



Considerazioni particolari

ONTAP 9

NetApp
February 12, 2026

Sommario

Considerazioni particolari	1
Prima di eseguire un aggiornamento, verificare la presenza di configurazioni ONTAP specifiche	1
Verificare la compatibilità delle versioni di ONTAP per i cluster di versioni miste	2
Cluster di versioni miste supportati per gli aggiornamenti software ONTAP	2
Aggiunta di nuovi nodi a un cluster ONTAP	4
Verificare i requisiti di aggiornamento di ONTAP per le configurazioni MetroCluster	5
Requisiti di configurazione per il normale funzionamento dell'MetroCluster	6
Requisiti di configurazione per lo switchover di MetroCluster	6
Verificare la configurazione dell'host SAN prima di un aggiornamento ONTAP	7
SnapMirror	7
Versioni ONTAP compatibili per le relazioni SnapMirror	8
Convertire una relazione di tipo ONTAP SnapMirror DP esistente in XDP	14
Disattiva gli snapshot di conservazione a lungo termine prima dell'aggiornamento di ONTAP	21
Verifica della licenza ONTAP per le configurazioni di SnapMirror S3	23
ONTAP 9.11.1 e versioni precedenti	23
ONTAP 9.12.1 e versioni successive	23
Relazioni esistenti con SnapMirror S3	23
Eliminare le connessioni al server di gestione chiavi esterno esistenti prima di aggiornare ONTAP	23
Verificare che il file netgroup sia presente su tutti i nodi prima di un aggiornamento di ONTAP	25
Assegnare un valore esplicito all'opzione v4,2-xatrs prima di un aggiornamento di ONTAP	26
Configurare i client LDAP in modo che utilizzino TLS prima di un aggiornamento ONTAP	26
Scopri gli effetti negativi dei protocolli orientati alla sessione durante gli aggiornamenti ONTAP	27
Verificare il supporto dell'algoritmo della chiave host SSH prima dell'aggiornamento di ONTAP	28
Risolvi gli avvisi delle attività nella protezione autonoma dal ransomware (ARP) prima di un upgrade ONTAP	29

Considerazioni particolari

Prima di eseguire un aggiornamento, verificare la presenza di configurazioni ONTAP specifiche

Alcune configurazioni cluster richiedono azioni specifiche prima di iniziare un aggiornamento software ONTAP. Ad esempio, se si dispone di una configurazione SAN, verificare che ogni host sia configurato con il numero corretto di percorsi diretti e indiretti prima di iniziare l'aggiornamento.

Consultare la tabella seguente per determinare quali ulteriori passaggi è necessario eseguire.

Prima di aggiornare ONTAP, chiediti...	Se la risposta è sì, eseguire questa operazione...
Il mio cluster è attualmente in uno stato di versione mista?	Verificare i requisiti di versione mista
Si dispone di una configurazione MetroCluster?	Verifica dei requisiti di aggiornamento specifici per le configurazioni MetroCluster
Si dispone di una configurazione SAN?	Verificare la configurazione dell'host SAN
Il mio cluster dispone di relazioni SnapMirror definite?	"Verifica la compatibilità delle versioni di ONTAP per le relazioni di SnapMirror"
Ho definito relazioni di SnapMirror di tipo DP e sto eseguendo l'aggiornamento a ONTAP 9.12.1 o versione successiva?	"Converti le relazioni di tipo DP esistenti in XDP"
Si utilizza SnapMirror S3 e si esegue l'aggiornamento a ONTAP 9.12.1 o versioni successive?	"Verifica della licenza per le configurazioni di SnapMirror S3"
Ho abilitato gli snapshot di conservazione a lungo termine sul volume intermedio di una cascata?	"Disattiva gli snapshot di conservazione a lungo termine nei volumi intermedi di topologie a cascata"
Utilizzo NetApp Storage Encryption con server di gestione delle chiavi esterni?	Eliminare le connessioni esistenti al server di gestione delle chiavi
I netgroup sono caricati nelle SVM?	Verificare che il file netgroup sia presente su ciascun nodo
Ho creato una SVM e sto eseguendo l'upgrade da ONTAP 9.12.1 o versione precedente a una versione successiva?	Assegnare un valore esplicito all'opzione v4,2-xattrs
I client LDAP utilizzano SSLv3?	Configurare i client LDAP per l'utilizzo di TLS
Si utilizzano protocolli orientati alla sessione?	Esaminare gli effetti negativi dei protocolli orientati alla sessione
La modalità SSL FIPS è abilitata su un cluster in cui gli account amministratore autenticano con una chiave pubblica SSH?	Verificare il supporto dell'algoritmo della chiave host SSH
La mia protezione autonoma da ransomware ha un avviso attivo?	Rispondi agli avvisi di protezione autonoma dal ransomware in caso di attività anomale

Verificare la compatibilità delle versioni di ONTAP per i cluster di versioni miste

In un cluster ONTAP versione mista, i nodi eseguono due diverse versioni principali di ONTAP per un breve periodo di tempo. Ad esempio, un cluster con nodi che eseguono ONTAP 9.8 e 9.12.1 o ONTAP 9.9.1 e 9.13.1 è una versione mista. I cluster con nodi che eseguono livelli di patch diversi all'interno della stessa versione, come ONTAP 9.9.1P1 e 9.9.1P5, non sono cluster di versioni miste.



I cluster di versioni miste non sono supportati per Cloud Volumes ONTAP.

NetApp supporta cluster ONTAP a versione mista per periodi di tempo limitati e in scenari specifici.

Di seguito sono riportati gli scenari più comuni in cui un cluster ONTAP sarà in uno stato di versione mista:

- Aggiornamenti del software ONTAP in cluster di grandi dimensioni

L'upgrade di tutti i nodi di un cluster di grandi dimensioni può richiedere diversi giorni o settimane. Il cluster entra e rimane in uno stato misto di versione fino all'upgrade di tutti i nodi.

- Gli aggiornamenti del software ONTAP sono necessari quando si prevede di aggiungere nuovi nodi a un cluster

È possibile aggiungere nuovi nodi al cluster per espanderne la capacità oppure aggiungere nuovi nodi durante il processo di sostituzione completa dei controller. In entrambi i casi, potrebbe essere necessario immettere uno stato di versione mista per consentire la migrazione dei dati dai controller esistenti ai nuovi nodi nel nuovo sistema.

