Configurare SnapLock

ONTAP 9

NetApp
April 24, 2024

Sommario

Configurare SnapLock

Configurare SnapLock

Prima di utilizzare SnapLock, è necessario configurare SnapLock completando varie attività, ad esempio "Installare la licenza SnapLock" Per ogni nodo che ospita un aggregato con un volume SnapLock, inizializzare l' "Orologio di conformità", Creare un aggregato SnapLock per i cluster che eseguono release ONTAP precedenti a ONTAP 9.10.1, "Creare e montare un volume SnapLock"e molto altro ancora.

Inizializzare il Compliance Clock

SnapLock utilizza *Volume Compliance Clock* per evitare manomissioni che potrebbero alterare il periodo di conservazione dei file WORM. È necessario prima inizializzare il *system ComplianceClock* su ogni nodo che ospita un aggregato SnapLock.

A partire da ONTAP 9.14.1, è possibile inizializzare o reinizializzare il clock di conformità del sistema quando non ci sono volumi SnapLock o nessun volume con il blocco delle copie Snapshot attivato. La possibilità di reinizializzare consente agli amministratori di sistema di reimpostare l'orologio di conformità del sistema nei casi in cui potrebbe essere stato inizializzato in modo errato o di correggere la deriva dell'orologio sul sistema. In ONTAP 9.13.1 e nelle versioni precedenti, una volta inizializzato il Compliance Clock su un nodo, non è possibile inizializzarlo nuovamente.

Prima di iniziare

Per reinizializzare il Compliance Clock:

- Tutti i nodi nel cluster devono essere in stato integro.
- Tutti i volumi devono essere online.
- La coda di ripristino non può contenere volumi.
- Non può essere presente alcun volume SnapLock.
- Non può essere presente alcun volume con il blocco della copia Snapshot abilitato.

Requisiti generali per l'inizializzazione dell'orologio di conformità:

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- "La licenza SnapLock deve essere installata sul nodo".

A proposito di questa attività

L'ora del Compliance Clock del sistema viene ereditata dal *Volume Compliance Clock*, quest'ultimo dei quali controlla il periodo di conservazione dei file WORM sul volume. Il clock di conformità del volume viene inizializzato automaticamente quando si crea un nuovo volume SnapLock.

> L'impostazione iniziale dell'orologio di conformità del sistema si basa sull'orologio di sistema hardware corrente. Per questo motivo, è necessario verificare che l'ora e il fuso orario del sistema siano corretti prima di inizializzare l'orologio di conformità del sistema su ciascun nodo. Una volta inizializzato il clock di conformità del sistema su un nodo, non è possibile inizializzarlo nuovamente quando sono presenti volumi SnapLock o volumi con blocco abilitato.

Fasi

È possibile utilizzare la CLI di ONTAP per inizializzare l'orologio di conformità oppure, a partire da ONTAP 9.12.1, utilizzare Gestione sistema per inizializzare l'orologio di conformità.

System Manager

1. Accedere a **Cluster > Panoramica**.
2. Nella sezione **nodi**, fare clic su **Inizializza clock di conformità SnapLock**.
3. Per visualizzare la colonna **Orologio conformità** e verificare che l'Orologio conformità sia inizializzato, nella sezione **Cluster > Panoramica > nodi**, fare clic su **Mostra/Nascondi** e selezionare **Orologio conformità SnapLock**.

