



# Gerenciar arquivos WORM

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Gerenciar arquivos WORM ..... 1
  - Gerenciar arquivos WORM ..... 1
  - Armazene dados no WORM ..... 1
  - Armazene snapshots em WORM em um destino de cofre ..... 5
  - Espelhar arquivos WORM para recuperação de desastres ..... 9
  - Retenha arquivos WORM durante o litígio usando retenção legal ..... 13
  - Exclua a visão geral de arquivos WORM ..... 14

# 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` de 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 `SVMvs1`:

```
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.

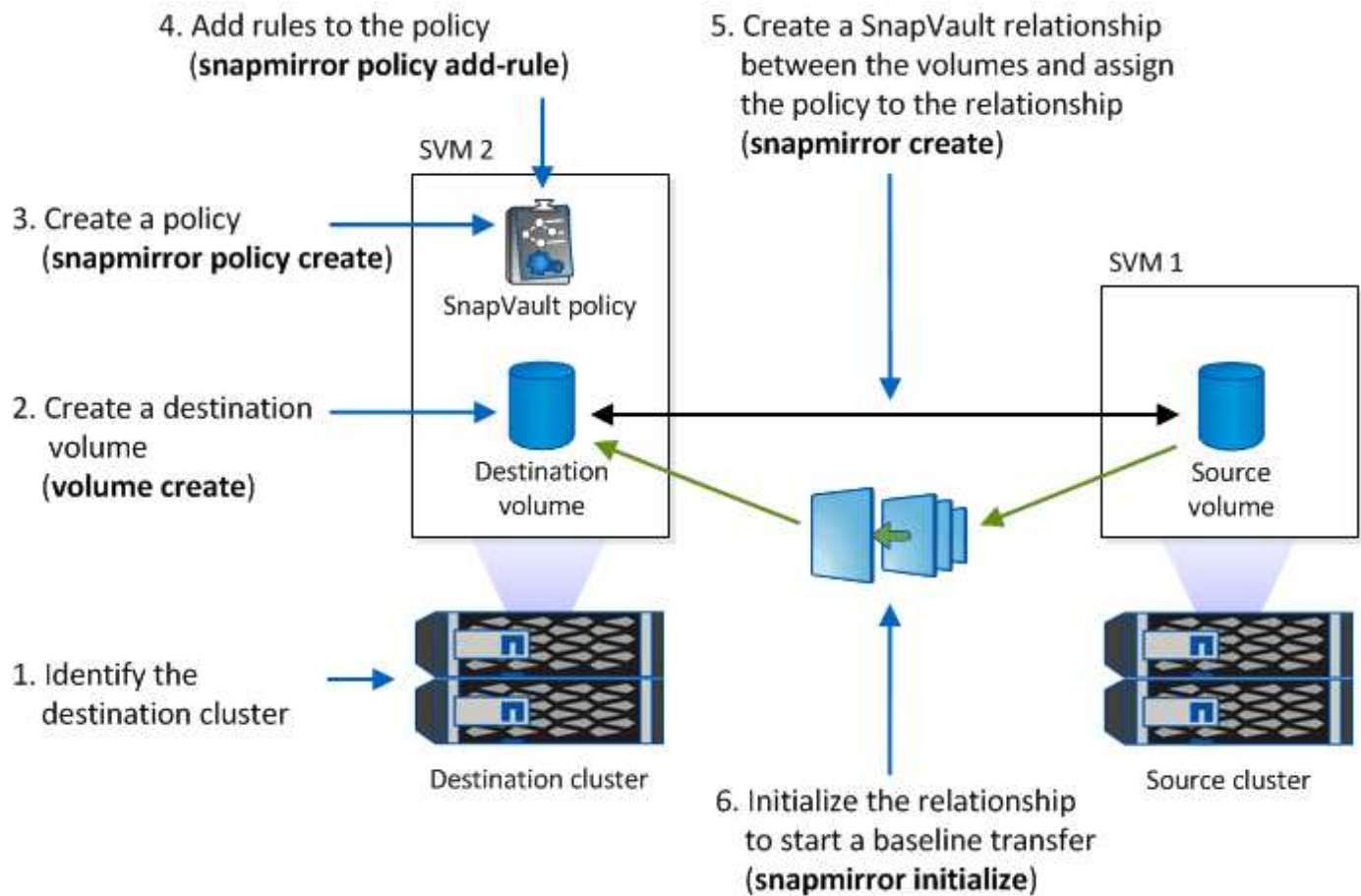
A partir do ONTAP 9.13.1, é possível restaurar instantaneamente um instantâneo bloqueado no volume SnapLock de destino de uma relação de Vault do SnapLock criando um FlexClone com a `snaplock-type` opção definida `non-snaplock` e especificando o instantâneo como o "pai-instantâneo" ao executar a operação 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 resincronização 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 resincronizada 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 resincronizada 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 resincronização após uma pausa, mesmo que os dados no destino tenham divergido da origem após a quebra.

