP, a verificação das conexões do dispositivo de fita, a ativação de reservas de fita, a configuração do NDMP no nível do SVM ou nó, a ativação do NDMP no cluster, a configuração de um usuário de backup, a configuração de LIFs e a configuração do aplicativo de backup.



Prepare-se para a configuração NDMP

Antes de configurar o acesso de backup em fita pelo Network Data Management Protocol (NDMP), você deve verificar se a configuração planejada é suportada, verificar se suas unidades de fita estão listadas como unidades qualificadas em cada nó, verificar se todos os nós têm LIFs entre clusters e identificar se o aplicativo de backup suporta a extensão CAB (Cluster Aware Backup).

Passos

1. Consulte a matriz de compatibilidade do fornecedor do aplicativo de backup para obter suporte ao ONTAP (o NetApp não qualifica aplicativos de backup de terceiros com ONTAP ou NDMP).

   Você deve verificar se os seguintes componentes do NetApp são compatíveis:

   - A versão do ONTAP 9 que está sendo executada no cluster.
   - O fornecedor e a versão do aplicativo de backup: Por exemplo, Veritas NetBackup 8,2 ou CommVault.

- Os detalhes dos dispositivos de fita, como o fabricante, o modelo e a interface das unidades de fita: Por exemplo, IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- As plataformas dos nós no cluster: Por exemplo, FAS8700 ou A400.

> Você pode encontrar matrizes de suporte de compatibilidade legadas do ONTAP para aplicativos de backup no "Ferramenta de Matriz de interoperabilidade do NetApp".

2. Verifique se suas unidades de fita estão listadas como unidades qualificadas no arquivo de configuração de fita interno de cada nó:

   a. Na interface de linha de comando, visualize o arquivo de configuração de fita incorporado usando o `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                 Is
Tape Drives                      Supported  Support Status
-------------------------------  ---------
--------------------------------
Certance Ultrium 2               true       Dynamically Qualified
Certance Ultrium 3               true       Dynamically Qualified
Digital DLT2000                  true       Qualified
```

   b. Compare suas unidades de fita com a lista de unidades qualificadas na saída.

> Os nomes dos dispositivos de fita na saída podem variar ligeiramente dos nomes na etiqueta do dispositivo ou na Matriz de interoperabilidade. Por exemplo, o Digital DLT2000 também pode ser conhecido como DLT2k. Você pode ignorar essas pequenas diferenças de nomenclatura.

   c. Se um dispositivo não estiver listado como qualificado na saída, mesmo que o dispositivo esteja qualificado de acordo com a Matriz de interoperabilidade, baixe e instale um arquivo de configuração atualizado para o dispositivo usando as instruções no site de suporte da NetApp.

      "Downloads do NetApp: Arquivos de configuração do dispositivo de fita"

   Um dispositivo qualificado pode não estar listado no arquivo de configuração de fita incorporado se o dispositivo de fita tiver sido qualificado após o nó ser enviado.

3. Verifique se cada nó no cluster tem um LIF entre clusters:

   a. Visualize as LIFs entre clusters nos nós usando o `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

b. Se um LIF entre clusters não existir em nenhum nó, crie um LIF entre clusters usando o `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

"Gerenciamento de rede"

4. Identifique se o aplicativo de backup suporta Backup ciente de cluster (CAB) usando a documentação fornecida com o aplicativo de backup.

   O suporte DA CAB é um fator chave para determinar o tipo de backup que você pode executar.

Verifique as conexões do dispositivo de fita

Você deve garantir que todas as unidades e alteradores de Mídia estejam visíveis no ONTAP como dispositivos.

Passos

1. Veja informações sobre todas as unidades e modificadores de Mídia usando o `storage tape show` comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID               Device Type     Description
Status
----------------------  -------------  ------------------------------
--------
sw4:10.11               tape drive      HP LTO-3
normal
0b.125L1                media changer   HP MSL G3 Series
normal
0d.4                    tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                  media changer   IBM 3573-TL
normal
...
```

2. Se uma unidade de fita não for exibida, solucione o problema.
3. Se um trocador de Mídia não for exibido, exiba informações sobre alteradores de Mídia usando o `storage tape show-media-changer` comando e solucione o problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Ative as reservas de fita

Você deve garantir que as unidades de fita sejam reservadas para uso por aplicativos de backup para operações de backup NDMP.

