Gestire i file WORM

ONTAP 9

NetApp
May 09, 2024

Sommario

Gestire i file WORM

Gestire i file WORM

È possibile gestire i file WORM nei seguenti modi:

- "Esegui il commit dei file su WORM"
- "Assegnare le copie Snapshot a WORM su una destinazione del vault"
- "Mirroring dei file WORM per il disaster recovery"
- "Conservare i file WORM durante i contenziosi"
- "Eliminare i file WORM"

Esegui il commit dei file su WORM

È possibile eseguire il commit dei file in WORM (write once, Read many) manualmente o automaticamente. È inoltre possibile creare file .WORM appendibili.

Esegui il commit dei file in WORM manualmente

Il commit di un file in WORM viene eseguito manualmente rendendo il file di sola lettura. È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per modificare l'attributo Read-write di un file in sola lettura. È possibile scegliere di eseguire il commit manuale dei file se si desidera garantire che un'applicazione abbia terminato la scrittura su un file in modo che il commit del file non venga eseguito in modo prematuro o che si siano riscontrati problemi di scalabilità per lo scanner di autocommit a causa di un elevato numero di volumi.

Di cosa hai bisogno

- Il file che si desidera assegnare deve risiedere in un volume SnapLock.
- Il file deve essere scrivibile.

A proposito di questa attività

Il volume ComplianceClock Time viene scritto su `ctime` del file quando viene eseguito il comando o il programma. Il tempo di ComplianceClock determina quando è stato raggiunto il tempo di conservazione del file.

Fasi

1. Utilizzare un comando o un programma adatto per modificare l'attributo Read-write di un file in sola lettura.

   In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

   ```
   chmod -w document.txt
   ```

   In una shell Windows, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

```
attrib +r document.txt
```

Esegui il commit dei file automaticamente SU WORM

La funzione di autocommit di SnapLock consente di assegnare automaticamente i file A WORM. La funzionalità di autocommit commit commette un file allo stato WORM su un volume SnapLock se il file non è stato modificato per la durata del periodo di autocommit. La funzione di invio automatico è disattivata per impostazione predefinita.

Di cosa hai bisogno

- I file che si desidera assegnare automaticamente devono risiedere in un volume SnapLock.
- Il volume SnapLock deve essere online.
- Il volume SnapLock deve essere un volume di lettura/scrittura.

> La funzione di autocommit di SnapLock esegue la scansione di tutti i file nel volume e commit un file se soddisfa i requisiti di autocommit. Potrebbe esserci un intervallo di tempo tra il momento in cui il file è pronto per l'autocommit e il momento in cui viene effettivamente salvato dallo scanner di autocommit SnapLock. Tuttavia, il file è ancora protetto dalle modifiche e dall'eliminazione da parte del file system non appena è idoneo per l'autocommit.

A proposito di questa attività

Il *periodo di autocommit* specifica il periodo di tempo in cui i file devono rimanere invariati prima di eseguire l'autocommit. La modifica di un file prima che sia trascorso il periodo di autocommit riavvia il periodo di autocommit per il file.

La seguente tabella mostra i valori possibili per il periodo di autocommit:

Valore	Unità	Note
nessuno	-	L'impostazione predefinita.
5 - 5256000	minuti	-
1 - 87600	ore	-
1 - 3650	giorni	-
1 - 120	mesi	-
1 - 10	anni	-

> Il valore minimo è di 5 minuti e il valore massimo è di 10 anni.

Fasi

1. Commit automatico dei file su un volume SnapLock in WORM:

volume snaplock modify -vserver *SVM_name* -volume *volume_name* -autocommit -period *autocommit_period*

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando esegue il commit automatico dei file sul volume `vol1` Di SVM vs1, a condizione che i file rimangano invariati per 5 ore:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

Creare un file .WORM appendibile

Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. È possibile utilizzare qualsiasi comando o programma adatto per creare un file .WORM appendibile oppure utilizzare la funzione *volume append mode* di SnapLock per creare file .WORM appendibili per impostazione predefinita.

