



# **Panoramica del prodotto**

## **SnapManager Oracle**

NetApp

October 04, 2023

This PDF was generated from [https://docs.netapp.com/it-it/snapmanager-oracle/unix-administration/concept\\_create\\_backups\\_using\\_snapshot\\_copies.html](https://docs.netapp.com/it-it/snapmanager-oracle/unix-administration/concept_create_backups_using_snapshot_copies.html) on October 04, 2023. Always check docs.netapp.com for the latest.

# Sommario

- Panoramica del prodotto ..... 1
  - Punti salienti di SnapManager ..... 1
  - Creare backup utilizzando copie Snapshot ..... 1
  - Perché è necessario ridurre i file di log dell'archivio ..... 2
  - Consolidamento dei log di archiviazione ..... 2
  - Ripristino completo o parziale dei database ..... 2
  - Verificare lo stato del backup ..... 3
  - Cloni di backup del database ..... 3
  - Tieni traccia dei dettagli e genera report ..... 4
  - Quali repository sono ..... 4
  - Quali sono i profili ..... 5
  - Quali sono gli stati operativi di SnapManager ..... 6
  - In che modo SnapManager mantiene la sicurezza ..... 7
  - Accesso e stampa della Guida in linea ..... 8
  - Layout generali del database e configurazioni di storage consigliati ..... 9
  - Limitazioni quando si lavora con SnapManager ..... 21

# Panoramica del prodotto

SnapManager per Oracle automatizza e semplifica i processi complessi, manuali e lunghi associati al backup, al ripristino e alla clonazione dei database Oracle. È possibile utilizzare SnapManager con la tecnologia SnapMirror di ONTAP per creare copie dei backup su un altro volume e con la tecnologia ONTAP SnapVault per archiviare i backup su disco in modo efficiente.

SnapManager si integra con le tecnologie Oracle native come Oracle Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) e Direct NFS su protocolli FC, iSCSI e NFS. Facoltativamente, i backup creati utilizzando SnapManager possono essere catalogati con Oracle Recovery Manager (RMAN) per conservare le informazioni di backup; questi backup possono essere utilizzati in un secondo momento nelle operazioni di ripristino a livello di blocco o tablespace point-in-time.

## Punti salienti di SnapManager

SnapManager offre un'integrazione perfetta con i database Oracle sull'host UNIX e con le tecnologie NetApp Snapshot, SnapRestore e FlexClone sul back-end. Offre un'interfaccia utente (UI) di facile utilizzo e un'interfaccia a riga di comando (CLI) per le funzioni amministrative.

SnapManager consente di eseguire le seguenti operazioni di database e gestire i dati in modo efficiente:

- Creazione di backup efficienti in termini di spazio sullo storage primario o secondario

È possibile eseguire il backup dei file di dati e archiviare i file di log separatamente.

- Pianificazione dei backup
- Ripristino di database completi o parziali mediante un'operazione di ripristino basata su file o volume
- Ripristino dei database mediante il rilevamento, il montaggio e l'applicazione dei file di log di archiviazione dai backup
- Eliminazione dei file di log dell'archivio dalle destinazioni dei log dell'archivio durante la creazione di backup dei soli log dell'archivio
- Conservazione automatica di un numero minimo di backup del log di archiviazione mantenendo solo i backup che contengono file di log di archiviazione univoci
- Monitoraggio dei dettagli delle operazioni e generazione di report
- Verifica dei backup per garantire che i backup siano in un formato a blocchi valido e che nessuno dei file di backup sia corrotto
- Mantenere una cronologia delle operazioni eseguite sul profilo del database

Un profilo contiene informazioni sul database che deve essere gestito da SnapManager.

- Creazione di cloni di backup efficienti in termini di spazio su sistemi storage primari o secondari

SnapManager consente di suddividere un clone di un database.

## Creare backup utilizzando copie Snapshot

SnapManager consente di creare backup sullo storage primario (locale) e sullo storage

secondario (remoto) utilizzando policy di protezione o script di post-elaborazione.