Sobre esta tarefa

As configurações de reserva variam em diferentes aplicativos de backup, e essas configurações devem corresponder ao aplicativo de backup e aos nós ou servidores que usam as mesmas unidades. Consulte a documentação do fornecedor do aplicativo de backup para obter as configurações corretas de reserva.

Passos

1. Ative as reservas usando o `options -option-name tape.reservations -option-value persistent` comando.

   O seguinte comando permite reservas com o `persistent` valor:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Verifique se as reservas estão ativadas em todos os nós usando o `options tape.reservations` comando e, em seguida, revise a saída.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                persistent

   cluster1-2
       tape.reservations                persistent
   2 entries were displayed.
   ```

Configurar NDMP com escopo SVM

Habilite NDMP com escopo SVM no cluster

Se o DMA oferecer suporte à extensão CAB (Cluster Aware Backup), você poderá fazer backup de todos os volumes hospedados em diferentes nós em um cluster habilitando NDMP com escopo SVM, habilitando o serviço NDMP no cluster (admin SVM) e configurando LIFs para conexão de dados e controle.

O que você vai precisar

A extensão DA CABINA tem de ser suportada pelo DMA.

Sobre esta tarefa

Desativar o modo NDMP com escopo de nó ativa o modo NDMP com escopo SVM no cluster.

Passos

1. Ativar o modo NDMP com escopo SVM:

```
cluster1::> system services ndmp node-scope-mode off
```

   O modo NDMP com escopo SVM está ativado.

2. Habilite o serviço NDMP no administrador SVM:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

   O tipo de autenticação é definido como `challenge` por padrão e a autenticação de texto sem formatação é desativada.

   Para uma comunicação segura, você deve manter a autenticação em texto simples desativada.

3. Verifique se o serviço NDMP está ativado:

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Ative um usuário de backup para autenticação NDMP

Para autenticar NDMP com escopo SVM a partir do aplicativo de backup, deve haver um usuário administrativo com Privileges suficiente e uma senha NDMP.

Sobre esta tarefa

Você deve gerar uma senha NDMP para usuários de administração de backup. É possível habilitar usuários de administração de backup no nível de cluster ou SVM e, se necessário, criar um novo usuário. Por padrão, os usuários com as seguintes funções podem se autenticar para backup NDMP:

- Em todo o cluster: `admin` Ou `backup`
- SVMs individuais: `vsadmin` Ou `vsadmin-backup`

Se estiver a utilizar um utilizador NIS ou LDAP, o utilizador tem de existir no respetivo servidor. Você não pode usar um usuário do ative Directory.

Passos

1. Exibir os usuários e permissões de administrador atuais:

```
security login show
```

2. Se necessário, crie um novo usuário de backup NDMP com o `security login create` comando e a função apropriada para o SVM Privileges individual ou em todo o cluster.

   Pode especificar um nome de utilizador de cópia de segurança local ou um nome de utilizador NIS ou LDAP para o `-user-or-group-name` parâmetro.

   O comando a seguir cria o usuário de backup `backup_admin1` com a `backup` função para todo o cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   O comando a seguir cria o usuário de `vsbackup_admin1` backup com a `vsadmin-backup` função de um SVM individual:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Introduza uma palavra-passe para o novo utilizador e confirme.

3. Gere uma senha para o administrador SVM usando o `vserver services ndmp generate password` comando.

   A senha gerada deve ser usada para autenticar a conexão NDMP pelo aplicativo de backup.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   Password: qG5CqQHYxw7tE57g
   ```

Configurar LIFs

Você precisa identificar os LIFs que serão usados para estabelecer uma conexão de dados entre os recursos de dados e fita, e para conexão de controle entre o SVM admin e o aplicativo de backup. Depois de identificar os LIFs, você deve verificar se as políticas de serviço e failover estão definidas.

> 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, "Gerencie o tráfego suportado"consulte .

ONTAP 9.10,1 ou posterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

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

2. Identifique o LIF de gerenciamento hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

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

3. Certifique-se de que o LIF entre clusters inclui o `backup-ndmp-control` serviço:

   ```
   network interface service-policy show
   ```

4. Certifique-se de que a política de failover esteja definida adequadamente para todos os LIFs:

   a. Verifique se a política de failover para o gerenciamento de cluster está definida como `broadcast-domain-wide`, e se a política para LIFs de gerenciamento de clusters e nós está definida como `local-only` usando o `network interface show -failover` comando.