CLI

1. Inizializzare l'orologio di conformità del sistema:

   `snaplock compliance-clock initialize -node` *`node_name`*

   Il seguente comando inizializza il Compliance Clock del sistema su `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. Quando richiesto, confermare che l'orologio di sistema è corretto e che si desidera inizializzare l'orologio di conformità:

   ```
   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. Ripetere questa procedura per ogni nodo che ospita un aggregato SnapLock.

Abilitare la risincronizzazione del clock di conformità per un sistema configurato con NTP

È possibile attivare la funzione di sincronizzazione dell'ora dell'orologio di conformità SnapLock quando è configurato un server NTP.

Di cosa hai bisogno

- Questa funzione è disponibile solo al livello di privilegio avanzato.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

- "La licenza SnapLock deve essere installata sul nodo".
- Questa funzione è disponibile solo per le piattaforme Cloud Volumes ONTAP, ONTAP Select e VSIM.

A proposito di questa attività

Quando il daemon di clock sicuro SnapLock rileva un'inclinazione oltre la soglia, ONTAP utilizza l'ora di sistema per reimpostare sia il sistema che i blocchi di conformità del volume. Come soglia di disallineamento viene impostato un periodo di 24 ore. Ciò significa che l'orologio di conformità del sistema è sincronizzato con l'orologio di sistema solo se l'inclinazione è più vecchia di un giorno.

Il daemon dell'orologio sicuro SnapLock rileva un'inclinazione e modifica l'orologio di conformità all'ora del sistema. Qualsiasi tentativo di modifica dell'ora di sistema per forzare la sincronizzazione dell'orologio di conformità con l'ora di sistema non riesce, poiché l'orologio di conformità si sincronizza con l'ora di sistema solo se l'ora di sistema è sincronizzata con l'ora NTP.

Fasi

1. Attivare la funzione sincronizzazione orologio conformità SnapLock quando è configurato un server NTP:

   `snaplock compliance-clock ntp`

   Il seguente comando abilita la funzione di sincronizzazione dell'ora dell'orologio di conformità del sistema:

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

2. Quando richiesto, verificare che i server NTP configurati siano attendibili e che il canale di comunicazione sia sicuro per abilitare la funzione:
3. Verificare che la funzione sia attivata:

   `snaplock compliance-clock ntp show`

   Il seguente comando verifica che la funzione di sincronizzazione dell'ora del clock di conformità del sistema sia attivata:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Creare un aggregato SnapLock

Il volume viene utilizzato `-snaplock-type` Opzione per specificare un tipo di volume Compliance o Enterprise SnapLock. Per le release precedenti a ONTAP 9.10.1, è necessario creare un aggregato SnapLock separato. 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.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

- Il SnapLock "la licenza deve essere installata" sul nodo. Questa licenza è inclusa in "ONTAP uno".
- "È necessario inizializzare il Compliance Clock sul nodo".
- Se i dischi sono stati partizionati come “root”, “data1” e “data2”, è necessario assicurarsi che siano disponibili dischi di riserva.

Considerazioni sull’upgrade

Quando si esegue l’aggiornamento a ONTAP 9.10.1, gli aggregati SnapLock e non SnapLock esistenti vengono aggiornati per supportare l’esistenza di volumi SnapLock e non SnapLock; tuttavia, gli attributi dei volumi SnapLock esistenti non vengono aggiornati automaticamente. Ad esempio, i campi di compaction dei dati, deduplica di volumi incrociati e deduplica di background di volumi incrociati rimangono invariati. I nuovi volumi SnapLock creati sugli aggregati esistenti hanno gli stessi valori predefiniti dei volumi non SnapLock e i valori predefiniti per i nuovi volumi e aggregati dipendono dalla piattaforma.

Considerazioni sul revert

Se è necessario ripristinare una versione di ONTAP precedente alla 9.10.1, è necessario spostare tutti i volumi SnapLock Compliance, SnapLock Enterprise e SnapLock nei propri aggregati SnapLock.

A proposito di questa attività

