



# Arquivamento e conformidade com a tecnologia SnapLock

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Arquivamento e conformidade com a tecnologia SnapLock ..... 1
  - O que é SnapLock ..... 1
  - Configurar o SnapLock ..... 6
  - Gerenciar arquivos WORM ..... 21
  - Mover um volume SnapLock ..... 36
  - Bloqueie um snapshot para proteção contra ataques de ransomware ..... 38
  - APIs da SnapLock ..... 45

# 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 eletrônicos](#)" 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 <a href="#">"Virtualização FlexArray"</a> )
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 <a href="#">Criptografia e SnapLock</a> sobre o .	Sim, começando com ONTAP 9.2. Saiba mais <a href="#">Criptografia e SnapLock</a> sobre o .
FabricPools em agregados SnapLock	Não	Sim, começando com ONTAP 9.8. Saiba mais <a href="#">FabricPool em agregados SnapLock Enterprises</a> sobre 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 <a href="#">[flexgroup]</a> sobre o .	Sim, começando com ONTAP 9.11,1. Saiba mais <a href="#">[flexgroup]</a> sobre o .
LUNs	Não. Saiba mais sobre <a href="#">Suporte LUN</a> o SnapLock.	Não. Saiba mais sobre <a href="#">Suporte LUN</a> o SnapLock.
Configurações do MetroCluster	Sim, começando com ONTAP 9.3. Saiba mais <a href="#">Suporte à MetroClusters</a> sobre o .	Sim, começando com ONTAP 9.3. Saiba mais <a href="#">Suporte à MetroClusters</a> sobre o .
Verificação multi-admin (MAV)	Sim, começando com ONTAP 9.13,1. Saiba mais <a href="#">Suporte MAV</a> sobre o .	Sim, começando com ONTAP 9.13,1. Saiba mais <a href="#">Suporte MAV</a> sobre 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 <a href="#">suporte à eficiência de storage</a> sobre o .	Sim, começando com ONTAP 9.9,1. Saiba mais <a href="#">suporte à eficiência de storage</a> sobre 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 detecta 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:

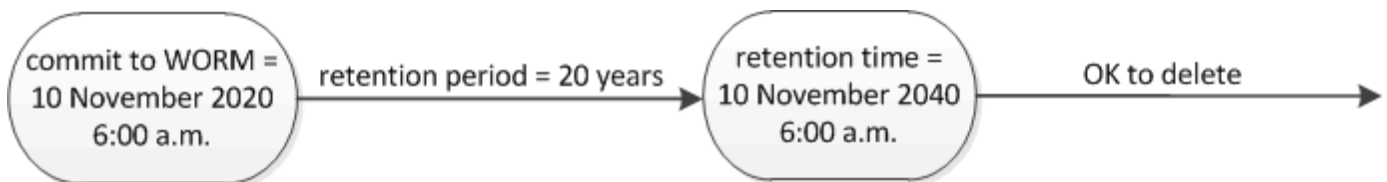
```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

## 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 voll -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 voll -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 voll -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume voll -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 voll -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 voll -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 registro 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`

`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/slc/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:8iMjqJXiNcqqXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=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 `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 .

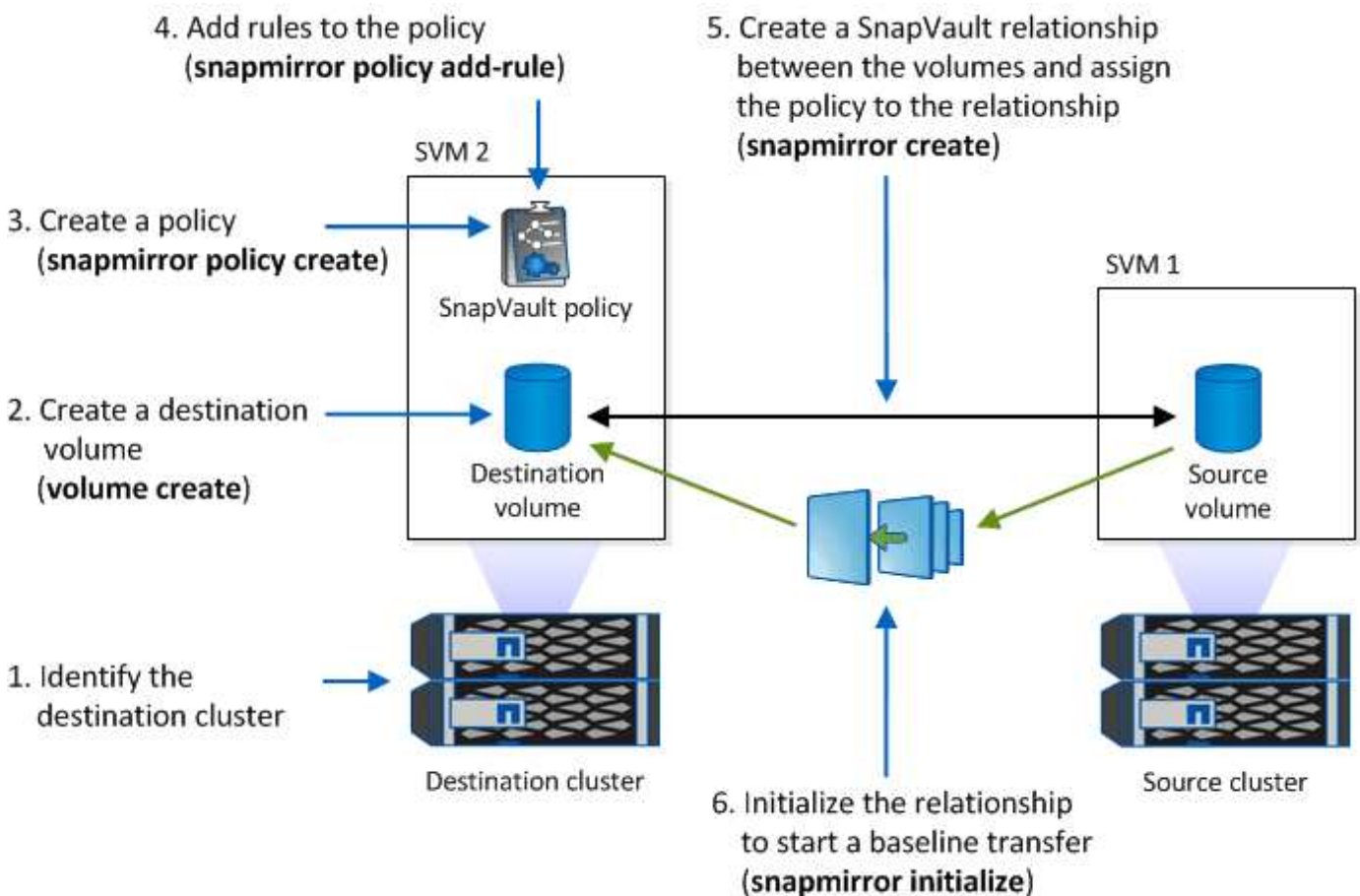
A partir do ONTAP 9.14.1, é possível especificar períodos de retenção para rótulos SnapMirror específicos na política SnapMirror da relação SnapMirror para que os snapshots replicados da origem para o volume de destino sejam retidos pelo período de retenção especificado na regra. Se nenhum período de 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 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.

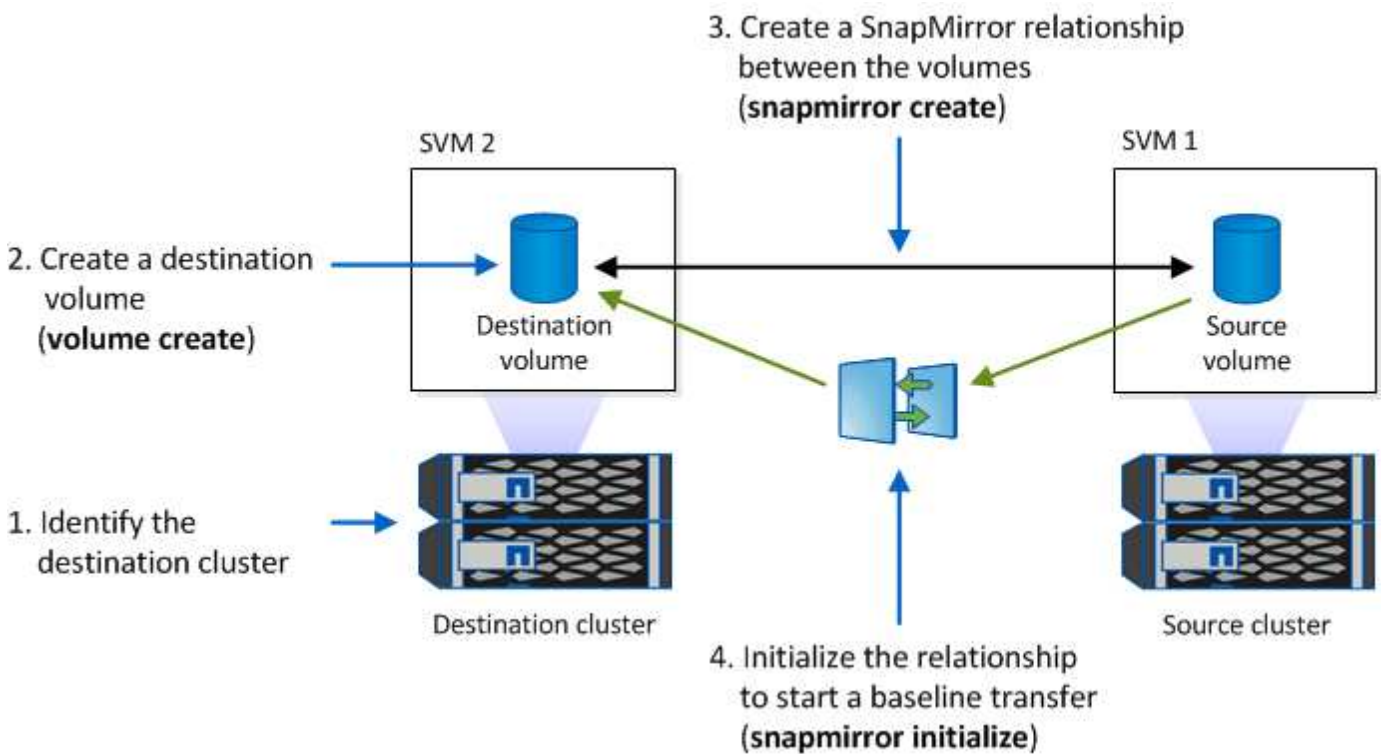
Se o volume de destino tiver um período de expiração posterior à origem, o período de expiração do destino será retido e não será substituído pelo período de expiração do volume de origem após a ressincronização.

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  
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
```

## 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 vs1 -volume vol1 -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 voll -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 voll -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.



## 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.