Per un funzionamento ottimale del cluster, il tempo in cui il cluster si trova in uno stato di versione mista deve essere il più breve possibile. Il periodo di tempo massimo per cui un cluster è idoneo per il supporto in uno stato misto dipende dalla versione più bassa di ONTAP nel cluster.

Se la versione più bassa di ONTAP in esecuzione nel cluster di versioni miste è...	Quindi è possibile rimanere in uno stato di versione mista per un massimo di...
ONTAP 9.8 o versione successiva	90 giorni
ONTAP 9.7 o versioni precedenti	7 giorni

Mentre il cluster si trova in uno stato di versione mista, non inserire alcun comando che alteri l'operazione o la configurazione del cluster, ad eccezione di quelli richiesti per il processo di aggiornamento o di migrazione dei dati. Ad esempio, attività come la migrazione LIF (ma non solo), operazioni pianificate di failover dello storage o la creazione o l'eliminazione di oggetti su larga scala non devono essere eseguite fino al completamento dell'upgrade e della migrazione dei dati.

Cluster di versioni miste supportati per gli aggiornamenti software ONTAP

È possibile immettere uno stato di versione mista con qualsiasi versione di ONTAP supportata per un aggiornamento diretto dalla versione corrente più bassa. Ad esempio, se si esegue ONTAP 9.11.1, è possibile immettere uno stato di versione misto con i nodi che eseguono ONTAP 9.15.1. Non è possibile immettere uno stato di versione misto con i nodi che eseguono ONTAP 9.11.1 e ONTAP 9.16.1. ONTAP 9.16.1 non è supportato per l'aggiornamento diretto da ONTAP 9.11.1.



Le versioni delle patch (P) ONTAP non hanno alcun impatto sulla compatibilità con i cluster a versione mista. Ad esempio, se si utilizza ONTAP 9.11.1P6, la versione ONTAP corrente per la compatibilità con i cluster a versione mista è ONTAP 9.11.1. Oppure, se si utilizza ONTAP 9.12.1 e si desidera eseguire l'aggiornamento a ONTAP 9.15.1P2, la versione ONTAP di destinazione per la compatibilità con i cluster a versione mista è ONTAP 9.15.1.

Per eseguire l'aggiornamento a una versione di ONTAP non supportata per un aggiornamento diretto dalla versione corrente, è necessario eseguire un aggiornamento a più fasi. In un aggiornamento a più fasi, è necessario prima immettere uno stato di versione mista con la versione più alta supportata per un aggiornamento diretto dalla versione corrente. L'aggiornamento viene completato, quindi viene eseguito un aggiornamento separato alla versione di destinazione. Ad esempio, se la release corrente più bassa è ONTAP 9.10.1 e si desidera eseguire l'aggiornamento a ONTAP 9.16.1, è necessario immettere uno stato di versione mista per aggiornare tutti i nodi a ONTAP 9.14.1; quindi eseguire un aggiornamento separato da ONTAP 9.14.1 a ONTAP 9.16.1. Ulteriori informazioni su "[aggiornamenti multi-fase](#)" e "[percorsi di aggiornamento supportati](#)".

Un cluster di versioni miste può contenere solo due release principali di ONTAP. Ad esempio, puoi avere un cluster in versione mista con nodi che eseguono ONTAP 9.13.1 e 9.15.1 o con nodi che eseguono ONTAP 9.13.1 e 9.16.1. Non puoi avere un cluster in versione mista con nodi che eseguono ONTAP 9.13.1, 9.15.1 e 9.16.1.

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Lo stato della versione mista per l'aggiornamento è...
9.17.1	9.18.1	Supportato
9.16.1	9.18.1	Supportato
	9.17.1	Supportato
9.15.1	9.18.1	Supportato
	9.17.1	Supportato
	9.16.1	Supportato
9.14.1	9.18.1	Supportato
	9.17.1	Supportato
	9.16.1	Supportato
	9.15.1	Supportato
9.13.1	9.18.1	Non supportato
	9.17.1	Supportato
	9.16.1	Supportato
	9.15.1	Supportato
	9.14.1	Supportato

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Lo stato della versione mista per l'aggiornamento è...
9.12.1	9.17.1 o successivo	Non supportato
	9.16.1	Supportato
	9.15.1	Supportato
	9.14.1	Supportato
	9.13.1	Supportato
9.11.1	9.16.1 o versione successiva	Non supportato
	9.15.1	Supportato
	9.14.1	Supportato
	9.13.1	Supportato
	9.12.1	Supportato
9.10.1	9.15.1 o versione successiva	Non supportato
	9.14.1	Supportato
	9.13.1	Supportato
	9.12.1	Supportato
	9.11.1	Supportato
9.9.1	9.14.1 o successivo	Non supportato
	9.13.1	Supportato
	9.12.1	Supportato
	9.11.1	Supportato
	9.10.1	Supportato
9.8	9.13.1 o successivo	Non supportato
	9.12.1	Supportato
	9.11.1	Supportato
	9.10.1	Supportato
	9.9.1	Supportato

Aggiunta di nuovi nodi a un cluster ONTAP

Se si prevede di aggiungere nuovi nodi al cluster e tali nodi richiedono una versione minima di ONTAP successiva alla versione attualmente in esecuzione nel cluster, è necessario eseguire eventuali aggiornamenti software supportati sui nodi esistenti nel cluster prima di aggiungere i nuovi nodi. Idealmente, si dovrebbe aggiornare tutti i nodi esistenti alla versione minima di ONTAP richiesta dai nodi che si intende aggiungere al

cluster. Tuttavia, se questo non è possibile perché alcuni dei nodi esistenti non supportano la versione successiva di ONTAP, sarà necessario immettere uno stato di versione mista per un periodo di tempo limitato come parte del processo di aggiornamento.

Fasi

1. ["Eseguire l'upgrade"](#) i nodi che non supportano la versione ONTAP minima richiesta dai nuovi controller alla versione ONTAP più alta da loro supportata.

Ad esempio, se si dispone di un FAS8080 con ONTAP 9.5 e si sta aggiungendo una nuova piattaforma C-Series con ONTAP 9.12.1, è necessario aggiornare il FAS8080 a ONTAP 9.8 (che è la versione ONTAP più recente supportata).

