



Archiviazione e conformità con la tecnologia SnapLock

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from <https://docs.netapp.com/it-it/ontap/snaplock/index.html> on April 24, 2024.
Always check docs.netapp.com for the latest.

Sommario

- Archiviazione e conformità con la tecnologia SnapLock 1
 - Che cos'è SnapLock 1
 - Configurare SnapLock 6
 - Gestire i file WORM 22
 - Spostare un volume SnapLock 35
 - Bloccare una copia Snapshot per la protezione dagli attacchi ransomware 37
 - API SnapLock 45

Archiviazione e conformità con la tecnologia SnapLock

Che cos'è SnapLock

SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage WORM per conservare i file in forma non modificata a scopo normativo e di governance.

SnapLock aiuta a prevenire l'eliminazione, la modifica o la ridenominazione dei dati per soddisfare normative come SEC 17a-4, HIPAA, FINRA, CFTC e GDPR. Con SnapLock, è possibile creare volumi speciali in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non scrivibile per un determinato periodo di conservazione o a tempo indeterminato. SnapLock consente di eseguire questa conservazione a livello di file attraverso protocolli di file aperti standard come CIFS e NFS. I protocolli di file aperti supportati per SnapLock sono NFS (versioni 2, 3 e 4) e CIFS (SMB 1.0, 2.0 e 3.0).

Utilizzando SnapLock, è possibile assegnare file e copie Snapshot allo storage WORM e impostare periodi di conservazione per i dati protetti DA WORM. Lo storage WORM di SnapLock utilizza la tecnologia Snapshot di NetApp e può sfruttare la replica SnapMirror e i backup SnapVault come tecnologia di base per fornire la protezione del backup recovery per i dati. Scopri di più sullo storage WORM: ["Storage WORM conforme con NetApp SnapLock - TR-4526"](#).

È possibile utilizzare un'applicazione per il commit dei file in WORM su NFS o CIFS oppure utilizzare la funzione di autocommit di SnapLock per il commit automatico dei file IN WORM. È possibile utilizzare un *file .WORM_appendibile* per conservare i dati scritti in modo incrementale, ad esempio le informazioni di log. Per ulteriori informazioni, vedere ["Utilizzare la modalità di aggiunta del volume per creare file .WORM appendibili"](#).

SnapLock supporta metodi di protezione dei dati che devono soddisfare la maggior parte dei requisiti di conformità:

- È possibile utilizzare SnapLock per SnapVault per proteggere WORM le copie Snapshot sullo storage secondario. Vedere ["Assegnare le copie Snapshot a WORM"](#).
- È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery. Vedere ["Mirrorare i file WORM"](#).

SnapLock è una funzionalità basata su licenza di NetApp ONTAP. Una singola licenza consente di utilizzare SnapLock in modalità di conformità rigorosa, per soddisfare mandati esterni come la norma SEC 17a-4 e una modalità aziendale più allentata, per soddisfare le normative interne per la protezione delle risorse digitali. Le licenze SnapLock fanno parte di ["ONTAP uno"](#) suite software.

SnapLock è supportato su tutti i sistemi AFF e FAS e su ONTAP Select. SnapLock non è una soluzione solo software, ma è una soluzione hardware e software integrata. Questa distinzione è importante per le rigide normative WORM come SEC 17a-4, che richiede una soluzione hardware e software integrata. Per ulteriori informazioni, fare riferimento a ["SEC interpretation: Archiviazione elettronica dei record dei broker-dealer"](#).