- Non è possibile creare aggregati di conformità per le LUN FlexArray, ma gli aggregati di conformità SnapLock sono supportati con le LUN FlexArray.
- Non è possibile creare aggregati di conformità con l’opzione SyncMirror.
- È possibile creare aggregati di conformità mirrorati in una configurazione MetroCluster solo se l’aggregato viene utilizzato per ospitare volumi di log di audit SnapLock.

> In una configurazione MetroCluster, SnapLock Enterprise è supportato su aggregati mirrorati e senza mirror. La conformità SnapLock è supportata solo su aggregati senza mirror.

Fasi

1. Creare un aggregato SnapLock:

   ```
   storage aggregate create -aggregate <aggregate_name> -node <node_name>
   -diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
   ```

   La pagina man del comando contiene un elenco completo di opzioni.

   Il seguente comando crea un SnapLock `Compliance` aggregato con nome `aggr1` con tre dischi su `node1`:

   ```
   cluster1::> storage aggregate create -aggregate aggr1 -node node1
   -diskcount 3 -snaplock-type compliance
   ```

Creare e montare volumi SnapLock

È necessario creare un volume SnapLock per i file o le copie Snapshot che si desidera assegnare allo stato WORM. A partire da ONTAP 9.10.1, qualsiasi volume creato,

indipendentemente dal tipo di aggregato, viene creato per impostazione predefinita come volume non SnapLock. È necessario utilizzare `-snaplock-type` Opzione per creare esplicitamente un volume SnapLock specificando Compliance o Enterprise come tipo SnapLock. Per impostazione predefinita, il tipo di SnapLock è impostato su `non-snaplock`.

Prima di iniziare

- L'aggregato SnapLock deve essere online.
- Dovresti "Verificare che sia installata una licenza SnapLock". Se una licenza SnapLock non è installata sul nodo, è necessario "installare" it. Questa licenza è inclusa con "ONTAP uno". Prima di ONTAP One, la licenza SnapLock era inclusa nel pacchetto sicurezza e conformità. Il bundle Security and Compliance non è più offerto, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo "Eseguire l'aggiornamento a ONTAP One".
- "È necessario inizializzare il Compliance Clock sul nodo".

A proposito di questa attività

Con le autorizzazioni SnapLock appropriate, è possibile distruggere o rinominare un volume Enterprise in qualsiasi momento. Non è possibile distruggere un volume Compliance fino allo scadere del periodo di conservazione. Non è mai possibile rinominare un volume Compliance.

È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock. Il volume clone sarà dello stesso tipo di SnapLock del volume padre.

> 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.

Eseguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per creare un volume SnapLock.

Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi) e fare clic su **Add** (Aggiungi).
2. Nella finestra **Add Volume** (Aggiungi volume), fare clic su **More Options** (altre opzioni).
3. Inserire le informazioni sul nuovo volume, inclusi il nome e le dimensioni del volume.
4. Selezionare **Enable SnapLock** (attiva conformità) e scegliere il tipo di SnapLock, Compliance (conformità) o Enterprise (Azienda).
5. Nella sezione **Auto-commit Files**, selezionare **Modified** e inserire il tempo in cui un file deve rimanere invariato prima che venga automaticamente salvato. Il valore minimo è di 5 minuti e il valore massimo è di 10 anni.
6. Nella sezione **conservazione dei dati**, selezionare il periodo di conservazione minimo e massimo.
7. Selezionare il periodo di conservazione predefinito.
8. Fare clic su **Save** (Salva).
9. Selezionare il nuovo volume nella pagina **Volumes** per verificare le impostazioni SnapLock.

CLI

1. Creare un volume SnapLock:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise>
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando. Le seguenti opzioni non sono disponibili per i volumi SnapLock: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, e. `vmalign`.

   Il seguente comando crea un SnapLock `Compliance` volume denominato `vol1` acceso `aggr1` acceso `vs1`:

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
   -snaplock-type compliance
   ```

