



Replica del volume SnapMirror

ONTAP 9

NetApp
April 24, 2024

Sommario

- Replica del volume SnapMirror 1
 - Nozioni di base sul disaster recovery asincrono di SnapMirror 1
 - Nozioni di base sul disaster recovery sincrono di SnapMirror 3
 - Informazioni sui carichi di lavoro supportati dalle policy di StrictSync e Sync 8
 - Archiviazione del vault con la tecnologia SnapMirror 8
 - Nozioni di base sulla replica unificata di SnapMirror 10
 - XDP sostituisce DP come impostazione predefinita di SnapMirror 12
 - Quando un volume di destinazione cresce automaticamente 14
 - Implementazioni di protezione dei dati fan-out e cascata 14
 - Licenze SnapMirror 17
 - Miglioramenti delle funzionalità dei sistemi DPO 20

Replica del volume SnapMirror

Nozioni di base sul disaster recovery asincrono di SnapMirror

SnapMirror è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o *mirror*, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

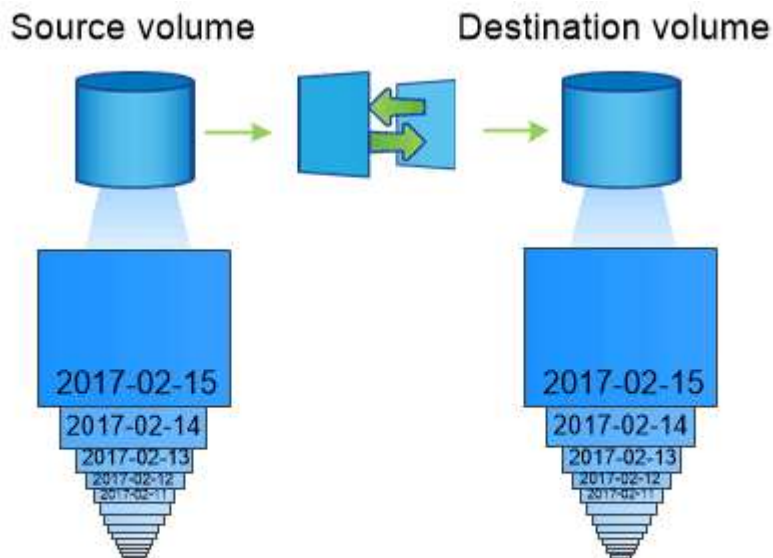
Se il sito primario è ancora disponibile per la fornitura dei dati, è possibile semplicemente trasferire di nuovo i dati necessari e non servire i client dal mirror. Come implica il caso di utilizzo del failover, i controller sul sistema secondario devono essere equivalenti o quasi equivalenti ai controller sul sistema primario per fornire i dati in modo efficiente dallo storage mirrorato.

Relazioni di data Protection

I dati vengono mirrorati a livello di volume. La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene chiamata *relazione di protezione dei dati*. I cluster in cui risiedono i volumi e le SVM che servono i dati dei volumi devono essere *peering*. Una relazione peer consente lo scambio di cluster e SVM dati in modo sicuro.

"Peering di cluster e SVM"

La figura seguente illustra le relazioni di protezione dei dati di SnapMirror.



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

Ambito delle relazioni di protezione dei dati

È possibile creare una relazione di protezione dei dati direttamente tra i volumi o tra le SVM che possiedono i volumi. In una relazione di protezione dei dati SVM, la configurazione SVM completa o parziale, dalle

esportazioni NFS e dalle condivisioni SMB a RBAC, viene replicata, così come i dati nei volumi di proprietà di SVM.

È inoltre possibile utilizzare SnapMirror per applicazioni speciali di protezione dei dati:

- Una copia *mirror per la condivisione del carico* del volume root SVM garantisce che i dati rimangano accessibili in caso di interruzione o failover di un nodo.
- Una relazione di protezione dei dati tra *volumi SnapLock* consente di replicare i file WORM sullo storage secondario.

"Archiviazione e conformità con la tecnologia SnapLock"

- A partire da ONTAP 9.13.1, è possibile utilizzare SnapMirror asincrono per la protezione [gruppi di coerenza](#). A partire da ONTAP 9.14.1, puoi utilizzare SnapMirror asincrono per replicare le snapshot granulari del volume nel cluster di destinazione usando la relazione del gruppo di coerenza. Per ulteriori informazioni, vedere [Configurare la protezione asincrona di SnapMirror](#).

Come vengono inizializzate le relazioni di protezione dei dati di SnapMirror

La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. La *policy SnapMirror* per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Trasferimento di riferimento con il criterio predefinito di SnapMirror `MirrorAllSnapshots` prevede i seguenti passaggi:

- Creare una copia Snapshot del volume di origine.
- Trasferire la copia Snapshot e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.
- Trasferire le copie Snapshot rimanenti, meno recenti, sul volume di origine al volume di destinazione per l'utilizzo in caso di danneggiamento del mirror "Active".

Come vengono aggiornate le relazioni di protezione dei dati di SnapMirror

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. La conservazione rispecchia la policy Snapshot sull'origine.

Ad ogni aggiornamento in `MirrorAllSnapshots` SnapMirror crea una copia Snapshot del volume di origine e trasferisce la copia Snapshot e le copie Snapshot eseguite dall'ultimo aggiornamento. Nel seguente output da `snapmirror policy show` comando per `MirrorAllSnapshots` policy, tenere presente quanto segue:

- `Create Snapshot` è "true", a indicare che `MirrorAllSnapshots` Crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- `MirrorAllSnapshots` Dispone delle regole "sm_created" e "all_source_snapshot", che indicano che sia la copia Snapshot creata da SnapMirror che le copie Snapshot eseguite dall'ultimo aggiornamento vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst:> snapmirror policy show -policy MirrorAllSnapshots -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: Asynchronous SnapMirror policy for mirroring
all snapshots
and the latest active file system.
Total Number of Rules: 2
Total Keep: 2
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
sm_created                  1  false      0  -
all_source_snapshots       1  false      0  -
```

Policy MirrorLatest

Preconfigurato `MirrorLatest` la policy funziona esattamente come `MirrorAllSnapshots`, Ad eccezione del fatto che solo la copia Snapshot creata da SnapMirror viene trasferita all'inizializzazione e all'aggiornamento.