Cosa puoi fare con SnapLock

Dopo aver configurato SnapLock, è possibile completare le seguenti attività:

- ["Esegui il commit dei file su WORM"](#)
- ["Assegnare copie Snapshot a WORM per lo storage secondario"](#)

- "Mirroring dei file WORM per il disaster recovery"
- "Conservare i file WORM durante i contenziosi utilizzando la conservazione a fini legali"
- "Eliminare i file WORM utilizzando la funzione di eliminazione con privilegi"
- "Impostare il periodo di conservazione del file"
- "Spostare un volume SnapLock"
- "Bloccare una copia Snapshot per la protezione dagli attacchi ransomware"
- "Esaminare l'utilizzo di SnapLock con il registro di controllo"
- "Utilizzare le API di SnapLock"

Conformità SnapLock e modalità aziendali

La conformità SnapLock e le modalità aziendali differiscono principalmente per il livello di protezione dei file WORM in ciascuna modalità:

Modalità SnapLock	Livello di protezione	Eliminazione del file WORM durante la conservazione
Modalità compliance	A livello di file	Impossibile eliminare
Modalità Enterprise	A livello di disco	Può essere eliminato dall'amministratore della compliance utilizzando una procedura controllata di "eliminazione con privilegi"

Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari. Una volta che un file è stato salvato in WORM, sia in modalità Compliance che Enterprise, non può essere modificato, anche dopo che il periodo di conservazione è scaduto.

Non è possibile spostare un file WORM durante o dopo il periodo di conservazione. È possibile copiare un file WORM, ma la copia non conserverà le sue caratteristiche WORM.

La seguente tabella mostra le differenze nelle funzionalità supportate dalle modalità di conformità SnapLock e Enterprise:

Funzionalità	Conformità SnapLock	Azienda SnapLock
Abilitare ed eliminare i file utilizzando l'opzione di eliminazione con privilegi	No	Sì
Reinizializzare i dischi	No	Sì
Distruggere gli aggregati e i volumi SnapLock durante il periodo di conservazione	No	Sì, ad eccezione del volume del registro di controllo di SnapLock
Rinominare aggregati o volumi	No	Sì

Utilizzare dischi non NetApp	No	Sì (con "Virtualizzazione FlexArray")
Utilizzare il volume SnapLock per la registrazione dell'audit	Sì	Sì, a partire da ONTAP 9.5

Funzioni supportate e non supportate con SnapLock

La seguente tabella mostra le funzionalità supportate dalla modalità di conformità SnapLock, dalla modalità aziendale SnapLock o da entrambe:

Funzione	Supportato con conformità SnapLock	Supportato con SnapLock Enterprise
Gruppi di coerenza	No	No
Volumi crittografati	Sì, a partire da ONTAP 9.2. Scopri di più Encryption e SnapLock .	Sì, a partire da ONTAP 9.2. Scopri di più Encryption e SnapLock .
FabricPools su aggregati SnapLock	No	Sì, a partire da ONTAP 9.8. Scopri di più FabricPool su aggregati aziendali SnapLock .
Aggregati di Flash Pool	Sì, a partire da ONTAP 9.1.	Sì, a partire da ONTAP 9.1.
FlexClone	È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.	È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.
Volumi FlexGroup	Sì, a partire da ONTAP 9.11.1. Scopri di più [flexgroup] .	Sì, a partire da ONTAP 9.11.1. Scopri di più [flexgroup] .
LUN	No Scopri di più Supporto del LUN Con SnapLock .	No Scopri di più Supporto del LUN Con SnapLock .
Configurazioni MetroCluster	Sì, a partire da ONTAP 9.3. Scopri di più Supporto MetroCluster .	Sì, a partire da ONTAP 9.3. Scopri di più Supporto MetroCluster .
Verifica multi-admin (MAV)	Sì, a partire da ONTAP 9.13.1. Scopri di più Supporto MAV .	Sì, a partire da ONTAP 9.13.1. Scopri di più Supporto MAV .
SAN	No	No
SnapRestore a file singolo	No	Sì
Continuità aziendale di SnapMirror	No	No

SnapRestore	No	Sì
SMTape	No	No
SnapMirror sincrono	No	No
SSD	Sì, a partire da ONTAP 9.1.	Sì, a partire da ONTAP 9.1.
Funzionalità per l'efficienza dello storage	Sì, a partire da ONTAP 9.9.1. Scopri di più supporto per l'efficienza dello storage .	Sì, a partire da ONTAP 9.9.1. Scopri di più supporto per l'efficienza dello storage .