Utilizzare un comando o un programma per creare un file .WORM appendibile

È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per creare un file .WORM appendibile. Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. I dati vengono aggiunti al file in blocchi da 256 KB. Man mano che ogni chunk viene scritto, il chunk precedente diventa protetto DA WORM. Non è possibile eliminare il file finché non è trascorso il periodo di conservazione.

Di cosa hai bisogno

Il file .WORM appendibile deve risiedere su un volume SnapLock.

A proposito di questa attività

I dati non devono essere scritti in sequenza nel blocco attivo da 256 KB. Quando i dati vengono scritti nel byte n×256KB+1 del file, il segmento precedente da 256 KB diventa protetto DA WORM.

Fasi

1. Utilizzare un comando o un programma adatto per creare un file di lunghezza zero con il tempo di conservazione desiderato.

   In una shell UNIX, utilizzare il seguente comando per impostare un tempo di conservazione del 21 novembre 2020 alle 6:00 su un file di lunghezza zero denominato `document.txt`:

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

2. Utilizzare un comando o un programma adatto per modificare l'attributo Read-write del file in sola lettura.

   In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

   ```
   chmod 444 document.txt
   ```

3. Utilizzare un comando o un programma adatto per modificare nuovamente l'attributo Read-write del file in Writable (scrivibile).

   > Questo passaggio non è considerato un rischio di conformità perché non sono presenti dati nel file.

   In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` scrivibile:

   ```
   chmod 777 document.txt
   ```

4. Utilizzare un comando o un programma adatto per iniziare a scrivere i dati nel file.

   In una shell UNIX, utilizzare il seguente comando per scrivere i dati `document.txt`:

   ```
   echo test data >> document.txt
   ```

   > Quando non è più necessario aggiungere dati al file, riportare i permessi del file in sola lettura.

Utilizzare la modalità di aggiunta del volume per creare file .WORM appendibili

A partire da ONTAP 9.3, è possibile utilizzare la funzione SnapLock *volume append mode* (VAM) per creare file .WORM appendibili per impostazione predefinita. Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. I dati vengono aggiunti al file in blocchi da 256 KB. Man mano che ogni chunk viene scritto, il chunk precedente diventa protetto DA WORM. Non è possibile eliminare il file finché non è trascorso il periodo di conservazione.

Di cosa hai bisogno

- Il file .WORM appendibile deve risiedere su un volume SnapLock.
- Il volume SnapLock deve essere smontato e vuoto di copie Snapshot e file creati dall'utente.

A proposito di questa attività

I dati non devono essere scritti in sequenza nel blocco attivo da 256 KB. Quando i dati vengono scritti nel byte n×256KB+1 del file, il segmento precedente da 256 KB diventa protetto DA WORM.

Se si specifica un periodo di autocommit per il volume, i file .WORM che non vengono modificati per un periodo superiore al periodo di autocommit vengono impegnati in WORM.

> VAM non è supportato sui volumi del registro di controllo di SnapLock.

Fasi

1. Attiva VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando attiva la funzione VAM sul volume `vol1` Di SVM`vs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. Utilizzare un comando o un programma adatto per creare file con permessi di scrittura.

   Per impostazione predefinita, i file sono associati A WORM.

Assegnare le copie Snapshot a WORM su una destinazione del vault

È possibile utilizzare SnapLock per SnapVault per proteggere WORM le copie Snapshot sullo storage secondario. Tutte le attività di base di SnapLock vengono eseguite sulla destinazione del vault. Il volume di destinazione viene montato automaticamente in sola lettura, pertanto non è necessario assegnare esplicitamente le copie Snapshot a WORM; pertanto, la creazione di copie Snapshot pianificate sul volume di destinazione utilizzando i criteri SnapMirror non è supportata.