```
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
sm_created                  1  false      0  -
```

Nozioni di base sul disaster recovery sincrono di SnapMirror

A partire da ONTAP 9.5, la tecnologia SnapMirror Synchronous (SM-S) è supportata su tutte le piattaforme FAS e AFF con almeno 16 GB di memoria e su tutte le piattaforme

ONTAP Select. La tecnologia SnapMirror Synchronous è una funzionalità concessa in licenza per nodo che fornisce la replica sincrona dei dati a livello di volume.

Questa funzionalità soddisfa i requisiti normativi e nazionali per la replica sincrona in settori finanziari, sanitari e altri settori regolamentati in cui non è richiesta alcuna perdita di dati.

Operazioni di SnapMirror Synchronous consentite

Il limite del numero di operazioni di replica sincrona di SnapMirror per coppia ha dipende dal modello di controller.

La tabella seguente elenca il numero di operazioni sincroni di SnapMirror consentite per coppia ha in base al tipo di piattaforma e alla release di ONTAP.

Piattaforma	Versioni precedenti a ONTAP 9.9.1	ONTAP 9.9.1	ONTAP 9.10.1	Da ONTAP 9.11.1 a ONTAP 9.14.1
AFF	80	160	200	400
ASA	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

Funzionalità supportate

La tabella seguente indica le funzionalità supportate con SnapMirror Synchronous e le release ONTAP in cui è disponibile il supporto.

Funzione	Release supportata per la prima volta	Ulteriori informazioni
Antivirus sul volume primario della relazione sincrona di SnapMirror	ONTAP 9.6	
Replica delle copie Snapshot creata dall'applicazione	ONTAP 9.7	Se una copia Snapshot viene contrassegnata con l'etichetta appropriata al momento della <code>snapshot create</code> Operazione, utilizzando l'interfaccia CLI o l'API ONTAP, SnapMirror Synchronous replica le copie Snapshot, create dall'utente o con script esterni, dopo aver terminato le applicazioni. Le copie Snapshot pianificate create utilizzando una policy Snapshot non vengono replicate. Per ulteriori informazioni sulla replica delle copie Snapshot create dall'applicazione, consultare l'articolo della Knowledge base: "Come replicare gli snapshot creati dall'applicazione con SnapMirror Synchronous" .
Clona eliminazione automatica	ONTAP 9.6	

Gli aggregati FabricPool con policy di tiering Nessuno, Snapshot o Auto sono supportati con origine e destinazione sincrone di SnapMirror.	ONTAP 9.5	Il volume di destinazione in un aggregato FabricPool non può essere impostato su tutti i criteri di tiering.
FC	ONTAP 9.5	Su tutte le reti per le quali la latenza non supera i 10ms ms.
FC-NVMe	ONTAP 9.7	
Cloni dei file	ONTAP 9.7	
FPolicy sul volume primario della relazione sincrone di SnapMirror	ONTAP 9.6	
Quote hard e soft sul volume primario della relazione di SnapMirror Synchronous	ONTAP 9.6	Le regole di quota non vengono replicate nella destinazione, pertanto il database di quota non viene replicato nella destinazione.
Relazioni sincrone all'interno del cluster	ONTAP 9.14.1	L'high Availability viene fornita quando i volumi di origine e destinazione vengono posizionati su diverse coppie ha. In caso di guasto dell'intero cluster, l'accesso ai volumi non sarà possibile fino al ripristino del cluster. Le relazioni sincrone intra-cluster di SnapMirror contribuiranno al limite complessivo della simultaneità Relazioni per coppia ha .
ISCSI	ONTAP 9.5	
Cloni LUN e cloni namespace NVMe	ONTAP 9.7	
Cloni LUN supportati dalle copie Snapshot create dalle applicazioni	ONTAP 9.7	
Accesso al protocollo misto (NFS v3 e SMB)	ONTAP 9.6	
Ripristino NDMP/NDMP	ONTAP 9.13.1	Sia il cluster di origine che quello di destinazione devono eseguire ONTAP 9.13.1 o versione successiva per utilizzare NDMP con SnapMirror Synchronous. Per ulteriori informazioni, vedere Trasferire i dati utilizzando la copia ndmp .
Operazioni sincrone SnapMirror senza interruzioni (NDO) solo su piattaforme AFF/ASA.	ONTAP 9.12.1	Il supporto per operazioni senza interruzioni consente di eseguire molte attività di manutenzione comuni senza pianificare i tempi di inattività. Le operazioni supportate includono takeover e giveback e spostamento del volume, a condizione che un singolo nodo sopravviva tra ciascuno dei due cluster.
NFS v4,2	ONTAP 9.10.1	
NFS v4,3	ONTAP 9.5	
NFS v4.0	ONTAP 9.6	
NFS v4,1	ONTAP 9.6	
NVMe/TCP	9.10.1	

Rimozione della limitazione di frequenza delle operazioni con metadati elevati	ONTAP 9.6	
Sicurezza per i dati sensibili in transito con crittografia TLS 1.2	ONTAP 9.6	
Ripristino di file singoli e file parziale	ONTAP 9.13.1	
SMB 2.0 o versione successiva	ONTAP 9.6	
Cascata del mirror sincrono di SnapMirror	ONTAP 9.6	Il rapporto dal volume di destinazione della relazione di SnapMirror Synchronous deve essere una relazione di SnapMirror asincrono.
Disaster recovery SVM	ONTAP 9.6	<p>* Una fonte di SnapMirror Synchronous può anche essere un'origine di disaster recovery SVM, ad esempio una configurazione fan-out con SnapMirror Synchronous come una tappa e il disaster recovery SVM come l'altra.</p> <p>* Un'origine SnapMirror Synchronous non può essere una destinazione di disaster recovery SVM perché SnapMirror Synchronous non supporta la catena di un'origine di data Protection. È necessario rilasciare la relazione sincrona prima di eseguire la risincronizzazione in caso di disaster recovery delle SVM nel cluster di destinazione.</p> <p>* Una destinazione SnapMirror Synchronous non può essere un'origine di disaster recovery SVM perché il disaster recovery SVM non supporta la replica dei volumi DP. Una risincronizzazione in flip dell'origine sincrona causerebbe il disaster recovery della SVM, escludendo il volume DP nel cluster di destinazione.</p>
Ripristino basato su nastro sul volume di origine	ONTAP 9.13.1	
Parità di timestamp tra volumi di origine e destinazione per NAS	ONTAP 9.6	Se è stato eseguito l'aggiornamento da ONTAP 9,5 a ONTAP 9,6, l'indicatore data e ora viene replicato solo per i file nuovi e modificati nel volume di origine. L'indicatore orario dei file esistenti nel volume di origine non viene sincronizzato.

Funzionalità non supportate

Le seguenti funzionalità non sono supportate con le relazioni di SnapMirror sincrono:

- Gruppi di coerenza
- Sistemi DP_Optimized (DPO)
- Volumi FlexGroup
- Volumi FlexCache

- Rallentamento globale
- In una configurazione fan-out, una sola relazione può essere una relazione sincrona di SnapMirror; tutte le altre relazioni del volume di origine devono essere relazioni asincrone di SnapMirror.
- Spostamento delle LUN
- Configurazioni MetroCluster
- I LUN di accesso MIST SAN e NVMe e gli spazi dei nomi NVMe non sono supportati sullo stesso volume o SVM.
- SnapCenter
- Volumi SnapLock
- Copie Snapshot a prova di manomissione
- Backup o ripristino su nastro utilizzando dump e SMTape sul volume di destinazione
- Throughput floor (QoS min) per volumi di origine
- SnapRestore volume
- Vol

Modalità operative

SnapMirror Synchronous dispone di due modalità operative in base al tipo di policy SnapMirror utilizzata:

- **Sync mode** in modalità Sync, le operazioni di i/o dell'applicazione vengono inviate in parallelo ai sistemi di storage primario e secondario. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'applicazione può continuare a scrivere sullo storage primario. Quando la condizione di errore viene corretta, la tecnologia SnapMirror Synchronous risincronizza automaticamente con lo storage secondario e riprende la replica dallo storage primario allo storage secondario in modalità sincrona. In modalità Sync, RPO=0 e RTO sono molto bassi fino a quando non si verifica un errore di replica secondario, in cui RPO e RTO diventano indeterminati, ma pari al tempo necessario per riparare il problema che ha causato il fallimento della replica secondaria e il completamento della risincronizzazione.
- **Modalità StrictSync** SnapMirror Synchronous può funzionare in modalità StrictSync. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'i/o dell'applicazione non riesce, garantendo che lo storage primario e secondario siano identici. L'i/o dell'applicazione verso il primario riprende solo dopo che la relazione SnapMirror ritorna a InSync stato. In caso di guasto dello storage primario, l'i/o dell'applicazione può essere ripristinato sullo storage secondario, dopo il failover, senza perdita di dati. In modalità StrictSync, l'RPO è sempre zero e l'RTO è molto basso.

Stato della relazione

Lo stato di una relazione sincrona di SnapMirror è sempre in InSync stato durante il normale funzionamento. Se il trasferimento di SnapMirror non riesce per qualsiasi motivo, la destinazione non è sincronizzata con l'origine e può andare al OutofSync stato.

Per le relazioni sincroni di SnapMirror, il sistema verifica automaticamente lo stato della relazione (InSync oppure OutofSync) a intervalli fissi. Se lo stato della relazione è OutofSync, ONTAP attiva automaticamente il processo di risincronizzazione automatica per riportare la relazione a InSync stato. La risincronizzazione automatica viene attivata solo se il trasferimento non riesce a causa di un'operazione, ad esempio un failover dello storage non pianificato all'origine o alla destinazione o un'interruzione della rete. Operazioni avviate dall'utente come `snapmirror quiesce` e `snapmirror break` non attivano la risincronizzazione automatica.

Se lo stato della relazione diventa `OutOfSync` Per una relazione sincrona di SnapMirror in modalità `StrictSync`, tutte le operazioni di i/o sul volume primario vengono interrotte. Il `OutOfSync` lo stato per la relazione sincrona di SnapMirror in modalità `Sync` non è disagiata per il principale e le operazioni di i/o sono consentite sul volume primario.

Informazioni correlate

["Report tecnico NetApp 4733: Configurazione sincrona e Best practice di SnapMirror"](#)

Informazioni sui carichi di lavoro supportati dalle policy di `StrictSync` e `Sync`

Le policy `StrictSync` e `Sync` supportano tutte le applicazioni basate su LUN con protocolli FC, iSCSI e FC-NVMe, nonché i protocolli NFSv3 e NFSv4 per applicazioni aziendali come database, VMware, quota, SMB e così via. A partire da ONTAP 9.6, SnapMirror Synchronous può essere utilizzato per i file service aziendali come EDA (Electronic Design Automation), home directory e carichi di lavoro di build del software.

In ONTAP 9.5, per una policy di sincronizzazione, è necessario considerare alcuni aspetti importanti durante la selezione dei carichi di lavoro NFSv3 o NFSv4. La quantità di operazioni di lettura o scrittura dei dati da parte dei carichi di lavoro non è una considerazione, in quanto la policy `Sync` può gestire elevati carichi di lavoro io in lettura o scrittura. In ONTAP 9.5, i carichi di lavoro che presentano una creazione di file, una creazione di directory, modifiche ai permessi dei file o modifiche ai permessi delle directory eccessive potrebbero non essere adatti (tali carichi di lavoro vengono definiti carichi di lavoro con metadati elevati). Un tipico esempio di workload con metadati elevati è un workload DevOps in cui è possibile creare più file di test, eseguire l'automazione ed eliminare i file. Un altro esempio è rappresentato dal carico di lavoro di creazione parallela che genera più file temporanei durante la compilazione. L'impatto di un elevato tasso di attività di scrittura dei metadati è che può causare la temporanea interruzione della sincronizzazione tra i mirror, che blocca gli iOS di lettura e scrittura dal client.

A partire da ONTAP 9.6, queste limitazioni vengono rimosse e SnapMirror Synchronous può essere utilizzato per i carichi di lavoro dei file service aziendali che includono ambienti multiutente, come home directory e carichi di lavoro di build del software.

Informazioni correlate

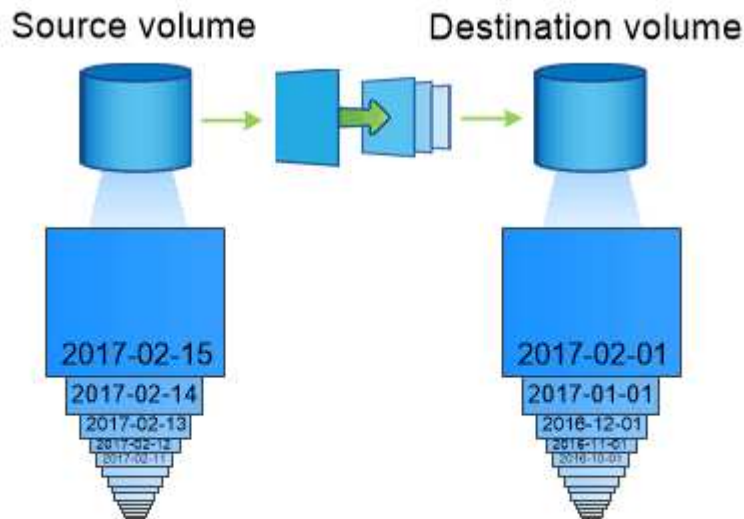
["Procedure consigliate e configurazione sincrona di SnapMirror"](#)

Archiviazione del vault con la tecnologia SnapMirror

I criteri di vault di SnapMirror sostituiscono la tecnologia SnapVault in ONTAP 9.3 e versioni successive. Si utilizza un criterio di vault SnapMirror per la replica delle copie Snapshot disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione del vault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

È possibile conservare copie Snapshot mensili dei dati per un periodo di 20 anni, ad esempio per rispettare le normative contabili governative per la propria azienda. Poiché non è necessario fornire dati dallo storage del vault, è possibile utilizzare dischi più lenti e meno costosi sul sistema di destinazione.

La figura seguente illustra le relazioni di protezione dei dati del vault SnapMirror.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Come vengono inizializzate le relazioni di protezione dei dati del vault

Il criterio SnapMirror per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Un trasferimento di riferimento con la policy di default del vault `XDPDefault` esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. A differenza delle relazioni SnapMirror, un backup del vault non include copie Snapshot precedenti nella linea di base.

Come vengono aggiornate le relazioni di protezione dei dati del vault

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. Le regole definite nella policy per la relazione identificano quali nuove copie Snapshot includere negli aggiornamenti e quante copie conservare. Le etichette definite nella policy ("monthly," ad esempio) devono corrispondere a una o più etichette definite nella policy Snapshot sull'origine. In caso contrario, la replica non riesce.

Ad ogni aggiornamento in `XDPDefault SnapMirror` trasferisce le copie Snapshot eseguite dall'ultimo aggiornamento, a condizione che le etichette corrispondano alle etichette definite nelle regole dei criteri. Nel seguente output da `snapmirror policy show` comando per `XDPDefault policy`, tenere presente quanto segue:

- `Create Snapshot` è “false”, a indicare che `XDPDefault` Non crea una copia Snapshot quando `SnapMirror` aggiorna la relazione.
- `XDPDefault` Dispone di regole “daily” e “settimanale”, che indicano che tutte le copie Snapshot con etichette corrispondenti sull’origine vengono trasferite quando `SnapMirror` aggiorna la relazione.