Montare un volume SnapLock

È possibile montare un volume SnapLock su un percorso di giunzione nello spazio dei nomi SVM per l'accesso al client NAS.

Di cosa hai bisogno

Il volume SnapLock deve essere online.

A proposito di questa attività

- È possibile montare un volume SnapLock solo sotto la directory principale della SVM.

- Non è possibile montare un volume normale sotto un volume SnapLock.

Fasi

1. Montare un volume SnapLock:

   volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*

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

   Il seguente comando consente di montare un volume SnapLock denominato `vol1` al percorso di giunzione `/sales` in `vs1` spazio dei nomi:

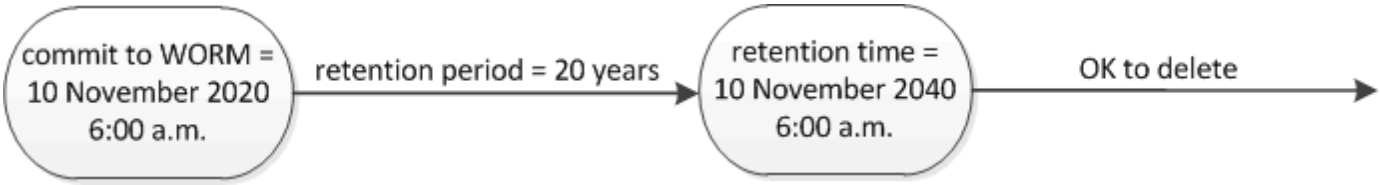
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Impostare il tempo di conservazione

È possibile impostare il tempo di conservazione per un file in modo esplicito oppure utilizzare il periodo di conservazione predefinito per il volume per derivare il tempo di conservazione. A meno che non si definisca esplicitamente il tempo di conservazione, SnapLock utilizza il periodo di conservazione predefinito per calcolare il tempo di conservazione. È inoltre possibile impostare la conservazione dei file dopo un evento.

Informazioni sul periodo di conservazione e sul tempo di conservazione

Il *periodo di conservazione* per un file WORM specifica il periodo di tempo in cui il file deve essere conservato dopo il commit allo stato WORM. Il *tempo di conservazione* per un file WORM è il tempo dopo il quale il file non deve più essere conservato. Un periodo di conservazione di 20 anni per un file impegnato nello stato WORM il 10 novembre 2020 alle 6:00, ad esempio, avrebbe un tempo di conservazione del 10 novembre 2040 alle 6:00



> A partire da ONTAP 9.10.1, è possibile impostare un periodo di conservazione fino al 26 ottobre 3058 e un periodo di conservazione fino a 100 anni. Quando estendi le date di conservazione, le policy precedenti vengono convertite automaticamente. In ONTAP 9.9.1 e versioni precedenti, a meno che il periodo di conservazione predefinito non sia impostato su infinito, il tempo di conservazione massimo supportato è gennaio 19 2071 (GMT).

Considerazioni importanti sulla replica

Quando si stabilisce una relazione di SnapMirror con un volume di origine SnapLock utilizzando una data di conservazione successiva al 19 gennaio 2071 (GMT), il cluster di destinazione deve eseguire ONTAP 9.10.1 o versione successiva, altrimenti il trasferimento di SnapMirror avrà esito negativo.

Considerazioni importanti sul revert

ONTAP impedisce di ripristinare un cluster da ONTAP 9.10.1 a una versione precedente di ONTAP quando sono presenti file con un periodo di conservazione successivo a "19 gennaio 2071 8:44:07".

Comprensione dei periodi di conservazione

Un volume aziendale o di conformità SnapLock prevede quattro periodi di conservazione:

- Periodo minimo di conservazione (`min`), con un valore predefinito pari a 0
- Periodo di conservazione massimo (`max`), con un valore predefinito di 30 anni
- Periodo di conservazione predefinito, con un valore predefinito pari a. `min` Sia per la modalità Compliance che per la modalità Enterprise a partire da ONTAP 9.10.1. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, il periodo di conservazione predefinito dipende dalla modalità:
  - Per la modalità Compliance, l'impostazione predefinita è uguale a. `max`.
  - Per la modalità Enterprise, il valore predefinito è uguale a. `min`.
- Periodo di conservazione non specificato.