Prima di iniziare

- Il cluster di origine deve eseguire ONTAP 8.2.2 o versione successiva.
- Gli aggregati di origine e destinazione devono essere a 64 bit.
- Il volume di origine non può essere un volume SnapLock.
- I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered.

  Per ulteriori informazioni, vedere "Peering dei cluster".

- Se la funzione di crescita automatica del volume è disattivata, lo spazio libero sul volume di destinazione deve essere superiore di almeno il cinque percento allo spazio utilizzato sul volume di origine.

A proposito di questa attività

Il volume di origine può utilizzare storage NetApp o non NetApp. Per lo storage non NetApp, è necessario utilizzare la virtualizzazione FlexArray.

> Non è possibile rinominare una copia Snapshot che è stata impegnata nello stato WORM.

È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.

> I LUN non sono supportati nei volumi SnapLock. Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

A partire da ONTAP 9.14.1, è possibile specificare i periodi di conservazione per etichette SnapMirror specifiche nella policy di SnapMirror della relazione di SnapMirror, in modo che le copie Snapshot replicate

dall'origine al volume di destinazione vengano conservate per il periodo di conservazione specificato nella regola. Se non viene specificato alcun periodo di conservazione, viene utilizzato il periodo di conservazione predefinito del volume di destinazione.

A partire da ONTAP 9.13.1, è possibile ripristinare istantaneamente una copia Snapshot bloccata sul volume SnapLock di destinazione di una relazione del vault di SnapLock creando un FlexClone con l' `snaplock-type` Opzione impostata su "non snaplock" e specifica la copia Snapshot come "snapshot principale" quando si esegue l'operazione di creazione del clone del volume. Scopri di più "Creazione di un volume FlexClone con un tipo di SnapLock".

Per le configurazioni MetroCluster, è necessario conoscere quanto segue:

- È possibile creare una relazione SnapVault solo tra le SVM di origine della sincronizzazione, non tra una SVM di origine della sincronizzazione e una SVM di destinazione della sincronizzazione.
- È possibile creare una relazione SnapVault da un volume su una SVM di origine della sincronizzazione a una SVM di servizio dati.
- È possibile creare una relazione SnapVault da un volume su una SVM di servizio dati a un volume DP su una SVM di origine sincronizzazione.

L'illustrazione seguente mostra la procedura per l'inizializzazione di una relazione del vault di SnapLock:

Fasi

1. Identificare il cluster di destinazione.
2. Sul cluster di destinazione, "Installare la licenza SnapLock", "Inizializzare l'orologio di conformità", E, se si utilizza una versione di ONTAP precedente alla 9.10.1, "Creazione di un aggregato SnapLock".
3. Nel cluster di destinazione, creare un volume di destinazione SnapLock di tipo `DP` di dimensioni uguali o superiori a quelle del volume di origine:

   volume create -vserver *SVM_name* -volume *volume_name* -aggregate *aggregate_name* -snaplock-type compliance|enterprise -type DP -size *size*

   > A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l'opzione volume -snaplock-type per specificare un tipo di volume Compliance o Enterprise SnapLock. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock, Compliance o Enterprise, viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

   Il seguente comando crea un SnapLock da 2 GB `Compliance` volume denominato `dstvolB` poll `SVM2` sull'aggregato `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

4. Nel cluster di destinazione, impostare il periodo di conservazione predefinito, come descritto in Impostare il periodo di conservazione predefinito.

> A un volume SnapLock che è una destinazione del vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo viene inizialmente impostato su un minimo di 0 anni per i volumi aziendali SnapLock e su un massimo di 30 anni per i volumi di conformità SnapLock. Ogni copia Snapshot di NetApp viene inizialmente impegnata con questo periodo di conservazione predefinito. Il periodo di conservazione può essere esteso in un secondo momento, se necessario. Per ulteriori informazioni, vedere Imposta la panoramica del tempo di conservazione.

5. Creare una nuova relazione di replica Tra l'origine non SnapLock e la nuova destinazione SnapLock creata nel passaggio 3.