      O comando a seguir exibe a política de failover para as LIFs de gerenciamento de clusters, clusters e nós:

```
cluster1::> network interface show -failover

          Logical          Home             Failover    Failover
Vserver   Interface        Node:Port        Policy      Group
-------   --------------   --------------   ----------  --------
cluster   cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                        Failover
Targets:
                                                        .......
cluster1  cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                        Failover
Targets:
                                                        .......
          IC1              cluster1-1:e0a   local-only  Default
                                                        Failover
Targets:
          IC2              cluster1-1:e0b   local-only  Default
                                                        Failover
Targets:
                                                        .......
cluster1-1 c1-1_mgmt1      cluster1-1:e0m   local-only  Default
                                                        Failover
Targets:
                                                        ......
cluster1-2 c1-2_mgmt1      cluster1-2:e0m   local-only  Default
                                                        Failover
Targets:
                                                        ......
```

a. Se as políticas de failover não forem definidas adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

5. Especifique os LIFs necessários para a conexão de dados usando o `vserver services ndmp modify` comando com o `preferred-interface-role` parâmetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Verifique se a função de interface preferida está definida para o cluster usando o `vserver`

`services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9 1.9 ou anterior

Passos

1. Identifique os LIFs entre clusters, gerenciamento de cluster e gerenciamento de nós usando o `network interface show` comando com o `-role` parâmetro.

   O comando a seguir exibe as LIFs entre clusters:

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   O comando a seguir exibe o LIF de gerenciamento de cluster:

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

   O comando a seguir exibe as LIFs de gerenciamento de nó:

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

2. Certifique-se de que a política de firewall está ativada para NDMP nos (`node-mgmt`LIFs entre clusters, gerenciamento de cluster (`cluster-mgmt`) e gerenciamento de nós):

   a. Verifique se a política de firewall está habilitada para NDMP usando o `system services firewall policy show` comando.

      O comando a seguir exibe a política de firewall para o LIF de gerenciamento de cluster:

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      O comando a seguir exibe a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

O comando a seguir exibe a política de firewall para o LIF de gerenciamento de nós:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Se a política de firewall não estiver ativada, ative a política de firewall utilizando o `system services firewall policy modify` comando com o `-service` parâmetro.

O seguinte comando ativa a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Certifique-se de que a política de failover esteja definida adequadamente para todos os LIFs:

a. Verifique se a política de failover para o gerenciamento de cluster está definida como `broadcast-domain-wide`, e se a política para LIFs de gerenciamento de clusters e nós está definida como `local-only` usando o `network interface show -failover` comando.

   O comando a seguir exibe a política de failover para as LIFs de gerenciamento de clusters, clusters e nós:

```
cluster1::> network interface show -failover

          Logical            Home               Failover
Failover
Vserver   Interface          Node:Port          Policy
Group
--------- -----------------  ------------------ --------------------
--------
cluster   cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1  cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
          IC1                 cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
          IC2                 cluster1-1:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1  cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1  cluster1-2:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
```

a. Se as políticas de failover não forem definidas adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Especifique os LIFs necessários para a conexão de dados usando o `vserver services ndmp modify` comando com o `preferred-interface-role` parâmetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verifique se a função de interface preferida está definida para o cluster usando o `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

Configurar NDMP com escopo de nó

Habilite NDMP com escopo de nó no cluster

Você pode fazer backup de volumes hospedados em um único nó habilitando NDMP com escopo de nó, habilitando o serviço NDMP e configurando um LIF para conexão de dados e controle. Isso pode ser feito para todos os nós do cluster.

O NDMP com escopo de nó está obsoleto no ONTAP 9.

Sobre esta tarefa

Ao usar NDMP no modo de escopo de nó, a autenticação deve ser configurada por nó. Para obter mais informações, "O artigo da base de dados de Conhecimento "como configurar a autenticação NDMP no modo 'nó-escopo'""consulte .

Passos

1. Ativar o modo NDMP com escopo de nó:

```
cluster1::> system services ndmp node-scope-mode on
```

O modo de escopo do nó NDMP está ativado.

2. Habilite o serviço NDMP em todos os nós do cluster:

   O uso do curinga "'*" permite o serviço NDMP em todos os nós ao mesmo tempo.