  A partire da ONTAP 9.8, è possibile impostare il periodo di conservazione dei file in un volume su `unspecified`, per consentire la conservazione del file fino a quando non si imposta un tempo di conservazione assoluto. È possibile impostare un file con tempo di conservazione assoluto su conservazione non specificata e su conservazione assoluta, a condizione che il nuovo tempo di conservazione assoluto sia successivo al tempo assoluto impostato in precedenza.

  A partire da ONTAP 9.12.1, i file WORM con il periodo di conservazione impostato su `unspecified` È garantito che un periodo di conservazione sia impostato sul periodo di conservazione minimo configurato per il volume SnapLock. Quando si modifica il periodo di conservazione del file da `unspecified` per un tempo di conservazione assoluto, il nuovo tempo di conservazione specificato deve essere maggiore del tempo di conservazione minimo già impostato nel file.

Pertanto, se non si imposta esplicitamente il tempo di conservazione prima di impostare un file in modalità Compliance allo stato WORM e non si modificano le impostazioni predefinite, il file verrà conservato per 30 anni. Allo stesso modo, se non si imposta esplicitamente il tempo di conservazione prima di eseguire il commit di un file in modalità Enterprise allo stato WORM e non si modificano le impostazioni predefinite, il file verrà conservato per 0 anni o, effettivamente, per niente.

Impostare il periodo di conservazione predefinito

È possibile utilizzare `volume snaplock modify` Per impostare il periodo di conservazione predefinito per i file su un volume SnapLock.

Di cosa hai bisogno

Il volume SnapLock deve essere online.

A proposito di questa attività

La tabella seguente mostra i valori possibili per l'opzione periodo di conservazione predefinito:

> Il periodo di conservazione predefinito deve essere maggiore o uguale al (>=) periodo di conservazione minimo e minore o uguale al (⇐) periodo di conservazione massimo.

Valore	Unità	Note
0 - 65535	secondi	

Valore	Unità	Note
0 - 24	ore	
0 - 365	giorni	
0 - 12	mesi	
0 - 100	anni	A partire da ONTAP 9.10.1. Per le release precedenti di ONTAP, il valore è 0 - 70.
max	-	Utilizzare il periodo di conservazione massimo.
min	-	Utilizzare il periodo di conservazione minimo.
infinito	-	Conserva i file per sempre.
non specificato	-	Conservare i file fino a quando non viene impostato un periodo di conservazione assoluto.

I valori e gli intervalli dei periodi di conservazione massimo e minimo sono identici, ad eccezione di `max` e. `min`, che non sono applicabili. Per ulteriori informazioni su questa attività, vedere "Imposta la panoramica del tempo di conservazione".

È possibile utilizzare `volume snaplock show` per visualizzare le impostazioni del periodo di conservazione per il volume. Per ulteriori informazioni, vedere la pagina man del comando.

> Una volta che un file è stato impegnato nello stato WORM, è possibile estendere ma non ridurre il periodo di conservazione.