FabricPool su aggregati aziendali SnapLock

FabricPool sono supportati negli aggregati aziendali di SnapLock a partire da ONTAP 9.8. Tuttavia, il tuo account team deve aprire una richiesta di variazione del prodotto che documenta che sei consapevole del fatto che i dati FabricPool su più livelli di un cloud pubblico o privato non sono più protetti da SnapLock perché un amministratore del cloud può eliminare tali dati.



Tutti i dati che FabricPool esegue il Tier in un cloud pubblico o privato non sono più protetti da SnapLock perché tali dati possono essere cancellati da un amministratore del cloud.

Volumi FlexGroup

SnapLock supporta i volumi FlexGroup a partire da ONTAP 9.11.1; tuttavia, le seguenti funzionalità non sono supportate:

- Conservazione a fini giudiziari
- Conservazione basata sugli eventi
- SnapLock per SnapVault (supportato a partire da ONTAP 9.12.1)

È inoltre necessario conoscere i seguenti comportamenti:

- Il clock di compliance del volume (VCC) di un volume FlexGroup è determinato dal VCC del costituente root. Tutti i componenti non root avranno il proprio VCC strettamente sincronizzato con il VCC root.
- Le proprietà di configurazione di SnapLock sono impostate solo su FlexGroup nel suo complesso. I singoli componenti non possono avere proprietà di configurazione diverse, come il tempo di conservazione predefinito e il periodo di autocommit.

Supporto del LUN

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.

Supporto MetroCluster

Il supporto SnapLock nelle configurazioni MetroCluster varia tra la modalità di conformità SnapLock e la modalità aziendale SnapLock.

Conformità SnapLock

- A partire da ONTAP 9.3, la conformità SnapLock è supportata su aggregati MetroCluster senza mirror.
- A partire da ONTAP 9.3, la conformità SnapLock è supportata sugli aggregati mirrorati, ma solo se l'aggregato viene utilizzato per ospitare i volumi del registro di controllo SnapLock.
- Le configurazioni SnapLock specifiche di SVM possono essere replicate su siti primari e secondari utilizzando MetroCluster.

Azienda SnapLock

- A partire da ONTAP 9, sono supportati gli aggregati aziendali di SnapLock.
- A partire da ONTAP 9.3, sono supportati gli aggregati aziendali SnapLock con eliminazione con privilegi.
- Le configurazioni SnapLock specifiche di SVM possono essere replicate in entrambi i siti utilizzando MetroCluster.

Configurazioni MetroCluster e orologi per la compliance

Le configurazioni MetroCluster utilizzano due meccanismi di clock di compliance, il clock di compliance del volume (VCC) e il clock di compliance del sistema (SCC). VCC e SCC sono disponibili per tutte le configurazioni SnapLock. Quando si crea un nuovo volume su un nodo, il relativo VCC viene inizializzato con il valore corrente di SCC su quel nodo. Una volta creato il volume, il tempo di conservazione del volume e del file viene sempre monitorato con il VCC.

Quando un volume viene replicato in un altro sito, viene replicato anche il relativo VCC. Quando si verifica uno switchover del volume, ad esempio dal sito A al sito B, il VCC continua ad essere aggiornato sul sito B mentre il SCC sul sito A si arresta quando il sito A passa alla modalità offline.

Quando il sito A viene riportato in linea e viene eseguito il switchback del volume, il clock SCC del sito A viene riavviato mentre il VCC del volume continua ad essere aggiornato. Poiché il VCC viene costantemente aggiornato, indipendentemente dalle operazioni di switchover e switchback, i tempi di conservazione dei file non dipendono dai clock SCC e non si allungano.

Supporto MAV (Multi-admin Ververifica)

A partire da ONTAP 9.13.1, un amministratore del cluster può abilitare esplicitamente la verifica multi-admin su un cluster per richiedere l'approvazione del quorum prima che vengano eseguite alcune operazioni SnapLock. Quando MAV è attivato, le proprietà del volume SnapLock come default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period e Privileged-delete richiedono l'approvazione del quorum. Scopri di più ["MAV"](#).