2. ["Aggiungere i nuovi nodi al cluster"](#).
3. ["Migrare i dati"](#) dai nodi rimossi dal cluster ai nuovi nodi aggiunti.
4. ["Rimuovere i nodi non supportati dal cluster"](#).
5. ["Eseguire l'upgrade"](#) il cluster alla stessa versione ONTAP e livello di patch in esecuzione sui nuovi nodi o al ["ultima versione di patch consigliata"](#) per la versione ONTAP in esecuzione sui nuovi nodi.
6. Verificare che tutti i nodi eseguano la stessa versione ONTAP .

- a. Mostra la versione ONTAP in esecuzione sul cluster:

```
version
```

- b. Mostra la versione ONTAP in esecuzione su ciascun nodo del cluster:

```
version *
```

Se c'è una differenza tra la versione ONTAP riportata nell'output per il `version *` (gruppo) e `version` (singoli nodi) comandi, aggiorna tutti i nodi alla stessa versione ONTAP e patch eseguendo un ["aggiornamento dell'immagine del cluster"](#).

Per ulteriori informazioni sulla migrazione dei dati, consulta:

- ["Creare un aggregato e spostare i volumi nei nuovi nodi"](#)
- ["Impostazione di nuove connessioni iSCSI per gli spostamenti dei volumi SAN"](#)
- ["Spostamento di volumi con crittografia"](#)

Verificare i requisiti di aggiornamento di ONTAP per le configurazioni MetroCluster

Prima di aggiornare il software ONTAP su una configurazione MetroCluster, i cluster devono soddisfare determinati requisiti.

- Entrambi i cluster devono eseguire la stessa versione di ONTAP.

È possibile verificare la versione di ONTAP utilizzando il comando `version`.

- Se si sta eseguendo un aggiornamento ONTAP importante, la configurazione MetroCluster deve essere in modalità normale.
- Se si sta eseguendo un aggiornamento di patch ONTAP, la configurazione MetroCluster può essere in modalità normale o di switchover.
- Per tutte le configurazioni, ad eccezione dei cluster a due nodi, è possibile aggiornare entrambi i cluster senza interruzioni allo stesso tempo.

Per un upgrade senza interruzioni in cluster a due nodi, i cluster devono essere aggiornati un nodo alla volta.

- Gli aggregati in entrambi i cluster non devono trovarsi nello stato RAID di risyncing.

Durante la riparazione MetroCluster , gli aggregati speculari vengono risincronizzati. È possibile verificare se la configurazione MetroCluster è in questo stato utilizzando `storage aggregate plex show -in-progress true` comando. Se sono presenti aggregati in fase di sincronizzazione, non eseguire un aggiornamento finché la risincronizzazione non sarà completata.

Scopri di più su `storage aggregate plex show` nel "["Riferimento al comando ONTAP"](#)" .

- Le operazioni di switchover negoziate non avranno esito positivo durante l'aggiornamento.

Per evitare problemi con le operazioni di upgrade o revert, non tentare uno switchover non pianificato durante un'operazione di upgrade o revert, a meno che tutti i nodi su entrambi i cluster non eseguano la stessa versione di ONTAP.

Requisiti di configurazione per il normale funzionamento dell'MetroCluster

- I LIF SVM di origine devono essere attivi e posizionati sui nodi domestici.

Non è necessario che le LIF dei dati per le SVM di destinazione siano attive o che si trovino sui propri nodi domestici.

- Tutti gli aggregati del sito locale devono essere online.
- Tutti i volumi root e di dati di proprietà delle SVM del cluster locale devono essere online.

Requisiti di configurazione per lo switchover di MetroCluster

- Tutti i LIF devono essere attivi e posizionati sui propri nodi domestici.
- Tutti gli aggregati devono essere online, ad eccezione degli aggregati root del sito DR.

Gli aggregati root del sito DR sono offline durante alcune fasi di switchover.

- Tutti i volumi devono essere online.

Informazioni correlate

["Verifica dello stato di rete e storage per le configurazioni MetroCluster"](#)

Verificare la configurazione dell'host SAN prima di un aggiornamento ONTAP

L'aggiornamento di ONTAP in un ambiente SAN modifica i percorsi diretti. Prima di eseguire l'upgrade di un cluster SAN, occorre verificare che ogni host sia configurato con il numero corretto di percorsi diretti e indiretti e che ogni host sia connesso alle LIF corrette.

Fasi

1. Su ciascun host, verificare che sia configurato un numero sufficiente di percorsi diretti e indiretti e che ciascun percorso sia attivo.

Ciascun host deve disporre di un percorso per ciascun nodo del cluster.

2. Verificare che ciascun host sia connesso a una LIF su ciascun nodo.

È necessario registrare l'elenco degli iniziatori per il confronto dopo l'aggiornamento. Se si utilizza ONTAP 9.11.1 o versione successiva, utilizzare Gestione sistema per visualizzare lo stato della connessione in quanto fornisce una visualizzazione molto più chiara di CLI.

System Manager

- a. In System Manager, fare clic su **Hosts > SAN Initiator Groups** (host > gruppi iniziatori SAN).

Nella pagina viene visualizzato un elenco di gruppi di iniziatori (igroups). Se l'elenco è grande, è possibile visualizzare altre pagine dell'elenco facendo clic sui numeri di pagina nell'angolo inferiore destro della pagina.

Le colonne visualizzano varie informazioni su igroups. A partire da 9.11.1, viene visualizzato anche lo stato di connessione dell'igroup. Passare il mouse sugli avvisi di stato per visualizzare i dettagli.

CLI

- Elenca iniziatori iSCSI:

```
iscsi initiator show -fields igrp,initiator-name,tpgroup
```

- Elenca iniziatori FC:

```
fcp initiator show -fields igrp,wwpn,lif
```

SnapMirror

Versioni ONTAP compatibili per le relazioni SnapMirror

Prima di creare una relazione di data Protection SnapMirror, i volumi di origine e destinazione devono eseguire versioni di ONTAP compatibili. Prima di eseguire l'aggiornamento di ONTAP, devi verificare che la tua versione attuale di ONTAP sia compatibile con la tua versione di ONTAP di destinazione per le relazioni SnapMirror.