I backup creati come copie Snapshot sono copie virtuali del database e vengono memorizzati nello stesso supporto fisico del database. Pertanto, l'operazione di backup richiede meno tempo e richiede molto meno spazio rispetto ai backup disk-to-disk completi. SnapManager consente di eseguire il backup di quanto segue:

- Tutti i file di dati, i file di log di archiviazione e i file di controllo
- File di dati o tablespace selezionati, tutti i file di log dell'archivio e i file di controllo

SnapManager 3.2 o versione successiva consente di eseguire il backup opzionale dei seguenti elementi:

- Tutti i file di dati e i file di controllo
- File di dati o tablespace selezionati insieme ai file di controllo
- Archiviare i file di log



I file di dati, i file di log dell'archivio e i file di controllo possono essere posizionati su diversi sistemi di storage, volumi del sistema di storage o LUN (Logical Unit Number). È inoltre possibile utilizzare SnapManager per eseguire il backup di un database quando sono presenti più database sullo stesso volume o LUN.

## Perché è necessario ridurre i file di log dell'archivio

SnapManager per Oracle consente di eliminare i file di log dell'archivio dal file system attivo di cui è già stato eseguito il backup.

L'eliminazione consente a SnapManager di creare backup di file di log di archivio distinti. L'eliminazione, insieme alla policy di conservazione del backup, libera spazio nel log di archiviazione quando i backup vengono eliminati.



Non è possibile eseguire l'eliminazione dei file di log dell'archivio quando Flash Recovery Area (fra) è abilitata per i file di log dell'archivio. Se si specifica la posizione del registro di archiviazione nell'area di ripristino flash, è necessario specificare anche la posizione del registro di archiviazione nel parametro `archive_log_dest`.

## Consolidamento dei log di archiviazione

SnapManager (3.2 o versioni successive) per Oracle consolida i backup dei log di archiviazione per mantenere un numero minimo di backup per i file di log di archiviazione. SnapManager per Oracle identifica e libera i backup che contengono file di log di archivio che sono sottoinsiemi di altri backup.

## Ripristino completo o parziale dei database

SnapManager offre la flessibilità necessaria per ripristinare database completi, spazi tabella specifici, file, file di controllo o una combinazione di queste entità. SnapManager consente di ripristinare i dati utilizzando un processore di ripristino basato su file, un processo di ripristino più rapido e basato su volume. Gli amministratori del database possono selezionare il processo che desiderano utilizzare o lasciare che SnapManager

decida quale processo è appropriato.

SnapManager consente agli amministratori di database (DBA) di visualizzare in anteprima le operazioni di ripristino. La funzione di anteprima consente ai DBA di visualizzare ogni operazione di ripristino file per file.

I DBA possono specificare il livello di ripristino e ripristino delle informazioni da parte di SnapManager durante le operazioni di ripristino. Ad esempio, i DBA possono ripristinare e ripristinare i dati in punti specifici nel tempo. Il punto di ripristino può essere una data e un'ora o un numero SCN (System Change Number) Oracle.

I DBA possono utilizzare SnapManager per ripristinare il database e un altro strumento per recuperare le informazioni. I DBA non sono richiesti per utilizzare SnapManager per entrambe le operazioni.

SnapManager (3.2 o versione successiva) consente di ripristinare e ripristinare automaticamente i backup del database senza l'intervento di DBA. È possibile utilizzare SnapManager per creare backup del registro di archiviazione e utilizzarli per ripristinare e ripristinare i backup del database. Anche se i file di log dell'archivio del backup sono gestiti in una posizione di log dell'archivio esterna, è possibile specificare la posizione esterna in modo che i log dell'archivio possano aiutare a ripristinare il database ripristinato.

## Verificare lo stato del backup

SnapManager può confermare l'integrità del backup utilizzando le operazioni di verifica del backup standard di Oracle.