```
cluster_dst:> snapmirror policy show -policy XDPDefault -instance

                Vserver: vs0
SnapMirror Policy Name: XDPDefault
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Default policy for XDP relationships with
daily and weekly
                        rules.
                Total Number of Rules: 2
                Total Keep: 59
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                        daily                7   false    0 -
-
                        weekly              52   false    0 -
-
```

Nozioni di base sulla replica unificata di SnapMirror

SnapMirror *replica unificata* consente di configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione. Quando la replica unificata è appropriata, offre vantaggi in termini di riduzione della quantità di storage secondario necessaria, limitazione del numero di trasferimenti di riferimento e riduzione del traffico di rete.

Come vengono inizializzate le relazioni unificate di protezione dei dati

Come con SnapMirror, la protezione unificata dei dati esegue un trasferimento di riferimento la prima volta che lo si richiama. Il criterio SnapMirror per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Un trasferimento di riferimento in base alla policy di protezione dei dati unificata predefinita `MirrorAndVault` esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. Come l'archiviazione del vault, la protezione unificata dei dati non include copie Snapshot precedenti nella linea di base.

Come vengono aggiornate le relazioni unificate di protezione dei dati

Ad ogni aggiornamento in MirrorAndVault Policy, SnapMirror crea una copia Snapshot del volume di origine e trasferisce la copia Snapshot e le copie Snapshot eseguite dall'ultimo aggiornamento, a condizione che le etichette corrispondano alle etichette definite nelle regole dei criteri di Snapshot. Nel seguente output da `snapmirror policy show` comando per MirrorAndVault policy, tenere presente quanto segue:

- Create Snapshot è "true", a indicare che MirrorAndVault Crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- MirrorAndVault Dispone delle regole "sm_created", "daily" e "settimanale", che indicano che sia la copia Snapshot creata da SnapMirror che le copie Snapshot con le etichette corrispondenti sull'origine vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst:> snapmirror policy show -policy MirrorAndVault -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAndVault
SnapMirror Policy Type: mirror-vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: A unified Synchronous SnapMirror and
SnapVault policy for
mirroring the latest file system and daily
and weekly snapshots.
Total Number of Rules: 3
Total Keep: 59
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                  1  false    0  -
daily                       7  false    0  -
weekly                     52  false    0  -
```

Politica Unified7year

Preconfigurato Unified7year la policy funziona esattamente come MirrorAndVault, Ad eccezione del fatto che una quarta regola trasferisce le copie Snapshot mensili e le conserva per sette anni.