Efficienza dello storage

A partire da ONTAP 9.9.1, SnapLock supporta funzionalità di efficienza dello storage, come la compattazione dei dati, la deduplica tra volumi e la compressione adattiva per volumi e aggregati SnapLock. Per ulteriori informazioni sull'efficienza dello storage, vedere ["Panoramica sulla gestione dello storage logico con la CLI"](#).

Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non

possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

Disclaimer: NetApp non può garantire che i file WORM protetti da SnapLock su dischi o volumi con crittografia automatica possano essere recuperati se la chiave di autenticazione viene persa o se il numero di tentativi di autenticazione non riusciti supera il limite specificato e il disco viene bloccato in modo permanente. È responsabilità dell'utente garantire la protezione dagli errori di autenticazione.



A partire da ONTAP 9.2, i volumi crittografati sono supportati negli aggregati SnapLock.

Transizione 7-Mode

È possibile migrare i volumi SnapLock da 7-Mode a ONTAP utilizzando la funzione CBT (Copy-Based Transition) dello strumento di transizione 7-Mode. La modalità SnapLock del volume di destinazione, Compliance o Enterprise, deve corrispondere alla modalità SnapLock del volume di origine. Non è possibile utilizzare la transizione senza copia (CFT) per migrare i volumi SnapLock.

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 iniziarlo 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 (\geq) periodo di conservazione minimo e minore o uguale al (\leq) 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 voll -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 `logVol1`. 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
```

```
svml1::> volume file fingerprint start -vserver svml -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
```

```
svml1::> volume file fingerprint dump -session-id 33619976
Vserver:svml
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

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 $n \times 256KB + 1$ 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 $n \times 256KB + 1$ 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 `SVMvs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume voll -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 per cento 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 SVMsVM1:

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

Spostare un volume SnapLock

A partire da ONTAP 9.8, è possibile spostare un volume SnapLock in un aggregato di destinazione dello stesso tipo, da Enterprise a Enterprise o Compliance a Compliance.

Per spostare un volume SnapLock, è necessario assegnare il ruolo di protezione SnapLock.

Creare un account amministratore di sicurezza SnapLock

Per eseguire lo spostamento di un volume SnapLock, è necessario disporre dei privilegi di amministratore della sicurezza di SnapLock. Questo privilegio viene concesso con il ruolo *SnapLock*, introdotto in ONTAP 9.8. Se non è stato ancora assegnato tale ruolo, è possibile chiedere all'amministratore del cluster di creare un utente di protezione SnapLock con questo ruolo di protezione 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).

A proposito di questa attività

Il ruolo SnapLock è associato alla SVM amministrativa, a differenza del ruolo vsadmin-snaplock, associato alla SVM dei dati.

Fase

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 snaplock Ruolo per accedere a SVM di amministrazione cluster1 utilizzo di una password:

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

Spostare un volume SnapLock

È possibile utilizzare `volume move` Comando per spostare un volume SnapLock in un aggregato di destinazione.

Di cosa hai bisogno

- È necessario aver creato un registro di controllo protetto da SnapLock prima di eseguire lo spostamento del volume SnapLock.

["Creare un registro di controllo".](#)

- Se si utilizza una versione di ONTAP precedente a ONTAP 9.10.1, l'aggregato di destinazione deve essere dello stesso tipo di SnapLock del volume SnapLock che si desidera spostare, ovvero Compliance to Compliance o Enterprise to Enterprise. A partire da ONTAP 9.10.1, questa restrizione viene rimossa e un aggregato può includere volumi Compliance e Enterprise SnapLock, oltre a volumi non SnapLock.
- Devi essere un utente con il ruolo di sicurezza SnapLock.