Gli amministratori di database (DBA) possono eseguire la verifica come parte dell'operazione di backup o in un altro momento. I DBA possono impostare l'operazione di verifica in modo che venga eseguita durante un periodo di tempo non di punta quando il carico sui server host è inferiore o durante una finestra di manutenzione pianificata.

## Cloni di backup del database

SnapManager utilizza la tecnologia FlexClone per creare un clone scrivibile ed efficiente in termini di spazio di un backup del database. È possibile modificare un clone senza modificare l'origine del backup.

È possibile clonare i database per consentire test o aggiornamenti in ambienti non di produzione. È possibile clonare un database che risiede nello storage primario o secondario. Un clone può trovarsi sullo stesso host o su un host diverso del database.

La tecnologia FlexClone consente a SnapManager di utilizzare le copie Snapshot del database per evitare di creare un'intera copia fisica da disco a disco. Le copie Snapshot richiedono meno tempo di creazione e occupano molto meno spazio rispetto alle copie fisiche.

Per ulteriori informazioni sulla tecnologia Data ONTAP, consultare la documentazione di FlexClone.

### Informazioni correlate

"Data ONTAP documentation:

[mysupport.netapp.com/documentation/productsatoz/index.html](https://mysupport.netapp.com/documentation/productsatoz/index.html)"

# Tieni traccia dei dettagli e genera report

SnapManager riduce il livello di dettaglio necessario agli amministratori dei database per tenere traccia dello stato delle diverse operazioni offrendo metodi per monitorare le operazioni da una singola interfaccia.

Dopo che gli amministratori hanno specificato quali database devono essere sottoposti a backup, SnapManager identifica automaticamente i file di database per il backup. SnapManager visualizza informazioni su repository, host, profili, backup e cloni. È possibile monitorare le operazioni su host o database specifici. È inoltre possibile identificare i backup protetti e determinare se i backup sono in corso o pianificati per essere eseguiti.

## Quali repository sono

SnapManager organizza le informazioni in profili, che vengono quindi associati ai repository. I profili contengono informazioni sul database gestito, mentre il repository contiene dati sulle operazioni eseguite sui profili.

Il repository registra quando è stato eseguito un backup, quali file sono stati sottoposti a backup e se è stato creato un clone dal backup. Quando gli amministratori del database ripristinano un database o ne ripristinano una parte, SnapManager esegue una query nel repository per determinare il backup.

Poiché il repository memorizza i nomi delle copie Snapshot del database create durante le operazioni di backup, il database del repository non può esistere nello stesso database e non può far parte dello stesso database di cui SnapManager esegue il backup. Quando si eseguono le operazioni SnapManager, è necessario disporre di almeno due database (il database del repository SnapManager e il database di destinazione gestito da SnapManager) attivi e attivi.

Se si tenta di aprire l'interfaccia grafica utente (GUI) quando il database del repository non è attivo, viene registrato il seguente messaggio di errore nel file `sm_gui.log`: [WARN]: SMO-01106: Errore durante la query del repository: Nessun altro dato da leggere dal socket. Inoltre, le operazioni SnapManager non riescono quando il database del repository non è attivo. Per ulteriori informazioni sui diversi messaggi di errore, consulta la sezione *risoluzione dei problemi noti*.

Per eseguire le operazioni, è possibile utilizzare un nome host, un nome di servizio o un nome utente valido. Affinché un repository supporti le operazioni SnapManager, il nome utente e il nome del servizio del repository devono essere composti solo dai seguenti caratteri: Caratteri alfabetici (A-Z), cifre (0-9), segno meno (-), carattere di sottolineatura (\_) e punto (.).

La porta del repository può essere qualsiasi numero di porta valido e il nome host del repository può essere qualsiasi nome host valido. Il nome host deve essere composto da caratteri alfabetici (A-Z), cifre (0-9), segno meno (-) e punto (.), ma non da un carattere di sottolineatura (\_).

Il repository deve essere creato in un database Oracle. Il database utilizzato da SnapManager deve essere configurato in conformità alle procedure Oracle per la configurazione del database.