Fasi

1. Impostare il periodo di conservazione predefinito per i file su un 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
   ```

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

   > Gli esempi seguenti presuppongono che i periodi di conservazione minimo e massimo non siano stati modificati in precedenza.

   Il comando seguente imposta il periodo di conservazione predefinito per un volume Compliance o Enterprise su 20 giorni:

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

Il seguente comando imposta il periodo di conservazione predefinito per un volume Compliance su 70 anni:

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

Il seguente comando imposta il periodo di conservazione predefinito per un volume Enterprise su 10 anni:

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

I seguenti comandi impostano il periodo di conservazione predefinito per un volume Enterprise su 10 giorni:

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

Il comando seguente imposta il periodo di conservazione predefinito per un volume Compliance su infinito:

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

Impostare il tempo di conservazione per un file in modo esplicito

È possibile impostare il tempo di conservazione di un file in modo esplicito modificando l'ultimo tempo di accesso. È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per modificare l'ultimo tempo di accesso.

A proposito di questa attività

Dopo che un file è stato eseguito il commit su WORM, è possibile estendere ma non ridurre il tempo di conservazione. Il tempo di conservazione viene memorizzato in `atime` per il file.

> Non è possibile impostare esplicitamente il tempo di conservazione di un file su `infinite`. Tale valore è disponibile solo quando si utilizza il periodo di conservazione predefinito per calcolare il tempo di conservazione.

Fasi

1. Utilizzare un comando o un programma adatto per modificare l'ultimo orario di accesso al file di cui si desidera impostare il tempo di conservazione.

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

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

   È possibile utilizzare qualsiasi comando o programma adatto per modificare l'ultimo orario di accesso in Windows.

Impostare il periodo di conservazione del file dopo un evento

A partire da ONTAP 9.3, è possibile definire per quanto tempo un file viene conservato dopo un evento utilizzando la funzione di conservazione basata su eventi (EBR)_ di SnapLock.

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

Il *criterio di conservazione degli eventi* definisce il periodo di conservazione del file dopo il verificarsi dell'evento. Il criterio può essere applicato a un singolo file o a tutti i file di una directory.

- Se un file non è UN file WORM, viene impegnato nello stato WORM per il periodo di conservazione definito nella policy.
- Se un file è UN file WORM o un file WORM appendibile, il suo periodo di conservazione verrà esteso dal periodo di conservazione definito nella policy.

È possibile utilizzare un volume Compliance-mode o Enterprise-mode.

I criteri EBR non possono essere applicati ai file in stato di conservazione a scopo legale.

Per informazioni sull'utilizzo avanzato, vedere "Storage WORM conforme con NetApp SnapLock".

utilizzo di EBR per estendere il periodo di conservazione dei file WORM già esistenti

EBR è utile quando si desidera estendere il periodo di conservazione dei file WORM già esistenti. Ad esempio, la politica della tua azienda potrebbe essere quella di conservare i record W-4 del dipendente in forma non modificata per tre anni dopo che il dipendente ha modificato un'elezione di ritenuta. Un'altra policy aziendale potrebbe richiedere la conservazione dei record W-4 per cinque anni dopo la cessazione del dipendente.

In questa situazione, è possibile creare una policy EBR con un periodo di conservazione di cinque anni. Una volta terminato il dipendente (il "evento"), applicherai la policy EBR al record W-4 del dipendente, prolungandone il periodo di conservazione. In genere, questo sarà più semplice dell'estensione manuale del periodo di conservazione, in particolare quando si tratta di un numero elevato di file.

Fasi

1. Creare un criterio EBR:

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   Il seguente comando crea il criterio EBR `employee_exit` acceso `vs1` con un periodo di conservazione di dieci anni:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. Applicare un criterio EBR:

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   Il seguente comando applica il criterio EBR `employee_exit` acceso `vs1` a tutti i file nella directory `d1`:

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Creare un registro di controllo

Se utilizzi ONTAP 9.9.1 o versioni precedenti, devi prima creare un aggregato SnapLock e quindi un audit log protetto da SnapLock prima di eseguire un'eliminazione con privilegi o lo spostamento di un volume SnapLock. Il registro di controllo registra la creazione e l'eliminazione degli account amministratore di SnapLock, le modifiche al volume di log, l'eventuale attivazione dell'eliminazione con privilegi, le operazioni di eliminazione con privilegi e le operazioni di spostamento del volume SnapLock.

A partire da ONTAP 9.10.1, non sarà più possibile creare un aggregato SnapLock. Devi utilizzare l'opzione -snaplock-type per "Creare esplicitamente un volume SnapLock" Specificando conformità o impresa come tipo di SnapLock.

Prima di iniziare

Se utilizzi ONTAP 9.9.1 o versioni precedenti, per creare un aggregato SnapLock devi essere un amministratore del cluster.

A proposito di questa attività

Non è possibile eliminare un registro di controllo fino a quando non è trascorso il periodo di conservazione del file di registro. Non è possibile modificare un registro di controllo anche dopo che è trascorso il periodo di conservazione. Ciò vale sia per la conformità SnapLock che per le modalità aziendali.

> In ONTAP 9.4 e versioni precedenti, non è possibile utilizzare un volume aziendale SnapLock per la registrazione dell'audit. È necessario utilizzare un volume di conformità SnapLock. In ONTAP 9.5 e versioni successive, è possibile utilizzare un volume aziendale SnapLock o un volume di conformità SnapLock per la registrazione dell'audit. In tutti i casi, il volume del log di audit deve essere montato sul percorso di giunzione `/snaplock_audit_log`. Nessun altro volume può utilizzare questo percorso di giunzione.

I registri di controllo di SnapLock sono disponibili in `/snaplock_log` directory sotto la directory principale del volume del registro di controllo, in sottodirectory denominate `privdel_log` (operazioni di eliminazione con privilegi) e. `system_log` (tutto il resto). I nomi dei file di log di audit contengono l'indicazione dell'ora della prima operazione registrata, semplificando la ricerca dei record in base all'ora approssimativa in cui sono state eseguite le operazioni.

- È possibile utilizzare `snaplock log file show` per visualizzare i file di log sul volume del registro di controllo.
- È possibile utilizzare `snaplock log file archive` comando per archiviare il file di log corrente e crearne uno nuovo, utile nei casi in cui è necessario registrare le informazioni del log di audit in un file separato.

Per ulteriori informazioni, consulta le pagine man dei comandi.

> Un volume di protezione dei dati non può essere utilizzato come volume del registro di controllo di SnapLock.

Fasi

1. Creare un aggregato SnapLock.

   Creare un aggregato SnapLock

2. Sulla SVM che si desidera configurare per la registrazione dell'audit, creare un volume SnapLock.

   Creare un volume SnapLock

3. Configurare la SVM per la registrazione dell'audit:

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   -size size -retention-period default_retention_period
   ```