Schedule Prefix	Rules: SnapMirror Label	Keep	Preserve	Warn
-----	-----	----	-----	----
-	sm_created	1	false	0 -
-	daily	7	false	0 -
-	weekly	52	false	0 -
-	monthly	84	false	0 -
-				

Protegersi da possibili danneggiamenti dei dati

La replica unificata limita il contenuto del trasferimento di riferimento alla copia Snapshot creata da SnapMirror all'inizializzazione. A ogni aggiornamento, SnapMirror crea un'altra copia Snapshot dell'origine e trasferisce tale copia Snapshot e le nuove copie Snapshot che presentano etichette corrispondenti alle etichette definite nelle regole dei criteri Snapshot.

È possibile proteggersi dalla possibilità che una copia Snapshot aggiornata venga danneggiata creando una copia dell'ultima copia Snapshot trasferita sulla destinazione. Questa "copia locale" viene conservata indipendentemente dalle regole di conservazione sull'origine, in modo che anche se l'istantanea originariamente trasferita da SnapMirror non è più disponibile sull'origine, una copia di essa sarà disponibile sulla destinazione.

Quando utilizzare la replica unificata dei dati

È necessario valutare i vantaggi derivanti dal mantenimento di un mirror completo rispetto ai vantaggi offerti dalla replica unificata nella riduzione della quantità di storage secondario, nella limitazione del numero di trasferimenti di riferimento e nella riduzione del traffico di rete.

Il fattore chiave per determinare l'adeguatezza della replica unificata è il tasso di cambiamento del file system attivo. Un mirror tradizionale potrebbe essere più adatto a un volume che contiene copie Snapshot orarie dei log delle transazioni del database, ad esempio.

XDP sostituisce DP come impostazione predefinita di SnapMirror

A partire da ONTAP 9.3, la modalità XDP (Extended Data Protection) di SnapMirror sostituisce la modalità DP (Data Protection) di SnapMirror come impostazione predefinita.

Prima di eseguire l'aggiornamento a ONTAP 9.12.1, è necessario convertire le relazioni di tipo DP esistenti in XDP prima di poter eseguire l'aggiornamento a ONTAP 9.12.1 e versioni successive. Per ulteriori informazioni, vedere ["Convertire una relazione di tipo DP esistente in XDP"](#).

Fino a ONTAP 9.3, SnapMirror invocato in modalità DP e SnapMirror richiamato in modalità XDP utilizzavano

diversi motori di replica, con diversi approcci alla dipendenza dalla versione:

- SnapMirror invocato in modalità DP utilizzava un motore di replica *dipendente dalla versione* in cui la versione di ONTAP doveva essere la stessa sullo storage primario e secondario:

```
cluster_dst::> snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror invocato in modalità XDP utilizzava un motore di replica *version-Flexible* che supportava diverse versioni di ONTAP sullo storage primario e secondario:

```
cluster_dst::> snapmirror create -type XDP -source-path ...
-destination-path ...
```

Con i miglioramenti delle performance, i benefici significativi di SnapMirror flessibile per la versione superano il leggero vantaggio nel throughput di replica ottenuto con la modalità dipendente dalla versione. Per questo motivo, a partire da ONTAP 9.3, la modalità XDP è stata impostata come nuova impostazione predefinita e tutte le invocazioni della modalità DP sulla riga di comando o in script nuovi o esistenti vengono automaticamente convertite in modalità XDP.

Le relazioni esistenti non vengono influenzate. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. A partire da ONTAP 9.5, MirrorAndVault è il nuovo criterio predefinito quando non viene specificata alcuna modalità di protezione dei dati o quando viene specificata la modalità XDP come tipo di relazione. La tabella seguente mostra il comportamento che ci si può aspettare.

Se si specifica...	Il tipo è...	Il criterio predefinito (se non si specifica un criterio) è...
DP	XDP	MirrorAllSnapshot (DR SnapMirror)
Niente	XDP	MirrorAndVault (replica unificata)
XDP	XDP	MirrorAndVault (replica unificata)

Come mostrato nella tabella, i criteri predefiniti assegnati a XDP in diverse circostanze garantiscono che la conversione mantenga l'equivalenza funzionale dei tipi precedenti. Naturalmente, è possibile utilizzare policy diverse in base alle esigenze, incluse le policy per la replica unificata:

Se si specifica...	E la policy è...	Il risultato è...
DP	MirrorAllSnapshot	Dr. SnapMirror
XDPDefault	SnapVault	MirrorAndVault
Replica unificata	XDP	MirrorAllSnapshot
Dr. SnapMirror	XDPDefault	SnapVault

Le uniche eccezioni alla conversione sono le seguenti:

- Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.3 e versioni precedenti.

A partire da ONTAP 9.4, le relazioni di protezione dei dati SVM passano per impostazione predefinita alla modalità XDP.

- Le relazioni di protezione dei dati per la condivisione del carico del volume root continuano a essere predefinite in modalità DP.
- Le relazioni di protezione dei dati di SnapLock continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.4 e versioni precedenti.

A partire da ONTAP 9.5, le relazioni di protezione dei dati di SnapLock passano per impostazione predefinita alla modalità XDP.

- Le invocazioni esplicite di DP continuano a essere predefinite in modalità DP se si imposta la seguente opzione a livello di cluster:

```
options replication.create_data_protection_rels.enable on
```

Questa opzione viene ignorata se non si richiama esplicitamente DP.

Quando un volume di destinazione cresce automaticamente

Durante il trasferimento di un mirror per la protezione dei dati, le dimensioni del volume di destinazione aumentano automaticamente se il volume di origine è cresciuto, a condizione che nell'aggregato sia presente spazio disponibile che contiene il volume.

Questo comportamento si verifica indipendentemente da qualsiasi impostazione di crescita automatica sulla destinazione. Non puoi limitare la crescita del volume o impedire a ONTAP di crescere.

Per impostazione predefinita, i volumi di protezione dei dati sono impostati su `grow_shrink` modalità di dimensionamento automatico, che consente al volume di crescere o ridursi in risposta alla quantità di spazio utilizzato. La dimensione automatica massima per i volumi di protezione dei dati è uguale alla dimensione massima FlexVol e dipende dalla piattaforma. Ad esempio:

- FAS6220, volume DP predefinito max-autodize = 70 TB
- FAS8200, volume DP predefinito max-autodize = 100 TB

Per ulteriori informazioni, vedere ["NetApp Hardware Universe"](#).

Implementazioni di protezione dei dati fan-out e cascata

È possibile utilizzare un'implementazione *fan-out* per estendere la protezione dei dati a più sistemi secondari. È possibile utilizzare un'implementazione *Cascade* per estendere la protezione dei dati ai sistemi terziari.

Le implementazioni fan-out e cascata supportano qualsiasi combinazione di DR SnapMirror, SnapVault o

replica unificata; tuttavia, le relazioni sincrone SnapMirror (supportate a partire da ONTAP 9.5) supportano solo implementazioni fan-out con una o più relazioni SnapMirror asincrone e non supportano implementazioni a cascata. Solo una relazione nella configurazione fan-out può essere una relazione sincrona di SnapMirror, mentre tutte le altre relazioni del volume di origine devono essere relazioni asincrone di SnapMirror. [Continuità aziendale di SnapMirror](#) (Supportato a partire da ONTAP 9.8) supporta anche le configurazioni fan-out.



È possibile utilizzare un'implementazione *fan-in* per creare relazioni di protezione dei dati tra più sistemi primari e un singolo sistema secondario. Ogni relazione deve utilizzare un volume diverso sul sistema secondario.

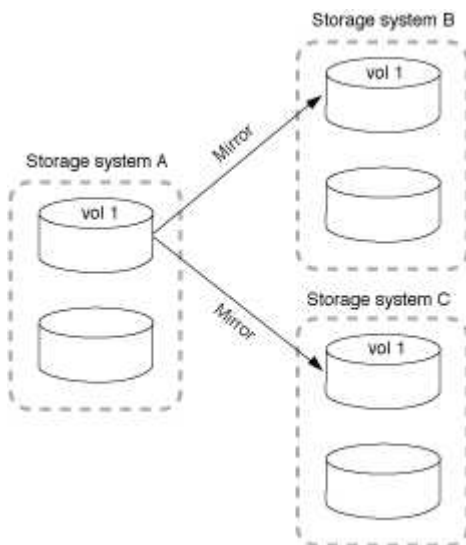


Tenere presente che la risincronizzazione dei volumi che fanno parte di una configurazione fan-out o a cascata può richiedere più tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

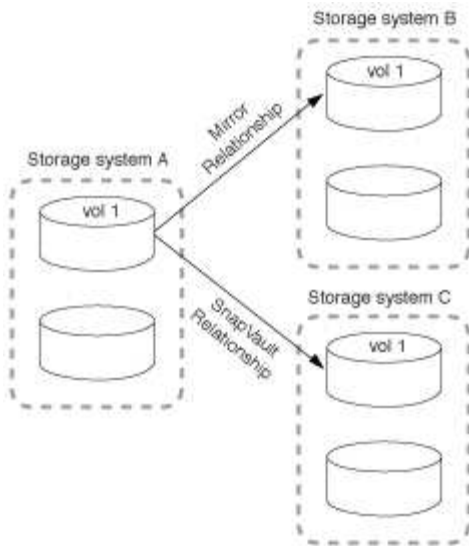
Come funzionano le implementazioni fan-out

SnapMirror supporta le implementazioni fan-out di *mirror multipli* e *mirror-vault*.

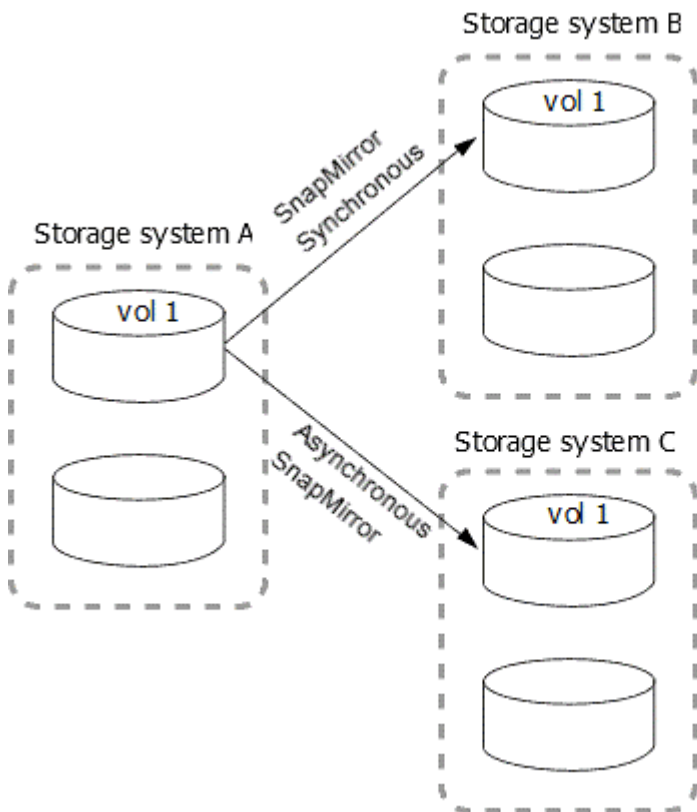
Un'implementazione fan-out con mirror multipli consiste in un volume di origine che ha una relazione di mirroring con più volumi secondari.



Un'implementazione fan-out del vault mirror è costituita da un volume di origine che ha una relazione di mirroring con un volume secondario e una relazione SnapVault con un volume secondario diverso.



A partire da ONTAP 9.5, è possibile avere implementazioni fan-out con relazioni sincrone di SnapMirror; tuttavia, solo una relazione nella configurazione fan-out può essere una relazione sincrona di SnapMirror, tutte le altre relazioni dal volume di origine devono essere relazioni asincrone di SnapMirror.



Come funzionano le implementazioni a cascata

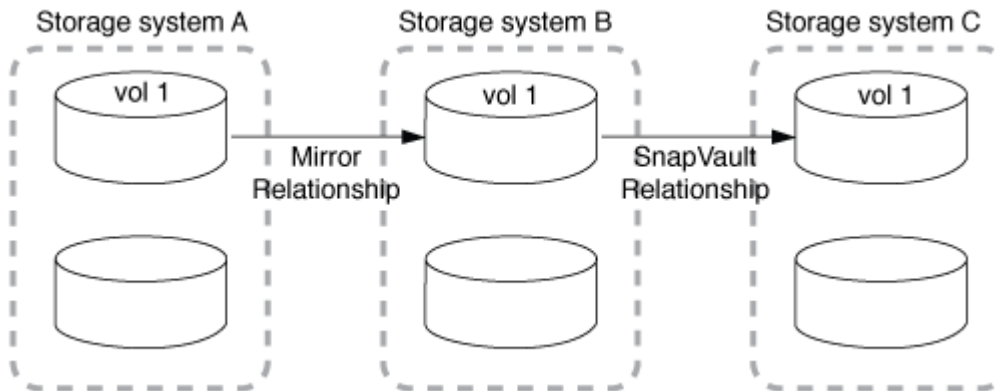
SnapMirror supporta le implementazioni a cascata di *mirror-mirror*, *mirror-vault*, *vault-mirror* e *vault-vault*.

Un'implementazione a cascata di mirror consiste in una catena di relazioni in cui un volume di origine viene mirrorato su un volume secondario e il volume secondario viene mirrorato su un volume terzo. Se il volume secondario non è più disponibile, è possibile sincronizzare la relazione tra il volume primario e il volume terzo senza eseguire un nuovo trasferimento di riferimento.

A partire da ONTAP 9.6, le relazioni sincroni di SnapMirror sono supportate in una distribuzione a cascata con mirror. Solo i volumi primari e secondari possono trovarsi in una relazione sincrona di SnapMirror. La relazione tra i volumi secondari e i volumi terziari deve essere asincrona.



Un'implementazione a cascata del vault mirror consiste in una catena di relazioni in cui un volume di origine viene mirrorato su un volume secondario e il volume secondario viene vault su un volume terzo.



Sono supportate anche le implementazioni Vault-Mirror e, a partire da ONTAP 9.2, Vault-Vault Cascade:

- Un'implementazione a cascata del vault-mirror consiste in una catena di relazioni in cui un volume di origine viene vault su un volume secondario e il volume secondario viene mirrorato su un volume terzo.