Un singolo repository può contenere informazioni su più profili; tuttavia, ogni database è normalmente associato a un solo profilo. Puoi avere più repository, con ogni repository contenente più profili.

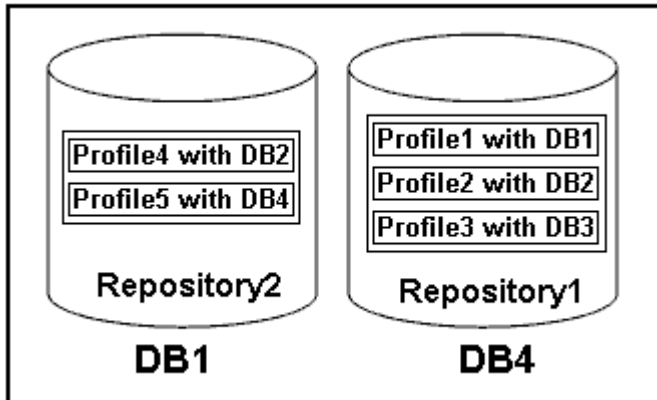
## Quali sono i profili

SnapManager utilizza i profili per memorizzare le informazioni necessarie per eseguire operazioni su un determinato database. Un profilo contiene le informazioni sul database, incluse le credenziali, i backup e i cloni. Creando un profilo, non è necessario specificare i dettagli del database ogni volta che si esegue un'operazione sul database.

Un profilo può fare riferimento a un solo database. Lo stesso database può essere referenziato da più profili. Non è possibile accedere ai backup creati utilizzando un profilo diverso, anche se entrambi i profili fanno riferimento allo stesso database.

Le informazioni del profilo vengono memorizzate in un repository. Il repository contiene sia le informazioni del profilo per il database che le informazioni sulle copie Snapshot che fungono da backup del database. Le copie Snapshot effettive vengono memorizzate nel sistema di storage. I nomi delle copie Snapshot vengono memorizzati nel repository contenente il profilo per il database. Quando si esegue un'operazione su un database, è necessario selezionare il profilo dal repository.

La figura seguente illustra come i repository possono contenere più profili, ma anche che ciascun profilo può definire un solo database:



Nell'esempio precedente, Repository2 si trova sul database DB1 e Repository1 nel database DB4.

Ogni profilo contiene le credenziali del database associato al profilo. Le credenziali consentono a SnapManager di connettersi al database e di lavorare con esso. Le credenziali memorizzate includono le coppie di nome utente e password per l'accesso all'host, al repository, al database e le informazioni di connessione richieste se si utilizza Oracle Recovery Manager (RMAN).

Non è possibile accedere a un backup creato utilizzando un profilo da un profilo diverso, anche se entrambi i profili sono associati allo stesso database. SnapManager inserisce un blocco nel database per impedire l'esecuzione simultanea di due operazioni incompatibili.

### Profilo per la creazione di backup completi e parziali

È possibile creare profili per eseguire backup completi o parziali.

I profili specificati per creare i backup completi e parziali contengono sia i file di dati che i file di log dell'archivio. SnapManager non consente a tali profili di separare i backup del registro di archiviazione dai backup del file di dati. I backup completi e parziali vengono conservati in base alle policy di conservazione dei backup esistenti e protetti in base alle policy di protezione esistenti. Puoi pianificare backup completi e parziali in base al tempo e alla frequenza che preferisci.

## Profili per la creazione di backup solo file di dati e backup solo log di archiviazione

SnapManager (3.2 o versione successiva) consente di creare profili che eseguono i backup dei file di log dell'archivio separatamente dai file di dati. Dopo aver utilizzato il profilo per separare i tipi di backup, è possibile creare backup solo file di dati o backup solo log di archiviazione del database. È inoltre possibile creare un backup contenente sia i file di dati che i file di registro dell'archivio.