   In questo esempio viene creata una nuova relazione di SnapMirror con il volume SnapLock di destinazione `dstvolB` utilizzando una policy di `XDPDefault` Per eseguire il vault delle copie Snapshot etichettate giornalmente e settimanalmente in base a una pianificazione oraria:

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

   > Creare un criterio di replica personalizzato oppure un programma personalizzato se le impostazioni predefinite disponibili non sono adatte.

6. Sulla SVM di destinazione, inizializzare la relazione SnapVault creata nella fase 5:

   `snapmirror initialize -destination-path` *`destination_path`*

   Il seguente comando inizializza la relazione tra il volume di origine `srcvolA` acceso `SVM1` e il volume di destinazione `dstvolB` acceso `SVM2`:

   ```
   cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

7. Una volta inizializzata la relazione e inattiva, utilizzare `snapshot show` Sulla destinazione per verificare il tempo di scadenza SnapLock applicato alle copie Snapshot replicate.

   Questo esempio elenca le copie Snapshot sul volume `dstvolB` Che hanno l'etichetta SnapMirror e la data di scadenza SnapLock:

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
   snapmirror-label, snaplock-expiry-time
   ```

Informazioni correlate

"Peering di cluster e SVM"

"Backup del volume con SnapVault"

Mirroring dei file WORM per il disaster recovery

È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery e altri scopi. Sia il volume di origine che il volume di destinazione devono essere configurati per SnapLock e entrambi i volumi devono avere la stessa modalità SnapLock, Compliance o Enterprise. Vengono replicate tutte le principali proprietà SnapLock del volume e dei file.

Prerequisiti

I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered. Per ulteriori informazioni, vedere "Peering di cluster e SVM".

A proposito di questa attività

- A partire da ONTAP 9.5, è possibile replicare i file WORM con la relazione SnapMirror di tipo XDP (Extended Data Protection) piuttosto che con la relazione di tipo DP (Data Protection). La modalità XDP è indipendente dalla versione di ONTAP ed è in grado di differenziare i file memorizzati nello stesso blocco, semplificando notevolmente la risincronizzazione dei volumi replicati in modalità Compliance. Per informazioni su come convertire una relazione di tipo DP esistente in una relazione di tipo XDP, vedere "Protezione dei dati".
- Un'operazione di risincronizzazione su una relazione SnapMirror di tipo DP non riesce per un volume in modalità di conformità se SnapLock determina che causerà una perdita di dati. Se un'operazione di risincronizzazione non riesce, è possibile utilizzare `volume clone create` per creare un clone del volume di destinazione. È quindi possibile risincronizzare il volume di origine con il clone.
- Una relazione SnapMirror di tipo XDP tra volumi compatibili con SnapLock supporta una risincronizzazione dopo un'interruzione anche se i dati sulla destinazione sono stati diversi dall'origine dopo l'interruzione.

  In una risincronizzazione, quando viene rilevata una divergenza di dati tra l'origine e la destinazione oltre lo snapshot comune, viene tagliata una nuova istantanea sulla destinazione per acquisire questa divergenza. Il nuovo snapshot e lo snapshot comune sono entrambi bloccati con un tempo di conservazione come segue:

  - Il tempo di scadenza del volume della destinazione
  - Se il tempo di scadenza del volume è passato o non è stato impostato, lo snapshot viene bloccato per un periodo di 30 giorni
  - Se la destinazione dispone di conservazione a fini giudiziari, il periodo di scadenza del volume effettivo viene mascherato e visualizzato come 'indefinito', tuttavia lo snapshot viene bloccato per la durata del periodo di scadenza del volume effettivo.

Se il volume di destinazione ha un periodo di scadenza successivo a quello di origine, il periodo di scadenza di destinazione viene mantenuto e non viene sovrascritto dal periodo di scadenza del volume di origine successivo alla risincronizzazione.