Em uma ressinchronização, 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.

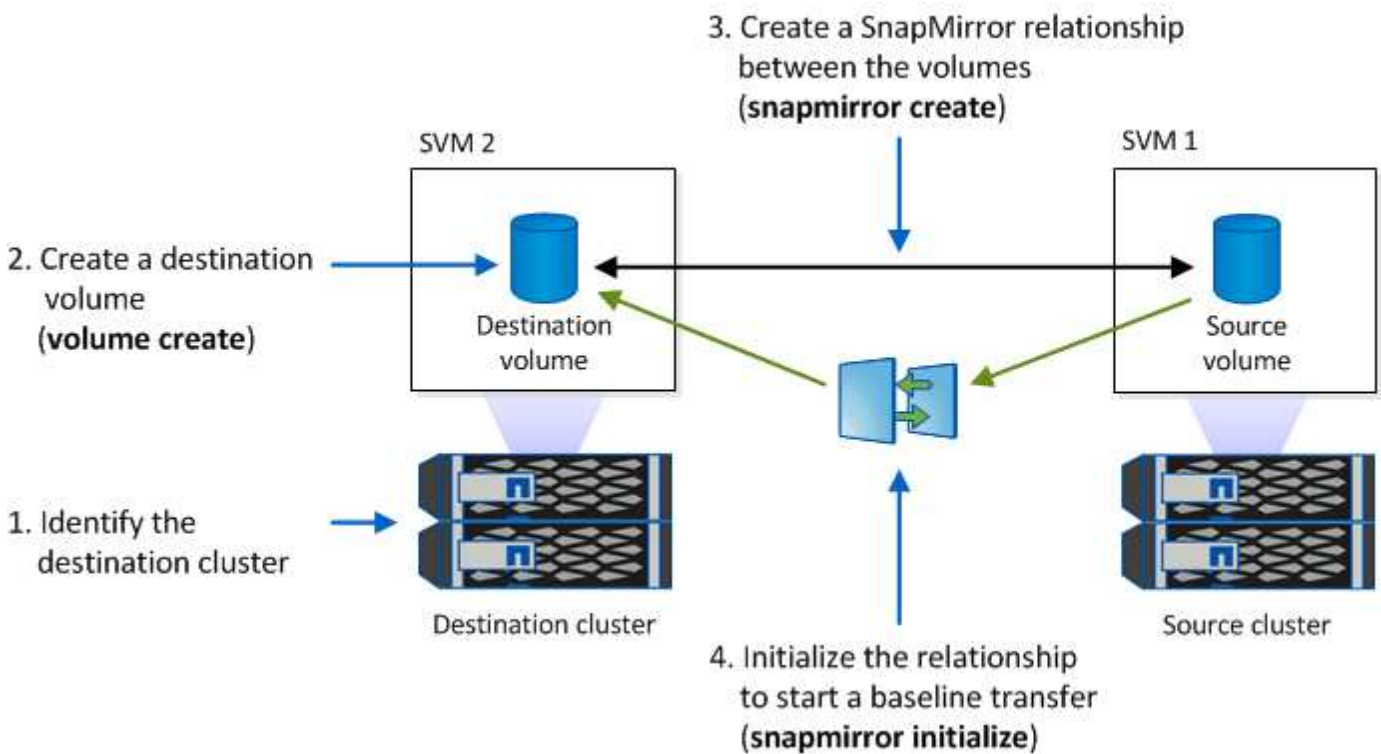
Se o volume de destino tiver um período de expiração posterior à origem, o período de expiração do destino será retido e não será substituído pelo período de expiração do volume de origem após a ressinchronização.

Se o destino tiver retenções legais que diferem da origem, não é permitido fazer uma ressinchronização. A origem e o destino devem ter retenção legal idêntica ou todas as retenção legal no destino devem ser liberadas antes de uma ressinchronização 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 voll:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
voll1 -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
```

## **Informações sobre direitos autorais**

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

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

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

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

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

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

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

## **Informações sobre marcas comerciais**

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