> Il periodo minimo di conservazione predefinito per i file di log di controllo è di sei mesi. Se il periodo di conservazione di un file interessato supera il periodo di conservazione del log di controllo, il periodo di conservazione del log eredita il periodo di conservazione del file. Pertanto, se il periodo di conservazione di un file cancellato mediante eliminazione con privilegi è di 10 mesi e il periodo di conservazione del registro di controllo è di 8 mesi, il periodo di conservazione del registro viene esteso a 10 mesi. Per ulteriori informazioni sul tempo di conservazione e sul periodo di conservazione predefinito, vedere "Impostare il tempo di conservazione".

Il seguente comando viene configurato `SVM1` Per la registrazione dell'audit utilizzando il volume SnapLock `logVol`. Il registro di controllo ha una dimensione massima di 20 GB e viene conservato per otto mesi.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. Sulla SVM configurata per la registrazione dell'audit, montare il volume SnapLock nel percorso di giunzione `/snaplock_audit_log`.

   Montare un volume SnapLock

Verificare le impostazioni SnapLock

È possibile utilizzare `volume file fingerprint start` e. `volume file fingerprint dump` Comandi per visualizzare informazioni chiave su file e volumi, tra cui il tipo di file (normale, WORM o appendice WORM), la data di scadenza del volume e così via.

Fasi

1. Generare un'impronta digitale del file:

   `volume file fingerprint start -vserver` *`SVM_name`* `-file` *`file_path`*

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   Il comando genera un ID sessione che è possibile utilizzare come input per `volume file fingerprint dump` comando.

   > È possibile utilizzare `volume file fingerprint show` Comando con l'ID di sessione per monitorare l'avanzamento dell'operazione di impronte digitali. Assicurarsi che l'operazione sia stata completata prima di provare a visualizzare l'impronta digitale.

2. Visualizzare l'impronta digitale per il file:

volume file fingerprint dump -session-id *session_ID*

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
```

```
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```