Se sulla destinazione sono presenti legal-stive che differiscono dall'origine, non è consentita una risincronizzazione. L'origine e la destinazione devono avere le stesse disposizioni legali o tutte le disposizioni legali sulla destinazione devono essere rilasciate prima di tentare una risincronizzazione.

Una copia Snapshot bloccata sul volume di destinazione creato per acquisire i dati divergenti può essere copiata nell'origine utilizzando la CLI eseguendo `snapmirror update -s snapshot` comando. Una volta copiata, l'istantanea continuerà a essere bloccata anche all'origine.

- Le relazioni di protezione dei dati SVM non sono supportate.

- Le relazioni di protezione dei dati di condivisione del carico non sono supportate.

La seguente illustrazione mostra la procedura per inizializzare una relazione SnapMirror:

System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione di sistema per impostare la replica di SnapMirror dei file WORM.

Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Fare clic su **Mostra/Nascondi** e selezionare **tipo SnapLock** per visualizzare la colonna nella finestra **volumi**.
3. Individuare un volume SnapLock.
4. Fare clic su ⋮ E selezionare **Protect**.
5. Scegliere il cluster di destinazione e la VM di storage di destinazione.
6. Fare clic su **altre opzioni**.
7. Selezionare **Mostra policy legacy** e selezionare **DPDefault (legacy)**.
8. Nella sezione **Destination Configuration details** (Dettagli configurazione destinazione), selezionare **Override transfer schedule** (Ignora pianificazione trasferimento) e selezionare **Hourly** (orario).
9. Fare clic su **Save** (Salva).
10. A sinistra del nome del volume di origine, fare clic sulla freccia per espandere i dettagli del volume, quindi a destra della pagina, esaminare i dettagli della protezione di SnapMirror remoto.
11. Sul cluster remoto, accedere a **Relazioni di protezione**.
12. Individuare la relazione e fare clic sul nome del volume di destinazione per visualizzare i dettagli della relazione.
13. Verificare che il tipo SnapLock del volume di destinazione e altre informazioni SnapLock siano disponibili.

CLI

1. Identificare il cluster di destinazione.
2. Sul cluster di destinazione, "Installare la licenza SnapLock", "Inizializzare l'orologio di conformità", E, se si utilizza una versione di ONTAP precedente alla 9.10.1, "Creazione di un aggregato SnapLock".
3. Nel cluster di destinazione, creare un volume di destinazione SnapLock di tipo `DP` di dimensioni uguali o superiori al volume di origine:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l'opzione volume -snaplock-type per specificare un tipo di volume Compliance o Enterprise SnapLock. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock (Compliance o Enterprise) viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

   Il seguente comando crea un SnapLock da 2 GB `Compliance` volume denominato `dstvolB` poll `SVM2` sull'aggregato `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Sulla SVM di destinazione, creare un criterio SnapMirror:

   snapmirror policy create -vserver *SVM_name* -policy *policy_name*

   Il seguente comando crea il criterio a livello di SVM `SVM1-mirror`:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. Sulla SVM di destinazione, creare una pianificazione SnapMirror:

   job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*

   Il comando seguente crea una pianificazione SnapMirror denominata `weekendcron`:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. Sulla SVM di destinazione, creare una relazione SnapMirror:

   snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*

   Il comando seguente crea una relazione SnapMirror tra il volume di origine `srcvolA` acceso `SVM1` e il volume di destinazione `dstvolB` acceso `SVM2`e assegna il criterio `SVM1-mirror` e il calendario `weekendcron`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   Il tipo di XDP è disponibile in ONTAP 9.5 e versioni successive. È necessario utilizzare il tipo di DP in ONTAP 9.4 e versioni precedenti.

7. Sulla SVM di destinazione, inizializzare la relazione SnapMirror:

   snapmirror initialize -destination-path *destination_path*

   Il processo di inizializzazione esegue un *trasferimento baseline* al volume di destinazione. SnapMirror crea una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. Inoltre, trasferisce al volume di destinazione tutte le altre copie Snapshot presenti nel volume di origine.