Relazioni di replica unificate

Per le relazioni SnapMirror di tipo “XDP”, utilizzando release on-premise o Cloud Volumes ONTAP:

A partire da ONTAP 9.9.0:

- Le release ONTAP 9.x,0 sono release solo per cloud e supportano i sistemi Cloud Volumes ONTAP. L'asterisco (*) dopo la versione della release indica una release solo cloud.



ONTAP 9.16.0 è un'eccezione alla regola del solo cloud perché fornisce supporto per "Sistemi ASA r2". Il segno più (+) dopo la versione di rilascio indica sia una versione supportata ASA r2 sia una versione supportata dal cloud. I sistemi ASA r2 supportano le relazioni SnapMirror solo con altri sistemi ASA r2.

- Le release ONTAP 9.x,1 sono release generali e supportano sistemi Cloud Volumes ONTAP e on-premise.



Quando "bilanciamento avanzato della capacità" è abilitato su volumi in cluster che eseguono ONTAP 9.16.1 o versione successiva, i trasferimenti SnapMirror non sono supportati ai cluster che eseguono versioni di ONTAP precedenti a ONTAP 9.16.1.



L'interoperabilità è bidirezionale.

Interoperabilità per ONTAP versione 9.4 e successive

Versione di ONTAP ...	Interagisce con queste versioni precedenti di ONTAP ...																				
	9.1 8.1	9.1 7.1	9.1 6.1	9.1 6.0	9.1 5.1	9.1 5.0	9.1 4.1	9.1 4.0	9.1 3.1	9.1 3.0	9.1 2.1	9.1 2.0	9.1 1.1	9.1 1.0	9.1 0.1	9.9 0.0	9.9 .1	9.8 .0*	9.7	9.6	9.5
9.1 8.1	Sì	Sì	Sì	Sì	Sì	No	Sì	No	Sì	Sì	No	No	No	No	No	No	No	No	No	No	
9.1 7.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No	No	No	No	
9.1 6.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No	No	No	

9.1 6.0 +	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No											
9.1 5.1	Sì	No	No	No	No	No																
9.1 5.0 *	No	Sì	Sì	No	Sì	Sì	Sì	No	No	No	No	No	No									
9.1 4.1	Sì	No	No	No	No	No																
9.1 4.0 *	No	Sì	Sì	No	Sì	No	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No	No	No	
9.1 3.1	Sì	No	No	No	No	No																
9.1 3.0 *	No	Sì	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No	
9.1 2.1	No	Sì	No	No	No																	
9.1 2.0 *	No	No	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì	Sì	No	No	No	
9.1 1.1	No	No	Sì	No																		
9.1 1.0 *	No	No	No	No	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	No								
9.1 0.1	No	No	No	Sì																		
9.1 0.0 *	No	No	No	No	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì									
9.9 .1	No	No	No	No	Sì																	
9.9 .0*	No	No	No	No	No	No	Sì	Sì	Sì	Sì	Sì											
9.8	No	Sì																				
9.7	No	Sì																				
9.6	No	Sì																				
9.5	No	Sì																				

Relazioni sincrone SnapMirror



La funzione sincrona SnapMirror non è supportata per le istanze cloud ONTAP.

Versi one di ONTA P...	Interagisce con queste versioni precedenti di ONTAP...														
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	
9.18.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No	No
9.17.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No	No
9.16.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No	No
9.15.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No
9.14.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No
9.13.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No
9.12.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No
9.11.1	No	No	Sì	Sì	Sì	No	No	No	No						
9.10.1	No	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No
9.9.1	No	No	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No
9.8	No	No	No	No	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No	No
9.7	No	No	No	No	No	Sì	Sì	No	No	Sì	Sì	Sì	Sì	Sì	Sì
9.6	No	No	No	No	No	No	No	No	No	No	Sì	Sì	Sì	Sì	Sì
9.5	No	No	No	No	No	No	No	No	No	No	No	No	Sì	Sì	Sì

Relazioni di disaster recovery di SnapMirror SVM



- Questa matrice si applica alla funzionalità di migrazione della mobilità dei dati SVM a partire da ONTAP 9.10.1.
- È possibile utilizzare SVM DR per migrare un SVM che non soddisfa le restrizioni indicate per ["Migrazione SVM \(mobilità dei dati SVM\)"](#).
- In entrambi i casi, un massimo di 2 versioni principali **più recenti** ONTAP possono separare i cluster di origine e di destinazione, con il requisito che la versione di destinazione sia la stessa o più recente della versione ONTAP di origine.

Per i dati di disaster recovery SVM e la protezione SVM:

Il disaster recovery delle SVM è supportato solo tra cluster che eseguono la stessa versione di ONTAP.
L'indipendenza dalla versione non è supportata per la replica SVM.

Per il disaster recovery SVM per la migrazione SVM:

- La replica è supportata in una singola direzione da una versione precedente di ONTAP sull'origine alla stessa o versione successiva di ONTAP sulla destinazione.
- La versione ONTAP nel cluster di destinazione non deve essere più di due versioni principali on-premise o

due versioni principali di cloud più recenti (a partire da ONTAP 9.9.0), come illustrato nella tabella seguente.

- La replica non è supportata per i casi di utilizzo a lungo termine della protezione dei dati.

L'asterisco (*) dopo la versione della release indica una release solo cloud.

Per determinare il supporto, individuare la versione di origine nella colonna della tabella a sinistra, quindi individuare la versione di destinazione nella riga superiore (DR/migrazione per le versioni simili e migrazione solo per le versioni più recenti).



Se si utilizza ONTAP 9.10.1 o versione successiva, è possibile utilizzare "["Mobilità dei dati SVM"](#)" funzionalità al posto di SVM DR per migrare le SVM da un cluster all'altro.