Il criterio di conservazione si applica a tutti i backup del database quando i backup del registro di archiviazione non sono separati. Dopo aver separato i backup del log di archiviazione, SnapManager consente di specificare diverse durate di conservazione e policy di protezione per i backup del log di archiviazione.

### Politica di conservazione

SnapManager determina se conservare un backup considerando sia il numero di conservazione (ad esempio, 15 backup) che la durata della conservazione (ad esempio, 10 giorni di backup giornalieri). Un backup scade quando la sua età supera la durata di conservazione impostata per la classe di conservazione e il numero di backup supera il numero di conservazione. Ad esempio, se il numero di backup è 15 (ovvero SnapManager ha eseguito 15 backup riusciti) e il requisito di durata è impostato per 10 giorni di backup giornalieri, i cinque backup più vecchi, riusciti e idonei scadono.

### Durata conservazione registro archivio

Una volta separati, i backup del registro di archiviazione vengono conservati in base alla durata di conservazione del registro di archiviazione. I backup dei log di archiviazione eseguiti con i backup dei file di dati vengono sempre conservati insieme ai backup dei file di dati, indipendentemente dalla durata della conservazione dei log di archiviazione.

### Informazioni correlate

[Gestione dei profili per backup efficienti](#)

## Quali sono gli stati operativi di SnapManager

Le operazioni SnapManager (backup, ripristino e clonazione) possono essere in stati diversi, con ciascuno stato che indica l'avanzamento dell'operazione.

Stato operativo	Descrizione
Operazione riuscita	Operazione completata correttamente.
In esecuzione	L'operazione è stata avviata, ma non è stata completata. Ad esempio, alle 11:00 viene pianificato un backup che richiede due minuti. Quando si visualizza la scheda <b>Schedule</b> alle 11:01, l'operazione viene visualizzata come in esecuzione.
Nessuna operazione trovata	La pianificazione non è stata eseguita o l'ultimo backup eseguito è stato eliminato.



Stato operativo	Descrizione
Non riuscito	Operazione non riuscita. SnapManager ha eseguito automaticamente il processo di interruzione e ha pulito l'operazione. <b>Nota:</b> è possibile dividere il clone creato. Quando si interrompe l'operazione di split clone avviata e l'operazione viene interrotta correttamente, lo stato dell'operazione di split clone viene visualizzato come failed (non riuscito).

## Eventi ripristinabili e non ripristinabili

Un evento SnapManager ripristinabile presenta i seguenti problemi:

- Il database non viene memorizzato in un sistema storage che esegue Data ONTAP.
- È stato configurato un database ASM (Automatic Storage Management), ma l'istanza ASM non è in esecuzione.
- SnapDrive per UNIX non è installato o non può accedere al sistema di storage.
- SnapManager non riesce a creare una copia Snapshot o a eseguire il provisioning dello storage se il volume è esaurito, se è stato raggiunto il numero massimo di copie Snapshot o se si verifica un'eccezione non prevista.

Quando si verifica un evento ripristinabile, SnapManager esegue un processo di interruzione e tenta di riportare l'host, il database e il sistema di storage allo stato iniziale. Se il processo di interruzione non riesce, SnapManager considera l'incidente come un evento irrecuperabile.

Un evento irreversibile (fuori banda) si verifica quando si verifica una delle seguenti condizioni:

- Si verifica un problema di sistema, ad esempio in caso di guasto di un host.
- Il processo SnapManager viene interrotto.
- Un'operazione di interruzione in-band non riesce quando il sistema storage si guasta, il numero di unità logica (LUN) o il volume di storage non è in linea o la rete non funziona.

Quando si verifica un evento irreversibile, SnapManager esegue immediatamente un processo di interruzione. L'host, il database e il sistema di storage potrebbero non essere tornati agli stati iniziali. In tal caso, è necessario eseguire una pulizia dopo l'operazione SnapManager, eliminando la copia Snapshot orfana e rimuovendo il file di blocco SnapManager.