Il seguente comando inizializza la relazione tra il volume di origine `srcvolA` acceso `SVM1` e il volume di destinazione `dstvolB` acceso `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Informazioni correlate

"Peering di cluster e SVM"

"Preparazione al disaster recovery dei volumi"

"Protezione dei dati"

Conservare i file WORM durante i contenziosi utilizzando la conservazione a fini legali

A partire da ONTAP 9.3, puoi conservare i file WORM in modalità di conformità per tutta la durata di un contenzioso utilizzando la funzione *conservazione legale*.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.

  "Creare un account amministratore di SnapLock"

- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

A proposito di questa attività

Un file in stato di conservazione legale si comporta come un file WORM con un periodo di conservazione indefinito. È responsabilità dell'utente specificare quando scade il periodo di conservazione legale.

Il numero di file che è possibile inserire in un blocco legale dipende dallo spazio disponibile sul volume.

Fasi

1. Avvio di un blocco legale:

   `snaplock legal-hold begin -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   Il seguente comando avvia un blocco legale per tutti i file in `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Fine di un periodo di conservazione legale:

   `snaplock legal-hold end -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

Il seguente comando termina un blocco legale per tutti i file in `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Panoramica sull'eliminazione dei file WORM

È possibile eliminare i file WORM in modalità Enterprise durante il periodo di conservazione utilizzando la funzione di eliminazione con privilegi. Prima di poter utilizzare questa funzione, è necessario creare un account amministratore di SnapLock e, utilizzando l'account, attivare la funzione.

Creare un account amministratore di SnapLock

Per eseguire un'eliminazione con privilegi, è necessario disporre dei privilegi di amministratore di SnapLock. Questi privilegi sono definiti nel ruolo vsadmin-snaplock. Se non è stato ancora assegnato tale ruolo, è possibile chiedere all'amministratore del cluster di creare un account amministratore SVM con il ruolo di amministratore di SnapLock.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

Fasi

1. Creare un account amministratore SVM con il ruolo di amministratore di SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   Il seguente comando attiva l'account amministratore SVM `SnapLockAdmin` con il predefinito `vsadmin-snaplock` ruolo di accesso `SVM1` utilizzo di una password:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

Attivare la funzione di eliminazione con privilegi

È necessario attivare esplicitamente la funzionalità di eliminazione con privilegi sul volume Enterprise che contiene i file WORM che si desidera eliminare.

A proposito di questa attività

Il valore di `-privileged-delete` l'opzione determina se l'eliminazione con privilegi è attivata. I valori possibili sono `enabled`, `disabled`, e. `permanently-disabled`.

`permanently-disabled` è lo stato del terminale. Non è possibile attivare l'eliminazione con privilegi sul volume dopo aver impostato lo stato su `permanently-disabled`.

Fasi

1. Abilitare l'eliminazione con privilegi per un volume aziendale SnapLock:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   Il comando seguente attiva la funzione di eliminazione con privilegi per il volume Enterprise `dataVol` acceso `SVM1`:

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

Eliminare i file WORM in modalità Enterprise

È possibile utilizzare la funzione di eliminazione con privilegi per eliminare i file WORM in modalità Enterprise durante il periodo di conservazione.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.
- È necessario aver creato un registro di controllo di SnapLock e attivato la funzione di eliminazione con privilegi sul volume aziendale.

A proposito di questa attività

Non è possibile utilizzare un'operazione di eliminazione con privilegi per eliminare un file WORM scaduto. È possibile utilizzare `volume file retention show` Per visualizzare il tempo di conservazione del file WORM che si desidera eliminare. Per ulteriori informazioni, vedere la pagina man del comando.

Fase

1. Eliminare un file WORM su un volume Enterprise:

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   Il seguente comando elimina il file `/vol/dataVol/f1` Su SVM`SVM1`:

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```