Fasi

1. Utilizzando una connessione sicura, accedere alla LIF di gestione del cluster di ONTAP:

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Spostamento di un volume SnapLock:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination  
-aggregate destination_aggregate_name
```

3. Controllare lo stato dell'operazione di spostamento del volume:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

Bloccare una copia Snapshot per la protezione dagli attacchi ransomware

A partire da ONTAP 9.12.1, è possibile bloccare una copia Snapshot su un volume non SnapLock per fornire protezione dagli attacchi ransomware. Il blocco delle copie Snapshot garantisce che non possano essere eliminate accidentalmente o in modo illecito.

La funzione clock di conformità SnapLock consente di bloccare le copie Snapshot per un periodo specificato in modo che non possano essere eliminate fino al raggiungimento dell'ora di scadenza. Il blocco delle copie Snapshot le rende a prova di manomissione, proteggendole dalle minacce ransomware. È possibile utilizzare le copie Snapshot bloccate per ripristinare i dati se un volume viene compromesso da un attacco ransomware.

A partire da ONTAP 9.14.1, il blocco delle copie Snapshot supporta la conservazione a lungo termine delle copie Snapshot sulle destinazioni del vault SnapLock e su volumi di destinazione SnapMirror non SnapLock. Il blocco della copia Snapshot viene attivato impostando il periodo di conservazione utilizzando le regole dei criteri di SnapMirror associate a un [etichetta criterio esistente](#). La regola ha la priorità sul periodo di conservazione predefinito impostato sul volume. Se non esiste un periodo di conservazione associato all'etichetta SnapMirror, viene utilizzato il periodo di conservazione predefinito del volume.

Requisiti e considerazioni sulle copie Snapshot a prova di manomissione

- Se si utilizza l'interfaccia utente di ONTAP, tutti i nodi del cluster devono eseguire ONTAP 9.12.1 o versione successiva. Se si utilizza Gestore di sistema, tutti i nodi devono eseguire ONTAP 9.13.1 o versione successiva.
- ["La licenza SnapLock deve essere installata sul cluster"](#). Questa licenza è inclusa in ["ONTAP uno"](#).
- ["È necessario inizializzare il clock di conformità sul cluster"](#).
- Quando il blocco Snapshot è attivato su un volume, è possibile aggiornare i cluster a una versione di ONTAP successiva a ONTAP 9.12.1; Tuttavia, non è possibile ripristinare una versione precedente di ONTAP fino a quando tutte le copie Snapshot bloccate non hanno raggiunto la data di scadenza e non vengono eliminate e il blocco delle copie Snapshot non viene disattivato.
- Quando un'istantanea è bloccata, il tempo di scadenza del volume viene impostato sul tempo di scadenza della copia Snapshot. Se più di una copia Snapshot è bloccata, il tempo di scadenza del volume riflette il tempo di scadenza maggiore tra tutte le copie Snapshot.
- Il periodo di conservazione per le copie Snapshot bloccate ha la precedenza sul conteggio copie Snapshot, il che significa che il limite di conservazione non viene rispettato se il periodo di conservazione

delle copie Snapshot bloccate non è scaduto.

- In una relazione SnapMirror, è possibile impostare un periodo di conservazione su una regola dei criteri del vault mirror e il periodo di conservazione viene applicato alle copie Snapshot replicate sulla destinazione se il volume di destinazione ha attivato il blocco delle copie Snapshot. Il periodo di conservazione ha la precedenza sul numero di conservazione; ad esempio, le copie Snapshot che non hanno superato la scadenza verranno conservate anche se il numero di conservazione viene superato.
- È possibile rinominare una copia Snapshot su un volume non SnapLock. Le operazioni di ridenominazione di Snapshot sul volume primario di una relazione SnapMirror si riflettono sul volume secondario solo se il criterio è MirrorAllSnapshots. Per gli altri tipi di policy, la copia Snapshot rinominata non viene propagata durante gli aggiornamenti.
- Se si utilizza l'interfaccia utente di ONTAP, è possibile ripristinare una copia Snapshot bloccata con `volume snapshot restore`. Solo se la copia Snapshot bloccata è la più recente. Se sono presenti copie Snapshot non scadute dopo quella da ripristinare, l'operazione di ripristino della copia Snapshot non riesce.

Funzionalità supportate con copie Snapshot antimanomissione

- Volumi FlexGroup

Il blocco delle copie Snapshot è supportato sui volumi FlexGroup. Il blocco di Snapshot si verifica solo sulla copia Snapshot del componente principale. L'eliminazione del volume FlexGroup è consentita solo se è trascorso il tempo di scadenza del costituente root.

- Conversione da FlexVol a FlexGroup

È possibile convertire un volume FlexVol con copie Snapshot bloccate in un volume FlexGroup. Le copie Snapshot rimangono bloccate dopo la conversione.

- Clone del volume e clone del file

È possibile creare cloni di volume e file da una copia Snapshot bloccata.

Funzionalità non supportate

Le seguenti funzioni attualmente non sono supportate con le copie Snapshot antimanomissione:

- Cloud Volumes ONTAP
- Gruppi di coerenza
- FabricPool
- Volumi FlexCache
- SMtape
- Continuità aziendale SnapMirror (SM-BC)
- Regole di policy di SnapMirror che utilizzano `-schedule` parametro
- SnapMirror sincrono
- Mobilità dei dati delle SVM (utilizzata per la migrazione o il trasferimento di una SVM da un cluster di origine a un cluster di destinazione)

Attiva il blocco delle copie Snapshot durante la creazione di un volume

A partire da ONTAP 9.12.1, è possibile attivare il blocco delle copie Snapshot quando si crea un nuovo volume

o quando si modifica un volume esistente utilizzando `-snapshot-locking-enabled` con `volume create` e `volume modify` Comandi nella CLI. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per attivare il blocco delle copie Snapshot.

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare **Add** (Aggiungi).
2. Nella finestra **Add Volume** (Aggiungi volume), selezionare **More Options** (altre opzioni).
3. Immettere il nome del volume, le dimensioni, la policy di esportazione e il nome della condivisione.
4. Selezionare **Enable Snapshot Locking** (attiva blocco snapshot). Questa selezione non viene visualizzata se la licenza SnapLock non è installata.
5. Se non è già abilitato, selezionare **Inizializza orologio conformità SnapLock**.
6. Salvare le modifiche.
7. Nella finestra **Volumes** (volumi), selezionare il volume aggiornato e scegliere **Overview** (Panoramica).
8. Verificare che **blocco copia snapshot SnapLock** sia visualizzato come **abilitato**.

CLI

1. Per creare un nuovo volume e attivare il blocco delle copie Snapshot, immettere il seguente comando:

```
volume create -vserver vs1 -volume vol1 -snapshot-locking-enabled true
```


Il comando seguente attiva il blocco delle copie Snapshot su un nuovo volume denominato vol1:

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot-locking-enabled true
Warning: Snapshot copy locking is being enabled on volume "vol1" in Vserver "vs1". It cannot be disabled until all locked Snapshot copies are past their expiry time. A volume with unexpired locked Snapshot copies cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

Attiva il blocco delle copie Snapshot su un volume esistente

A partire da ONTAP 9.12.1, è possibile attivare il blocco delle copie Snapshot su un volume esistente utilizzando l'interfaccia utente di ONTAP. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per attivare il blocco delle copie Snapshot su un volume esistente.

System Manager

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Selezionare  E scegliere **Modifica > Volume**.
3. Nella finestra **Edit Volume** (Modifica volume), individuare la sezione Snapshot Copies (Local) Settings (Impostazioni snapshot Copies (locali)) e selezionare **Enable Snapshot Locking** (attiva blocco snapshot).

Questa selezione non viene visualizzata se la licenza SnapLock non è installata.

4. Se non è già abilitato, selezionare **Inizializza orologio conformità SnapLock**.
5. Salvare le modifiche.
6. Nella finestra **Volumes** (volumi), selezionare il volume aggiornato e scegliere **Overview** (Panoramica).
7. Verificare che **blocco copia snapshot SnapLock** sia visualizzato come **abilitato**.

CLI

1. Per modificare un volume esistente per attivare il blocco delle copie Snapshot, immettere il seguente comando:

```
volume modify -vserver vservice_name -volume volume_name -snapshot-locking
-enabled true
```

Creare una policy di copia Snapshot bloccata e applicare la conservazione

A partire da ONTAP 9.12.1, è possibile creare criteri di copia Snapshot per applicare un periodo di conservazione delle copie Snapshot e applicare il criterio a un volume per bloccare le copie Snapshot per il periodo specificato. È inoltre possibile bloccare una copia Snapshot impostando manualmente un periodo di conservazione. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per creare policy di blocco delle copie Snapshot e applicarle a un volume.

Creare un criterio di blocco delle copie Snapshot

System Manager

1. Accedere a **Storage > Storage VM** e selezionare una storage VM.
2. Selezionare **Impostazioni**.
3. Individuare **Snapshot Policies** e selezionare ➔.
4. Nella finestra **Add Snapshot Policy**, inserire il nome del criterio.
5. Selezionare **+ Add**.
6. Fornire i dettagli della pianificazione della copia Snapshot, inclusi il nome della pianificazione, il numero massimo di copie Snapshot da conservare e il periodo di conservazione SnapLock.
7. Nella colonna **SnapLock Retention Period**, immettere il numero di ore, giorni, mesi o anni per conservare le copie Snapshot. Ad esempio, un criterio di copia Snapshot con un periodo di conservazione di 5 giorni blocca una copia Snapshot per 5 giorni dal momento della creazione e non può essere eliminata durante tale periodo. Sono supportati i seguenti intervalli di periodi di conservazione:
 - Anni: 0 - 100
 - Mesi: 0 - 1200
 - Giorni: 0 - 36500
 - Orario: 0 - 24
8. Salvare le modifiche.

CLI

1. Per creare un criterio di copia Snapshot, immettere il seguente comando:

```
volume snapshot policy create -policy policy_name -enabled true -schedule1  
schedule1_name -count1 maximum_Snapshot_copies -retention-period1  
_retention_period
```


Il seguente comando crea un criterio di blocco delle copie Snapshot:

```
cluster1> volume snapshot policy create -policy policy_name -enabled  
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

Una copia Snapshot non viene sostituita se è in stato di conservazione attivo; in altri termini, il conteggio delle trattenute non viene rispettato se sono presenti copie Snapshot bloccate che non sono ancora scadute.

Applicare un criterio di blocco a un volume

System Manager

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Selezionare  E scegliere **Modifica > Volume**.
3. Nella finestra **Edit Volume** (Modifica volume), selezionare **Schedule Snapshot Copies** (Pianifica copie Snapshot).
4. Selezionare il criterio di copia Snapshot di blocco dall'elenco.
5. Se il blocco della copia Snapshot non è già attivato, selezionare **Enable Snapshot Locking** (attiva blocco Snapshot).
6. Salvare le modifiche.

CLI

1. Per applicare un criterio di blocco delle copie Snapshot a un volume esistente, immettere il seguente comando:

```
volume modify -volume volume_name -vserver vserver_name -snapshot-policy policy_name
```

Applica il periodo di conservazione durante la creazione manuale della copia Snapshot

È possibile applicare un periodo di conservazione delle copie Snapshot quando si crea manualmente una copia Snapshot. Il blocco della copia Snapshot deve essere attivato sul volume, altrimenti l'impostazione del periodo di conservazione viene ignorata.

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare un volume.
2. Nella pagina dei dettagli del volume, selezionare la scheda **copie Snapshot**.
3. Selezionare **+ Add**.
4. Inserire il nome della copia Snapshot e la data di scadenza del SnapLock. È possibile selezionare il calendario per scegliere la data e l'ora di scadenza della conservazione.
5. Salvare le modifiche.
6. Nella pagina **volumi > copie Snapshot**, selezionare **Mostra/Nascondi** e scegliere **ora scadenza SnapLock** per visualizzare la colonna **ora scadenza SnapLock** e verificare che il tempo di conservazione sia impostato.