Se si desidera eliminare il file di blocco SnapManager, accedere a Oracle\_HOME sul computer di destinazione ed eliminare il file SM\_LOCK\_TargetDBName. Dopo aver eliminato il file, riavviare il server SnapManager per Oracle.

## In che modo SnapManager mantiene la sicurezza

È possibile eseguire operazioni SnapManager solo se si dispone delle credenziali appropriate. La sicurezza in SnapManager è regolata dall'autenticazione dell'utente e dal RBAC (role-based access control). RBAC consente agli amministratori di database di limitare le operazioni che SnapManager può eseguire rispetto ai volumi e alle LUN che contengono i file di dati in un database.

Gli amministratori di database abilitano RBAC per SnapManager utilizzando SnapDrive. Gli amministratori del database assegnano quindi le autorizzazioni ai ruoli SnapManager e assegnano questi ruoli agli utenti nell'interfaccia grafica utente (GUI) o nell'interfaccia a riga di comando (CLI) di Operations Manager. I controlli delle autorizzazioni RBAC avvengono nel server DataFabric Manager.

Oltre all'accesso basato sui ruoli, SnapManager garantisce la sicurezza richiedendo l'autenticazione dell'utente tramite password richieste o impostando le credenziali dell'utente. Un utente effettivo viene autenticato e autorizzato con il server SnapManager.

Le credenziali SnapManager e l'autenticazione dell'utente differiscono in modo significativo da SnapManager 3.0:

- Nelle versioni di SnapManager precedenti alla 3.0, è necessario impostare una password server arbitraria quando si installa SnapManager. Chiunque desideri utilizzare il server SnapManager necessita della password del server SnapManager. La password del server SnapManager deve essere aggiunta alle credenziali utente utilizzando il comando `smo credential set -host`.
- In SnapManager (3.0 e versioni successive), la password del server SnapManager è stata sostituita dall'autenticazione del sistema operativo (OS) per singolo utente. Se il client non viene eseguito dallo stesso server dell'host, il server SnapManager esegue l'autenticazione utilizzando i nomi utente e le password del sistema operativo. Se non si desidera che venga richiesto di inserire le password del sistema operativo, è possibile salvare i dati nella cache delle credenziali utente di SnapManager utilizzando il comando `smo credential set -host`.



Il comando `smo credential set -host` memorizza le credenziali quando la proprietà `host.credentials.Persist` nel file `smo.config` è impostata su `true`.

**Esempio**

User1 e User2 condividono un profilo denominato Prof2. L'utente 2 non può eseguire un backup di Database1 nell'host 1 senza l'autorizzazione ad accedere all'host 1. L'utente 1 non può clonare un database in Host3 senza il permesso di accedere all'host 3.

La seguente tabella descrive le diverse autorizzazioni assegnate agli utenti:

Tipo di autorizzazione	Utente1	Utente2
Password host	Host 1, host 2	Host2, Host3
Password repository	Repo1	Repo1
Password del profilo	Prof1, Prof2	Prof2

Nel caso in cui l'utente 1 e l'utente 2 non dispongano di profili condivisi, si supponga che l'utente 1 disponga delle autorizzazioni per gli host denominati Host1 e Host2 e che l'utente 2 disponga delle autorizzazioni per l'host denominato Host2. L'utente 2 non può eseguire nemmeno i comandi non di profilo come `dump` e `system verify` sull'host 1.

# Accesso e stampa della Guida in linea

La Guida in linea fornisce istruzioni per le attività che è possibile eseguire utilizzando l'interfaccia grafica utente di SnapManager. La Guida in linea fornisce anche descrizioni

dei campi delle finestre e delle procedure guidate.

1. Eseguire una delle seguenti operazioni:
  - Nella finestra principale, fare clic su **Guida > Guida**.
  - In qualsiasi finestra o procedura guidata, fare clic su **Help** (Guida) per visualizzare la guida specifica per la finestra.
2. Utilizzare il **Sommario** nel riquadro di sinistra per spostarsi tra gli argomenti.
3. Fare clic sull'icona stampante nella parte superiore della finestra della guida per stampare singoli argomenti.