Ori gin e	Destinazione																					
	9.5	9.6	9.7	9.8	9.9 .0*	9.9 .1	9.1 0.0	9.1 0.1	9.1 1.0	9.1 1.1	9.1 2.0	9.1 2.1	9.1 3.0	9.1 3.1	9.1 4.0	9.1 4.1	9.1 4.1	9.1 5.0	9.1 5.1	9.1 6.0	9.1 6.1	9.1 7.1
9.5	Dr/ mig razi on on e	Mig razi on on e	Mig razi on on e																			
9.6		Dr/ mig razi on on e	Mig razi on on e	Mig razi on on e																		
9.7			Dr/ mig razi on on e	Mig razi on on e	Mig razi on on e																	
9.8				Dr/ mig razi on on e	Mig razi on on e	Mig razi on on e		Mig razi on on e														
9.9 .0*					Dr/ mig razi on on e	Mig razi on on e	Mig razi on on e	Mig razi on on e	Mig razi on on e	Mig razi on on e												
9.9 .1						Dr/ mig razi on on e	Mig razi on on e	Mig razi on on e	Mig razi on on e	Mig razi on on e												

9.1 0.0 *					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 0.1					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 1.0 *					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 1.1					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 2.0 *					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 2.1					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 3.0 *					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 3.1					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									
9.1 4.0 *					Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e									

9.1 4.1							Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	
9.1 5.0 *							Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	
9.1 5.1							Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	
9.1 6.0							Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	
9.1 6.1							Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	
9.1 7.1							Dr/ mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	Mig razi on e	
9.1 8.1							Dr/ mig razi on e					Dr/ mig razi on e

Relazioni di disaster recovery di SnapMirror

Per le relazioni SnapMirror di tipo “DP” e di tipo di policy “async-mirror”:



I mirror di tipo DP non possono essere inizializzati a partire da ONTAP 9.11.1 e sono completamente deprecati in ONTAP 9.12.1. Per ulteriori informazioni, vedere ["Deprecazione delle relazioni SnapMirror per la protezione dei dati"](#).



Nella tabella seguente, la colonna a sinistra indica la versione di ONTAP sul volume di origine, mentre la riga superiore indica le versioni di ONTAP disponibili sul volume di destinazione.

Origine	Destinazione
---------	--------------

	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	Sì	No	No	No	No	No	No	No	No
9.10.1	Sì	Sì	No	No	No	No	No	No	No
9.9.1	Sì	Sì	Sì	No	No	No	No	No	No
9.8	No	Sì	Sì	Sì	No	No	No	No	No
9.7	No	No	Sì	Sì	Sì	No	No	No	No
9.6	No	No	No	Sì	Sì	Sì	No	No	No
9.5	No	No	No	No	Sì	Sì	Sì	No	No
9.4	No	No	No	No	No	Sì	Sì	Sì	No
9.3	No	No	No	No	No	No	Sì	Sì	Sì



L'interoperabilità non è bidirezionale.

Convertire una relazione di tipo ONTAP SnapMirror DP esistente in XDP

Se si esegue l'aggiornamento a ONTAP 9.12.1 o versioni successive, è necessario convertire le relazioni di tipo DP in XDP prima di eseguire l'aggiornamento. ONTAP 9.12.1 e versioni successive non supportano le relazioni di tipo DP. È possibile convertire facilmente una relazione di tipo DP esistente in XDP per sfruttare SnapMirror flessibile in versione.

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.

A proposito di questa attività

- SnapMirror non converte automaticamente le relazioni di tipo DP esistenti in XDP. Per convertire la relazione, è necessario interrompere ed eliminare la relazione esistente, creare una nuova relazione XDP e risincronizzare la relazione.
- Durante la pianificazione della conversione, è necessario tenere presente che la preparazione in background e la fase di data warehousing di una relazione SnapMirror XDP possono richiedere molto tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.



Dopo aver convertito un tipo di relazione SnapMirror da DP a XDP, le impostazioni relative allo spazio, come la dimensione automatica e la garanzia dello spazio, non vengono più replicate nella destinazione.

Fasi

1. Dal cluster di destinazione, assicurarsi che la relazione SnapMirror sia di tipo DP, che lo stato del mirror sia SnapMirrored, che lo stato della relazione sia inattivo e che la relazione sia integra:

```
snapmirror show -destination-path <SVM:volume>
```

L'esempio seguente mostra l'output di `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Potrebbe essere utile conservare una copia dell'output del `snapmirror show` comando per tenere traccia delle impostazioni di relazione esistenti. Ulteriori informazioni su `snapmirror show` nella "[Riferimento al comando ONTAP](#)".

2. Dai volumi di origine e di destinazione, verificare che entrambi i volumi abbiano uno snapshot comune:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Nell'esempio riportato di seguito viene illustrato il `volume snapshot show` output per i volumi di origine e di destinazione:

```

cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.

```

```

cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026

```

3. Per garantire che gli aggiornamenti pianificati non vengano eseguiti durante la conversione, interrompere la relazione DP-type esistente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path  
<SVM:volume>
```



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene meno la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Ulteriori informazioni su `snapmirror quiesce` nella ["Riferimento al comando ONTAP"](#).

4. Interrompere la relazione di tipo DP esistente:

```
snapmirror break -destination-path <SVM:volume>
```



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene spezzata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Ulteriori informazioni su `snapmirror break` nella ["Riferimento al comando ONTAP"](#).

5. Se l'eliminazione automatica degli snapshot è attivata sul volume di destinazione, disattivarla:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_  
-enabled false
```

Nell'esempio seguente viene disattivata l'eliminazione automatica dello snapshot sul volume di destinazione `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup  
-volume volA_dst -enabled false
```

6. Eliminare la relazione DP-type esistente:

```
snapmirror delete -destination-path <SVM:volume>
```

Ulteriori informazioni su snapmirror-delete nella "[Riferimento al comando ONTAP](#)".



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio riportato di seguito viene eliminata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Rilasciare la relazione di disaster recovery della SVM di origine sull'origine:

```
snapmirror release -destination-path <SVM:volume> -relationship-info  
-only true
```

L'esempio seguente rilascia la relazione di disaster recovery della SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst  
-relationship-info-only true
```

Ulteriori informazioni su snapmirror release nella "[Riferimento al comando ONTAP](#)".

8. È possibile utilizzare l'output conservato da snapmirror show Comando per creare la nuova relazione XDP-type:

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nuova relazione deve utilizzare lo stesso volume di origine e di destinazione. Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "[Riferimento al comando ONTAP](#)".



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

L'esempio seguente crea una relazione di disaster recovery SnapMirror tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup` utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst  
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Per migliorare il tempo di risincronizzazione, puoi utilizzare `-quick-resync` opzione, ma bisogna essere consapevoli che i risparmi in termini di efficienza di archiviazione potrebbero andare persi.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

Scopri di più su `snapmirror resync` nel "[Riferimento al comando ONTAP](#)".