- (A partire da ONTAP 9.2) Una distribuzione a cascata di vault è costituita da una catena di relazioni in cui un volume di origine viene vault su un volume secondario e il volume secondario viene vault su un volume terzo.

Ulteriori letture

- [Ripristino della protezione in una configurazione fan-out con SM-BC](#)

Licenze SnapMirror

Panoramica sulle licenze di SnapMirror

A partire da ONTAP 9.3, le licenze sono state semplificate per la replica tra istanze di ONTAP. Nelle versioni di ONTAP 9, la licenza SnapMirror supporta le relazioni di vault e mirror. Puoi utilizzare una licenza SnapMirror per supportare la replica ONTAP per casi d'utilizzo di backup e disaster recovery.

Prima della release di ONTAP 9.3, era necessaria una licenza SnapVault separata per configurare le relazioni *vault* tra le istanze di ONTAP, in cui l'istanza DP poteva mantenere un numero più elevato di copie Snapshot per supportare i casi d'utilizzo del backup con tempi di conservazione più lunghi, inoltre, era necessaria una licenza SnapMirror per configurare relazioni *mirror* tra istanze di ONTAP, in cui ciascuna istanza di ONTAP

conservava lo stesso numero di copie Snapshot (ovvero un'immagine *mirror*) per supportare i casi d'utilizzo di disaster recovery al fine di rendere possibili i failover dei cluster. Le licenze SnapMirror e SnapVault continuano a essere utilizzate e supportate per le release di ONTAP 8.x e 9.x.

Mentre le licenze SnapVault continuano a funzionare e sono supportate per entrambe le release di ONTAP 8.x e 9.x, la licenza SnapMirror può essere utilizzata al posto di una licenza SnapVault e può essere utilizzata sia per le configurazioni mirror che per quelle del vault.

Per la replica asincrona di ONTAP, a partire da ONTAP 9.3 viene utilizzato un singolo motore di replica unificato per configurare i criteri XDP (Extended Data Protection Mode), in cui la licenza SnapMirror può essere configurata per un criterio mirror, un criterio di vault o un criterio di vault mirror. È necessaria una licenza SnapMirror sia per i cluster di origine che per quelli di destinazione. Se è già installata una licenza SnapVault, non è necessaria alcuna licenza SnapMirror. La licenza perpetua asincrona SnapMirror è inclusa nella suite software ONTAP One installata sui nuovi sistemi AFF e FAS.

I limiti di configurazione per la protezione dei dati vengono determinati in base a diversi fattori, tra cui la versione di ONTAP, la piattaforma hardware e le licenze installate. Per ulteriori informazioni, vedere ["Hardware Universe"](#).

Licenza SnapMirror Synchronous

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. Per creare una relazione sincrona con SnapMirror sono necessarie le seguenti licenze:

- La licenza SnapMirror Synchronous è richiesta sia sul cluster di origine che sul cluster di destinazione.

La licenza SnapMirror Synchronous è parte di ["Suite di licenze ONTAP One"](#).

Se il sistema è stato acquistato prima di giugno 2019 con un pacchetto Premium o Flash, è possibile scaricare una chiave master NetApp per ottenere la licenza SnapMirror Synchronous richiesta dal sito di supporto NetApp: ["Chiavi di licenza master"](#).

- La licenza SnapMirror è richiesta sia sul cluster di origine che sul cluster di destinazione.

Licenza SnapMirror Cloud

A partire da ONTAP 9.8, la licenza di SnapMirror Cloud offre la replica asincrona delle copie Snapshot dalle istanze di ONTAP agli endpoint dello storage a oggetti. Le destinazioni di replica possono essere configurate utilizzando archivi di oggetti on-premise e servizi di storage a oggetti cloud pubblico compatibili con S3 e S3. Le relazioni cloud di SnapMirror sono supportate dai sistemi ONTAP alle destinazioni di storage a oggetti pre-qualificate.

SnapMirror Cloud non è disponibile come licenza standalone. È necessaria una sola licenza per cluster ONTAP. Oltre a una licenza SnapMirror Cloud, è necessaria anche la licenza SnapMirror asincrona.

Per creare una relazione SnapMirror Cloud sono necessarie le seguenti licenze:

- Sia una licenza SnapMirror che una licenza SnapMirror Cloud per la replica direttamente nell'endpoint dell'archivio di oggetti.
- Quando si configura un flusso di lavoro di replica multi-policy (ad esempio, da disco a disco a cloud), è necessaria una licenza SnapMirror su tutte le istanze di ONTAP, mentre la licenza SnapMirror Cloud è richiesta solo per il cluster di origine che esegue la replica direttamente sull'endpoint dello storage a oggetti.

A partire da ONTAP 9.9.1, è possibile ["Utilizza System Manager per la replica SnapMirror Cloud"](#).

Un elenco delle applicazioni di terze parti autorizzate di SnapMirror Cloud è pubblicato sul sito Web di NetApp.

Licenza ottimizzata per la protezione dei dati

Le licenze DPO (Data Protection Optimized) non vengono più vendute e il DPO non è supportato sulle piattaforme correnti; tuttavia, se si dispone di una licenza DPO installata su una piattaforma supportata, NetApp continua a fornire supporto fino alla fine della disponibilità di tale piattaforma.