   Você deve especificar uma senha para autenticação da conexão NDMP pelo aplicativo de backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Desative a `-clear-text` opção de comunicação segura da senha NDMP:

   Usando a opção curinga "'*" `disables the `-clear-text` em todos os nós ao mesmo tempo.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Verifique se o serviço NDMP está ativado e se a `-clear-text` opção está desativada:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configurar um LIF

Você deve identificar um LIF que será usado para estabelecer uma conexão de dados e controlar a conexão entre o nó e o aplicativo de backup. Depois de identificar o LIF, você deve verificar se as políticas de firewall e failover estão definidas para o LIF.

> 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, "Gerencie o tráfego suportado"consulte .

ONTAP 9.10,1 ou posterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

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

2. Certifique-se de que o LIF entre clusters inclui o `backup-ndmp-control` serviço:

   ```
   network interface service-policy show
   ```

3. Certifique-se de que a política de failover esteja definida adequadamente para os LIFs entre clusters:

   a. Verifique se a política de failover para os LIFs entre clusters está definida como `local-only` usando o `network interface show -failover` comando.

   ```
   cluster1::> network interface show -failover
               Logical          Home               Failover
   Failover
   Vserver     Interface        Node:Port          Policy       Group
   --------    ---------------  -----------------  ------------
   --------
   cluster1    IC1               cluster1-1:e0a    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
               IC2               cluster1-2:e0b    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   ```

   b. Se a política de failover não for definida adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

   ```
   cluster1::> network interface modify -vserver cluster1 -lif IC1
   -failover-policy local-only
   ```

ONTAP 9 1.9 ou anterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-role` parâmetro.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. Certifique-se de que a política de firewall está ativada para NDMP nos LIFs entre clusters:

   a. Verifique se a política de firewall está habilitada para NDMP usando o `system services firewall policy show` comando.

   O comando a seguir exibe a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. Se a política de firewall não estiver ativada, ative a política de firewall utilizando o `system services firewall policy modify` comando com o `-service` parâmetro.

   O seguinte comando ativa a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Certifique-se de que a política de failover esteja definida adequadamente para os LIFs entre clusters:
   a. Verifique se a política de failover para os LIFs entre clusters está definida como `local-only` usando o `network interface show -failover` comando.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. Se a política de failover não for definida adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configure a aplicação de cópia de segurança

Depois que o cluster é configurado para o acesso NDMP, você deve coletar informações da configuração do cluster e, em seguida, configurar o resto do processo de backup no aplicativo de backup.

Passos

1. Reúna as seguintes informações que você configurou anteriormente no ONTAP:
   - O nome de usuário e a senha que o aplicativo de backup requer para criar a conexão NDMP
   - Os endereços IP das LIFs entre clusters que o aplicativo de backup requer para se conetar ao cluster
2. No ONTAP, exiba os aliases atribuídos pelo ONTAP a cada dispositivo usando o `storage tape alias show` comando.

   Os aliases são muitas vezes úteis na configuração do aplicativo de backup.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                          Alias     Mapping
----------------------------- --------- ------------------------------
stsw-3220-4a-4b-02            st2       SN[HU19497WVR]
...
```

3. No aplicativo de backup, configure o restante do processo de backup usando a documentação do aplicativo de backup.

Depois de terminar

Se ocorrer um evento de mobilidade de dados, como uma movimentação de volume ou migração de LIF, você deve estar preparado para reinicializar quaisquer operações de backup interrompidas.

Visão geral da replicação entre o software NetApp Element e o ONTAP

Você pode garantir a continuidade dos negócios em um sistema Element usando o SnapMirror para replicar cópias Snapshot de um volume Element para um destino ONTAP. No caso de um desastre no local do Element, você pode fornecer dados aos clientes a partir do sistema ONTAP e reativar o sistema Element quando o serviço for restaurado.

A partir do ONTAP 9.4, é possível replicar cópias Snapshot de um LUN criado em um nó ONTAP de volta para um sistema Element. Você pode ter criado um LUN durante uma interrupção no site do Element ou pode estar usando um LUN para migrar dados do software ONTAP para o Element.

"Configurar a replicação do software NetApp Element e do ONTAP".

Informações sobre direitos autorais

Informações sobre marcas comerciais