10. Se è stata disattivata l'eliminazione automatica degli snapshot, riattivarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

Al termine

1. Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror.

Ulteriori informazioni su `snapmirror show` nella "[Riferimento al comando ONTAP](#)".

2. Quando il volume di destinazione SnapMirror XDP inizia ad aggiornare gli snapshot come definito dal criterio SnapMirror, utilizzare l'output del `snapmirror list-destinations` comando dal cluster di origine per visualizzare la nuova relazione SnapMirror XDP.

Ulteriori informazioni sulle relazioni di tipo DP

A partire da ONTAP 9,3, la modalità XDP è quella predefinita e tutte le chiamate della modalità DP sulla riga di comando o negli script nuovi o esistenti vengono convertite automaticamente 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 criterio predefinito quando non è specificata alcuna modalità di protezione dei dati o quando la modalità XDP è specificata come tipo di relazione. La tabella seguente mostra

il comportamento previsto.

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 illustrato nella tabella, i criteri predefiniti assegnati a XDP in circostanze diverse 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.

Informazioni correlate

- "creazione di snapmirror"
- "eliminazione di snapmirror"
- "snapmirror quiesce"
- "versione di snapmirror"
- "risincronizzazione snapmirror"

Disattiva gli snapshot di conservazione a lungo termine prima dell'aggiornamento di ONTAP

In una relazione di volumi a cascata, gli snapshot di conservazione a lungo termine sono supportati solo sul volume di destinazione SnapMirror finale della cascata in tutte le versioni di ONTAP 9. L'abilitazione di snapshot di conservazione a lungo termine su qualsiasi volume intermedio nella cascata comporta la perdita di backup e snapshot.

Scopri di più su "[snapshot di conservazione a lungo termine](#)" .

Se si dispone di una configurazione non supportata in cui gli snapshot di conservazione a lungo termine sono stati abilitati su un volume intermedio di una cascata, contattare l'assistenza tecnica e fare riferimento al collegamento: [https://kb.netapp.com/on-prem/ontap/DP/SnapMirror/SnapMirror-KBs/Cascading_a_volume_with_Long-Term_Retention_\(long-term_retention\)_snapshots_enabled_is_not_supported](https://kb.netapp.com/on-prem/ontap/DP/SnapMirror/SnapMirror-KBs/Cascading_a_volume_with_Long-Term_Retention_(long-term_retention)_snapshots_enabled_is_not_supported)[NetApp Knowledge Base: La cascata di un volume con snapshot di conservazione a lungo termine (LTR) abilitati non è supportata^] per assistenza.

Le seguenti versioni ONTAP non consentono di abilitare snapshot di conservazione a lungo termine su alcun volume in una cascata, ad eccezione del volume di destinazione SnapMirror finale.

- 9.15.1 e versioni successive
- 9.14.1P2 e P4 fino a P14
- 9.13.1P9 attraverso P17
- 9.12.1 P12 attraverso P19
- 9.11.1P15 attraverso P20
- 9.10.1P18 attraverso P20
- 9.9.1P20

Prima di eseguire l'aggiornamento da una versione ONTAP che consente di abilitare snapshot di conservazione a lungo termine sui volumi intermedi di una cascata a una versione ONTAP che lo blocca, è necessario disabilitare gli snapshot di conservazione a lungo termine per evitare backup e snapshot persi.

È necessario intervenire nei seguenti scenari:

- Gli snapshot di conservazione a lungo termine vengono configurati sul volume "B" in una cascata SnapMirror **A** → **B** → **C** o su un altro volume di destinazione SnapMirror intermedio nella cascata più grande.
- gli snapshot di conservazione a lungo termine sono definiti da una pianificazione applicata a una regola di policy SnapMirror . Questa regola non replica gli snapshot dal volume di origine, ma li crea direttamente sul volume di destinazione.



Per ulteriori informazioni sulle pianificazioni e sulle policy SnapMirror , vedere "[NetApp Knowledge Base: come funziona il parametro "schedule" in una regola di policy ONTAP 9 SnapMirror ?](#)" .

Fasi

1. Rimuovere la regola di conservazione a lungo termine dalla policy SnapMirror sul volume centrale della cascata:

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>  
-snapmirror-label <>
```

Scopri di più su `snapmirror policy remove-rule` nel "["Riferimento al comando ONTAP"](#)" .

2. Aggiungere nuovamente la regola per l'etichetta SnapMirror senza la pianificazione di conservazione a lungo termine:

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>  
-snapmirror-label <> -keep <>
```



La rimozione degli snapshot di conservazione a lungo termine dalle regole dei criteri di SnapMirror significa che SnapMirror estrarrà gli snapshot con l'etichetta specificata dal volume di origine. Potrebbe anche essere necessario aggiungere o modificare una pianificazione nella policy di snapshot del volume di origine per creare snapshot correttamente etichettati.

Ulteriori informazioni su `snapmirror policy add-rule` nella "["Riferimento al comando ONTAP"](#)" .

3. Se necessario, modificare (o creare) una pianificazione nel policy di snapshot del volume di origine per consentire la creazione di snapshot con un'etichetta SnapMirror:

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>  
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>  
-schedule <> -snapmirror-label <> -count <>
```



gli snapshot di conservazione a lungo termine possono comunque essere abilitati sul volume di destinazione SnapMirror finale all'interno di una configurazione a cascata SnapMirror .

Verifica della licenza ONTAP per le configurazioni di SnapMirror S3

Prima di aggiornare ONTAP, se si utilizza SnapMirror S3 e si sta eseguendo l'aggiornamento a ONTAP 9.12,1 o versioni successive, è necessario verificare di disporre delle licenze SnapMirror corrette.

Dopo l'aggiornamento di ONTAP, le modifiche apportate alle licenze tra ONTAP 9.11,1 e versioni precedenti e ONTAP 9.12,1 e versioni successive potrebbero causare un errore nelle relazioni di SnapMirror S3.

ONTAP 9.11.1 e versioni precedenti

- Durante la replica su un bucket di destinazione ospitato da NetApp (ONTAP S3 o StorageGRID), SnapMirror S3 verifica la licenza sincrona SnapMirror, inclusa nel bundle di data Protection prima dell'introduzione della "[ONTAP uno](#)"suite software.
- Durante la replica su un bucket di destinazione non NetApp, SnapMirror S3 verifica la licenza cloud SnapMirror, inclusa nel bundle di cloud ibrido, disponibile prima dell'introduzione della "[ONTAP uno](#)"suite software.

ONTAP 9.12.1 e versioni successive

- Durante la replica su un bucket di destinazione ospitato da NetApp (ONTAP S3 o StorageGRID), SnapMirror S3 verifica la licenza di SnapMirror S3, incluso nel bundle di data Protection, disponibile prima dell'introduzione della "[ONTAP uno](#)"suite software.
- Quando si esegue la replica su un bucket di destinazione non NetApp, SnapMirror S3 controlla la licenza SnapMirror S3 External, inclusa nel bundle cloud ibrido, disponibile prima dell'introduzione della "[ONTAP uno](#)"suite software e di "[Pacchetto di compatibilità ONTAP One](#)".

Relazioni esistenti con SnapMirror S3

Le relazioni esistenti di SnapMirror S3 devono continuare a funzionare anche dopo un upgrade da ONTAP 9.11,1 o versione precedente a ONTAP 9.12,1 o versione successiva, anche se il cluster non dispone della nuova licenza.

La creazione di nuove relazioni di SnapMirror S3 non riesce se il cluster non dispone della licenza corretta installata.

Eliminare le connessioni al server di gestione chiavi esterno esistenti prima di aggiornare ONTAP

Prima di eseguire l'upgrade di ONTAP, se si esegue ONTAP 9,2 o versione precedente con crittografia dello storage NetApp (NSE) ed eseguire l'aggiornamento a ONTAP 9,3 o versione successiva, è necessario utilizzare l'interfaccia a riga di comando (CLI) per eliminare qualsiasi connessione server di gestione delle chiavi esterna (KMIP) esistente.

Fasi

1. Verificare che le unità NSE siano sbloccate, aperte e impostate sull'ID protetto predefinito 0x0:

```
storage encryption disk show -disk *
```

Ulteriori informazioni su `storage encryption disk show` nella "[Riferimento al comando ONTAP](#)".

2. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

Ulteriori informazioni su `set` nella "[Riferimento al comando ONTAP](#)".

3. Utilizzare l'ID protetto predefinito 0x0 per assegnare la chiave FIPS ai dischi con crittografia automatica (SED):

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

Ulteriori informazioni su `storage encryption disk modify` nella "[Riferimento al comando ONTAP](#)".

4. Verificare che l'assegnazione della chiave FIPS a tutti i dischi sia completata:

```
storage encryption disk show-status
```

Ulteriori informazioni su `storage encryption disk show-status` nella "[Riferimento al comando ONTAP](#)".

5. Verificare che la **modalità** per tutti i dischi sia impostata su dati

```
storage encryption disk show
```

Ulteriori informazioni su `storage encryption disk show` nella "[Riferimento al comando ONTAP](#)".

6. Visualizzare i server KMIP configurati:

```
security key-manager keystore show
```

Scopri di più su `security key-manager keystore show` nel "[Riferimento al comando ONTAP](#)".

7. Eliminare i server KMIP configurati:

```
security key-manager delete -address <kmip_ip_address>
```

Ulteriori informazioni su `security key-manager delete` nella "[Riferimento al comando ONTAP](#)".

8. Eliminare la configurazione del gestore delle chiavi esterno:

```
security key-manager external disable
```

Scopri di più su `security key-manager external disable` nel "[Riferimento al comando ONTAP](#)".



Questo passaggio non rimuove i certificati NSE.

Cosa succederà

Una volta completato l'aggiornamento, è necessario [Riconfigurare le connessioni del server KMIP](#).

Verificare che il file netgroup sia presente su tutti i nodi prima di un aggiornamento di ONTAP

Prima di eseguire l'upgrade di ONTAP, se sono stati caricati netgroup nelle Storage Virtual Machine (SVM), è necessario verificare la presenza del file netgroup in ciascun nodo. Un file netgroup mancante su un nodo può causare un errore di aggiornamento.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Visualizzare lo stato del netgroup per ogni SVM:

```
vserver services netgroup status
```

3. Verificare che per ogni SVM, ciascun nodo mostri lo stesso valore hash del file netgroup:

```
vserver services name-service netgroup status
```

In questo caso, è possibile saltare il passaggio successivo e procedere con l'aggiornamento o il ripristino. In caso contrario, passare alla fase successiva.

4. Su un nodo qualsiasi del cluster, caricare manualmente il file netgroup:

```
vserver services netgroup load -vserver vserver_name -source uri
```

Questo comando scarica il file netgroup su tutti i nodi. Se un file netgroup esiste già su un nodo, viene sovrascritto.

Informazioni correlate

Assegnare un valore esplicito all'opzione v4.2-xattrs prima di un aggiornamento di ONTAP

Se si dispone di un client NFSv4,2, prima di eseguire l'aggiornamento da determinate release e patch di ONTAP 9.12,1 e versioni successive è necessario fornire un valore esplicito per l'opzione attributi estesi NFSv4,2 per evitare errori di risposta NFS dopo l'aggiornamento.

Se all' `v4.2-xattrs` opzione non viene mai assegnato esplicitamente un valore prima dell'aggiornamento di ONTAP alle versioni interessate, i client NFSv4,2 non vengono informati della modifica dell'opzione attributi estesi del server. Ciò causa errori di risposta NFS a chiamate specifiche `xattrs` a causa di una mancata corrispondenza tra client e server.

Prima di iniziare

È necessario assegnare un valore esplicito per l'opzione NFSv4,2 attributi estesi se è vero quanto segue:

- Stai utilizzando NFSv4,2 con una SVM creata utilizzando ONTAP 9.11,1 o una versione precedente
- Si sta eseguendo l'aggiornamento di ONTAP da una delle seguenti release e patch interessate:
 - Da 9.12.1RC1 a 9.12.1P11
 - Da 9.13.1RC1 a 9.13.1P8
 - Da 9.14.1RC1 a 9.14.1P1

A proposito di questa attività

È necessario eseguire ONTAP 9.12,1 o versioni successive per impostare il valore utilizzando il comando descritto in questa procedura.

Se `v4.2-xattrs` è già impostato su `enabled`, deve essere impostato esplicitamente su `enabled` per evitare interruzioni future. Se si imposta `v4.2-xattrs` su disattivato, i client NFSv4,2 possono ricevere risposte "argomento non valido" finché non vengono rimontati o l' `v4.2-xattrs` opzione è impostata su `enabled`.

Fasi

- Assegnare un valore esplicito all' `v4.2-xattrs` opzione:

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

Informazioni correlate

["Il campo NFS v4.2-xattrs viene capovolto dopo gli aggiornamenti"](#)

Configurare i client LDAP in modo che utilizzino TLS prima di un aggiornamento ONTAP

Prima di aggiornare ONTAP, è necessario configurare i client LDAP utilizzando SSLv3

per comunicazioni protette con i server LDAP per utilizzare TLS. SSL non sarà disponibile dopo l'aggiornamento.

Per impostazione predefinita, le comunicazioni LDAP tra applicazioni client e server non sono crittografate. È necessario non consentire l'utilizzo di SSL e imporre l'utilizzo di TLS.

Fasi

1. Verificare che i server LDAP nel proprio ambiente supportino TLS.

In caso contrario, non procedere. È necessario aggiornare i server LDAP a una versione che supporti TLS.

2. Controllare quali configurazioni del client LDAP ONTAP hanno abilitato LDAP su SSL/TLS:

```
vserver services name-service ldap client show
```

In caso contrario, è possibile saltare i passaggi rimanenti. Tuttavia, è consigliabile utilizzare LDAP su TLS per una maggiore sicurezza.

3. Per ogni configurazione del client LDAP, non consentire a SSL di imporre l'utilizzo di TLS:

```
vserver services name-service ldap client modify -vserver <vserver_name>
-client-config <ldap_client_config_name> -allow-ssl false
```

4. Verificare che l'utilizzo di SSL non sia più consentito per i client LDAP:

```
vserver services name-service ldap client show
```

Informazioni correlate

["Gestione NFS"](#)

Scopri gli effetti negativi dei protocolli orientati alla sessione durante gli aggiornamenti ONTAP

I cluster e i protocolli orientati alle sessioni possono causare effetti negativi su client e applicazioni in determinate aree, come il servizio i/o durante gli aggiornamenti.

Se si utilizzano protocolli orientati alla sessione, considerare quanto segue:

- PMI

Se si utilizzano condivisioni CA (Continuously Available) con SMBv3, è possibile utilizzare il metodo di aggiornamento automatico senza interruzioni (con System Manager o CLI) e il client non subiva alcuna interruzione.

Se si forniscono condivisioni con SMBv1 o SMBv2 o condivisioni non CA con SMBv3, le sessioni client vengono interrotte durante le operazioni di takeover e reboot dell'upgrade. Gli utenti devono terminare le sessioni prima di eseguire l'aggiornamento.

Hyper-V e SQL Server su SMB supportano operazioni senza interruzioni (NDOS). Se è stata configurata una soluzione Hyper-V o SQL Server su SMB, i server delle applicazioni e le macchine virtuali o i database contenuti rimangono online e garantiscono una disponibilità continua durante l'aggiornamento di ONTAP.

- NFSv4.x

I client NFSv4.x ripristineranno automaticamente le perdite di connessione riscontrate durante l'aggiornamento utilizzando le normali procedure di ripristino NFSv4.x. Durante questo processo, le applicazioni potrebbero riscontrare un ritardo i/O.

- NDMP

Lo stato viene perso e l'utente client deve riprovare l'operazione.

- Backup e ripristini

Lo stato viene perso e l'utente client deve riprovare l'operazione.



Non avviare un backup o un ripristino durante o immediatamente prima di un aggiornamento. Ciò potrebbe causare la perdita di dati.

- Applicazioni (ad esempio, Oracle o Exchange)

Gli effetti dipendono dalle applicazioni. Per le applicazioni basate sul timeout, potrebbe essere possibile modificare l'impostazione del timeout su un tempo superiore al tempo di riavvio di ONTAP per ridurre al minimo gli effetti negativi.

Verificare il supporto dell'algoritmo della chiave host SSH prima dell'aggiornamento di ONTAP

Prima di aggiornare ONTAP, se la modalità SSL FIPS è attivata su un cluster in cui gli account amministratore si autenticano con una chiave pubblica SSH, è necessario assicurarsi che l'algoritmo della chiave host sia supportato nella versione ONTAP di destinazione.

La seguente tabella indica gli algoritmi del tipo di chiave host supportati per le connessioni SSH ONTAP. Questi tipi di chiave non si applicano alla configurazione dell'autenticazione pubblica SSH.

Release di ONTAP	Tipi di chiave supportati in modalità FIPS	Tipi di chiave supportati in modalità non FIPS
9.11.1 e versioni successive	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa



Il supporto per l'algoritmo della chiave host ssh-ed25519 viene rimosso a partire da ONTAP 9.11.1.

Per ulteriori informazioni, vedere "[Configurare la sicurezza di rete utilizzando FIPS](#)".

Gli account a chiave pubblica SSH esistenti senza gli algoritmi a chiave supportati devono essere riconfigurati con un tipo di chiave supportato prima di eseguire l'aggiornamento, altrimenti l'autenticazione dell'amministratore avrà esito negativo.

"[Scopri di più sull'abilitazione degli account a chiave pubblica SSH.](#)"

Risolvi gli avvisi delle attività nella protezione autonoma dal ransomware (ARP) prima di un upgrade ONTAP

Prima di eseguire l'aggiornamento a ONTAP 9.16,1 o versione successiva, dovresti rispondere a qualsiasi avviso di attività anomala segnalato dalla protezione autonoma dal ransomware (ARP). In ONTAP 9.16,1, ARP è cambiato in un modello basato su apprendimento automatico/intelligenza artificiale (ai). A causa di questa modifica, tutti gli avvisi attivi non risolti provenienti dall'ARP esistente in ONTAP 9.15,1 o versioni precedenti andranno persi dopo l'aggiornamento.

Fasi

1. Rispondere a eventuali avvisi di attività anomala segnalati da "[ARP](#)" e risolvere eventuali problemi potenziali.
2. Confermare la risoluzione di questi problemi prima dell'aggiornamento selezionando **Aggiorna e Cancella tipi di file sospetti** per registrare la decisione e riprendere il normale monitoraggio ARP.

Informazioni sul copyright

Copyright © 2026 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 COMMERCIALITÀ 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.