DPO non è incluso nel pacchetto di licenze di ONTAP One e non è possibile eseguire l'aggiornamento al pacchetto di licenze di ONTAP One se la licenza DPO è installata su un sistema.

Per informazioni sulle piattaforme supportate, vedere ["Hardware Universe"](#).

Installare le licenze di SnapMirror Cloud

È possibile orchestrare le relazioni con SnapMirror Cloud utilizzando applicazioni di backup di terze parti prequalificate. A partire da ONTAP 9.9.1, puoi anche utilizzare System Manager per orchestrare la replica cloud di SnapMirror. Le licenze di capacità di SnapMirror e SnapMirror Cloud sono necessarie quando si utilizza System Manager per orchestrare ONTAP on-premise ai backup di storage a oggetti. Devi anche richiedere e installare la licenza SnapMirror Cloud API.

A proposito di questa attività

Le licenze di SnapMirror Cloud e S3 SnapMirror sono licenze cluster, non di nodi, quindi *non* vengono fornite con il bundle della licenza di ONTAP One. Queste licenze sono incluse nel pacchetto di compatibilità ONTAP One separato. Per abilitare SnapMirror Cloud, devi richiedere questo bundle.

Inoltre, l'orchestrazione di System Manager dei backup SnapMirror Cloud nello storage a oggetti richiede una chiave SnapMirror Cloud API. Si tratta di una licenza API a singola istanza estesa a tutto il cluster, che non richiede l'installazione su ogni nodo del cluster.

Fasi

Devi richiedere e scaricare il bundle di compatibilità di ONTAP ONE e la licenza API di SnapMirror Cloud, quindi installarli utilizzando System Manager.

1. Individuare e registrare l'UUID del cluster per il cluster che si desidera concedere in licenza.

L'UUID del cluster è necessario quando invii la richiesta di ordinare il bundle di compatibilità di ONTAP One per il tuo cluster.

2. Contatta il tuo team di vendita NetApp e richiedi il pacchetto compatibilità ONTAP One.
3. Richiedere la licenza SnapMirror Cloud API seguendo le istruzioni fornite sul sito di supporto NetApp.

["Richiedere la chiave di licenza API di SnapMirror Cloud"](#)

4. Una volta ricevuti e scaricati i file di licenza, utilizzare Gestione sistema per caricare nel cluster la compatibilità cloud NLF di ONTAP e l'API cloud di SnapMirror NLF:
 - a. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
 - b. Nella finestra **Impostazioni**, fare clic su **licenze**.
 - c. Nella finestra **licenze**, fare clic su **+ Add**.

- d. Nella finestra di dialogo **Aggiungi licenza**, fare clic su **Sfoglia** per selezionare l'NLF scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

Informazioni correlate

["Eseguire il backup dei dati nel cloud utilizzando SnapMirror"](#)

["Ricerca licenze software NetApp"](#)

Miglioramenti delle funzionalità dei sistemi DPO

A partire da ONTAP 9.6, il numero massimo di volumi FlexVol supportati aumenta quando viene installata la licenza DP_Optimized (DPO). A partire da ONTAP 9.4, i sistemi con licenza DPO supportano il backoff di SnapMirror, la deduplica in background tra volumi, l'utilizzo di blocchi Snapshot come donatori e la compattazione.

A partire da ONTAP 9.6, il numero massimo di volumi FlexVol supportati sui sistemi secondari o di protezione dei dati è aumentato, consentendo di scalare fino a 2,500 volumi FlexVol per nodo o fino a 5,000 in modalità di failover. L'aumento dei volumi FlexVol viene abilitato con ["Licenza DP_Optimized \(DPO\)"](#). R ["Licenza SnapMirror"](#) è comunque necessario sia sui nodi di origine che su quelli di destinazione.

A partire da ONTAP 9.4, ai sistemi DPO sono stati apportati i seguenti miglioramenti:

- Backoff di SnapMirror: Nei sistemi DPO, al traffico di replica viene assegnata la stessa priorità dei carichi di lavoro client.

Il backoff di SnapMirror è disattivato per impostazione predefinita nei sistemi DPO.

- Deduplica del volume in background e deduplica del cross-volume in background: La deduplica del volume in background e la deduplica del cross-volume in background sono abilitate nei sistemi DPO.

È possibile eseguire `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` per deduplicare i dati esistenti. La Best practice consiste nell'eseguire il comando durante le ore di lavoro fuori dalle ore di punta per ridurre l'impatto sulle performance.

- Maggiori risparmi utilizzando i blocchi Snapshot come donatori: I blocchi di dati che non sono disponibili nel file system attivo ma sono intrappolati nelle copie Snapshot vengono utilizzati come donatori per la deduplica dei volumi.

I nuovi dati possono essere deduplicati con i dati intrappolati nelle copie Snapshot, condividendo efficacemente anche i blocchi Snapshot. L'aumento dello spazio dei donatori offre maggiori risparmi, soprattutto quando il volume dispone di un elevato numero di copie Snapshot.

- Compaction (compattazione): La compattazione dei dati è attivata per impostazione predefinita sui volumi DPO.

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.