CLI

1. Per creare manualmente una copia Snapshot e applicare un periodo di conservazione a blocchi, immettere il seguente comando:

```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name
-snaplock-expiry-time expiration_date_time
```

Il seguente comando crea una nuova copia Snapshot e imposta il periodo di conservazione:

```
cluster1> volume snapshot create -vserver vs1 -volume voll -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

Applicare il periodo di conservazione a una copia Snapshot esistente

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare un volume.
2. Nella pagina dei dettagli del volume, selezionare la scheda **copie Snapshot**.
3. Selezionare la copia Snapshot, quindi **E** scegliere **Modify SnapLock Expiration Time** (Modifica ora di scadenza protocollo). È possibile selezionare il calendario per scegliere la data e l'ora di scadenza della conservazione.
4. Salvare le modifiche.
5. Nella pagina **volumi > copie Snapshot**, selezionare **Mostra/Nascondi** e scegliere **ora scadenza SnapLock** per visualizzare la colonna **ora scadenza SnapLock** e verificare che il tempo di conservazione sia impostato.

CLI

1. Per applicare manualmente un periodo di conservazione a una copia Snapshot esistente, immettere il seguente comando:

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

Nell'esempio seguente viene applicato un periodo di conservazione a una copia Snapshot esistente:

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1  
-snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

Modifica di un criterio esistente per applicare la conservazione a lungo termine

A partire da ONTAP 9.14.1, è possibile modificare una policy SnapMirror esistente aggiungendo una regola per impostare la conservazione a lungo termine delle copie Snapshot. La regola viene utilizzata per ignorare il periodo di conservazione dei volumi predefinito sulle destinazioni del vault SnapLock e sui volumi di destinazione non SnapLock SnapMirror.

1. Aggiunta di una regola a una policy SnapMirror esistente:

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name>  
-snapmirror-label <label name> -keep <number of Snapshot copies> -retention  
-period [<integer> days|months|years]
```

Nell'esempio seguente viene creata una regola che applica un periodo di conservazione di 6 mesi al criterio esistente denominato "lockvault":

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror  
-label test1 -keep 10 -retention-period "6 months"
```

API SnapLock

È possibile utilizzare le API Zephyr per l'integrazione con la funzionalità SnapLock negli script o nell'automazione del workflow. Le API utilizzano la messaggistica XML su HTTP, HTTPS e Windows DCE/RPC. Per ulteriori informazioni, vedere ["Documentazione sull'automazione ONTAP"](#).

file-fingerprint-abortire

Interrompere un'operazione di impronta digitale del file.

file-fingerprint-dump

Visualizzare le informazioni sull'impronta digitale del file.

file-fingerprint-get-iter

Visualizza lo stato delle operazioni di impronte digitali del file.

file-fingerprint-start

Generare un'impronta digitale del file.

snaplock-archive-vserver-log

Archiviare il file di log di audit attivo.

snaplock-create-vserver-log

Creare una configurazione del registro di controllo per una SVM.

snaplock-delete-vserver-log

Eliminare una configurazione del registro di controllo per una SVM.

snaplock-file-privileged-delete

Eseguire un'operazione di eliminazione con privilegi.

snaplock-get-file-retention

Ottenere il periodo di conservazione di un file.

snaplock-get-node-compliance-clock

Ottenere la data e l'ora del nodo ComplianceClock.

snaplock-get-vserver-active-log-files-iter

Visualizza lo stato dei file di log attivi.

snaplock-get-vserver-log-iter

Visualizzare la configurazione del registro di controllo.

snaplock-modify-vserver-log

Modificare la configurazione del registro di controllo per una SVM.

snaplock-set-file-retention

Impostare il tempo di conservazione di un file.

snaplock-set-node-compliance-clock

Impostare la data e l'ora del nodo ComplianceClock.

snaplock-volume-set-privileged-delete

Impostare l'opzione Privileged-delete su un volume aziendale SnapLock.

volume-get-snaplock-attrs

Ottenere gli attributi di un volume SnapLock.

volume-set-snaplock-attrs

Impostare gli attributi di un volume SnapLock.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.