



Configurar o SnapLock

ONTAP 9

NetApp
January 08, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/ontap/snaplock/snaplock-config-overview-concept.html> on January 08, 2026. Always check docs.netapp.com for the latest.

Índice

Configurar o SnapLock	1
Saiba mais sobre como configurar o ONTAP SnapLock	1
Inicializar o relógio de conformidade ONTAP	1
Ativar a ressincronização do relógio de conformidade para um sistema configurado por NTP	3
Criar um agregado ONTAP SnapLock	4
Criar e montar volumes ONTAP SnapLock	5
Monte um volume SnapLock	6
Defina o tempo de retenção do ONTAP SnapLock	7
Defina o período de retenção padrão	8
Defina o tempo de retenção de um arquivo explicitamente	10
Defina o período de retenção do arquivo após um evento	11
Crie um log de auditoria protegido ONTAP SnapLock	12
Verificar as configurações do ONTAP SnapLock	14

Configurar o SnapLock

Saiba mais sobre como configurar o ONTAP 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.

Inicializar o relógio de conformidade ONTAP

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 instantâneo 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 instantâneo 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
```

Saiba mais sobre `snaplock compliance-clock initialize` o ["Referência do comando ONTAP"](#) na .

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 ressyncronização do relógio de conformidade para um sistema configurado por NTP

Você pode habilitar o recurso de sincronização do SnapLock Compliance Clock quando um servidor NTP estiver configurado.

Antes de começar

- 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 detecta 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. Habilite o recurso de sincronização do relógio de SnapLock Compliance quando um servidor NTP estiver configurado:

```
snaplock compliance-clock ntp
```

O comando a seguir habilita o recurso de sincronização do relógio de conformidade do sistema:

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
```

Saiba mais sobre `snaplock compliance-clock ntp modify` o ["Referência do comando ONTAP"](#) na .

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 do relógio de conformidade do sistema está habilitado:

```
cluster1::*> snaplock compliance-clock ntp show  
  
Enable clock sync to NTP system time: true
```

Criar um agregado ONTAP 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 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>
```

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
```

Saiba mais sobre `storage aggregate create` o ["Referência do comando ONTAP"](#) na .

Criar e montar volumes ONTAP SnapLock

Você precisa criar um volume SnapLock para os arquivos ou snapshots 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 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.

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>
```

Saiba mais sobre `volume create` o ["Referência do comando ONTAP"](#) na . 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.

Antes de começar

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
```

Saiba mais sobre `volume mount` o ["Referência do comando ONTAP"](#) na .

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 do ONTAP SnapLock

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 há 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.



Em versões anteriores ao ONTAP 9.10.1, se você não definir explicitamente o tempo de retenção antes de confirmar um arquivo no modo de conformidade para o estado WORM e não modificar os valores padrão, o arquivo será retido por 30 anos. Essa alteração *não pode* ser desfeita. Da mesma forma, no ONTAP 9.10.1 e versões posteriores, se você não definir explicitamente o tempo de retenção antes de confirmar um arquivo do modo Enterprise para o estado WORM e não modificar os valores padrão, o arquivo será retido por 0 anos ou, efetivamente, não será retido de forma alguma.

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.

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.

Antes de começar

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	
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. Saiba mais sobre `volume snaplock show` o "[Referência do comando ONTAP](#)" na .



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
```

Saiba mais sobre `volume snaplock modify` o "[Referência do comando ONTAP](#)" na .



Os exemplos a seguir pressupõem que os períodos de retenção mínimo e máximo não foram modificados anteriormente.

O comando a seguir define o período de retenção padrão para um volume de conformidade ou empresa para 20 dias:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period 20days
```

O comando a seguir define o período de retenção padrão para um volume de conformidade para 70 anos:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum  
-retention-period 70years
```

O comando a seguir define o período de retenção padrão para um volume Enterprise para 10 anos:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period max -maximum-retention-period 10years
```

Os comandos a seguir definem o período de retenção padrão para um volume Enterprise para 10 dias:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum  
-retention-period 10days  
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period min
```

O comando a seguir define o período de retenção padrão para um volume de conformidade como infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period infinite -maximum-retention-period infinite
```

Defina o tempo de retenção de um arquivo explicitamente

Você pode definir o tempo de retenção de um arquivo explicitamente modificando seu último tempo de acesso. Você pode usar qualquer comando ou programa adequado em NFS ou CIFS para modificar o último tempo de acesso.

Sobre esta tarefa

Depois que um arquivo foi comprometido com WORM, você pode estender, mas não reduzir o tempo de retenção. O tempo de retenção é armazenado `atime` no campo para o arquivo.



Não é possível definir explicitamente o tempo de retenção de um arquivo como `infinite`. Esse valor só está disponível quando você usa o período de retenção padrão para calcular o tempo de retenção.

Passos

1. Use um comando ou programa adequado para modificar a última hora de acesso para o arquivo cujo tempo de retenção você deseja definir.

Em um shell UNIX, use o seguinte comando para definir um tempo de retenção de 21 de novembro de 2020 6:00 em um arquivo chamado `document.txt`:

```
touch -a -t 202011210600 document.txt
```



Você pode usar qualquer comando ou programa adequado para modificar a última hora de acesso no Windows.

Defina o período de retenção do arquivo após um evento

A partir do ONTAP 9.3, você pode definir quanto tempo um arquivo é retido após um evento ocorrer usando o recurso SnapLock *retenção baseada em eventos (EBR)*.

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

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
```

Informações relacionadas

- ["criação de política de retenção de eventos snaplock"](#)
- ["aplicar retenção de evento snaplock"](#)

Crie um log de auditoria protegido ONTAP SnapLock

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.

Saiba mais sobre `snaplock log file show` e `snaplock log file archive` no ["Referência do comando ONTAP"](#).



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 `logVol1` . 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
```

Saiba mais sobre `snaplock log create` o ["Referência do comando ONTAP"](#) na .

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](#)

Verificar as configurações do ONTAP SnapLock

Use os `volume file fingerprint start` comandos e `volume file fingerprint dump` para visualizar as principais informações sobre arquivos e volumes, incluindo o tipo de arquivo (normal, WORM ou WORM anexado), a data de expiração do volume e assim por diante.

Passos

1. Gerar uma impressão digital de arquivo:

```
volume file fingerprint start -vserver <SVM_name> -file <file_path>
```

```
svm1::> volume file fingerprint start -vserver svm1 -file /vol/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

Informações sobre direitos autorais

Copyright © 2026 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 SOBRESSAIENTES; 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 DOCUMENTOS, 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.