## Layout generali del database e configurazioni di storage consigliati

Conoscere i layout generali dei database e le configurazioni di storage consigliati può aiutare a evitare problemi relativi a gruppi di dischi, tipi di file e spazi delle tabelle.

- Non includere nel database file di più tipi DI file system SAN o di gestore di volumi.

Tutti i file che costituiscono un database devono risiedere nello stesso tipo di file system.

- SnapManager richiede un multiplo di blocchi di dimensioni 4K.
- Includere l'identificatore del sistema di database nel file oratab.

Includere una voce nel file oratab per ciascun database da gestire. SnapManager si affida al file oratab per determinare quale sede Oracle utilizzare.

- Se si desidera registrare i backup di SnapManager con Oracle Recovery Manager (RMAN), è necessario creare profili abilitati per RMAN.

Se si desidera sfruttare il nuovo ripristino basato su volume o il ripristino completo del gruppo di dischi, prendere in considerazione le seguenti linee guida relative ai file system e ai gruppi di dischi:

- Più database non possono condividere lo stesso gruppo di dischi ASM (Automatic Storage Management).
- Un gruppo di dischi contenente file di dati non può contenere altri tipi di file.
- Il numero di unità logica (LUN) per il gruppo di dischi del file di dati deve essere l'unico oggetto nel volume di storage.

Di seguito sono riportate alcune linee guida per la separazione dei volumi:

- I file di dati di un solo database devono essere presenti nel volume.
- È necessario utilizzare volumi separati per ciascuna delle seguenti classificazioni di file: File binari di database, file di dati, file di log di ripristino online, file di log di ripristino archiviati e file di controllo.
- Non è necessario creare un volume separato per i file di database temporanei perché SnapManager non esegue il backup dei file di database temporanei.

### Definizione della home database con il file oratab

SnapManager utilizza il file oratab durante le operazioni per determinare la home directory del database Oracle. Affinché SnapManager funzioni correttamente, è

necessario che nel file oratab sia presente una voce per il database Oracle. Il file oratab viene creato durante l'installazione del software Oracle.

Il file oratab si trova in posizioni diverse in base al sistema operativo host, come mostrato nella tabella seguente:

Sistema operativo host	Percorso del file
Linux	/etc/oratab
Solaris	/var/opt/oracle/oratab
IBM AIX	/etc/oratab

Il file oratab di esempio contiene le seguenti informazioni:

```
+ASM1:/u01/app/11.2.0/grid:N    # line added by Agent
oelpro:/u01/app/11.2.0/oracle:N    # line added by Agent
# SnapManager generated entry      (DO NOT REMOVE THIS LINE)
smoclone:/u01/app/11.2.0/oracle:N
```



Una volta installato Oracle, assicurarsi che il file oratab si trovi nella posizione specificata nella tabella precedente. Se il file oratab non si trova nella posizione corretta per il sistema operativo in uso, contattare il supporto tecnico per assistenza.

## Requisiti per l'utilizzo di database RAC con SnapManager

È necessario conoscere i consigli per l'utilizzo di database RAC (Real Application Clusters) con SnapManager. I consigli includono numeri di porta, password e modalità di autenticazione.

- In modalità di autenticazione del database, il listener su ciascun nodo che interagisce con un'istanza del database RAC deve essere configurato in modo da utilizzare lo stesso numero di porta.

Il listener che interagisce con l'istanza primaria del database deve essere avviato prima di iniziare un backup.

- In modalità di autenticazione del sistema operativo o in un ambiente di gestione automatica dello storage (ASM), il server SnapManager deve essere installato e in esecuzione su ciascun nodo dell'ambiente RAC.
- La password dell'utente del database (ad esempio, per un amministratore di sistema o un utente con il privilegio sysdba) deve essere la stessa per tutte le istanze di database Oracle in un ambiente RAC.

## Requisiti per l'utilizzo di database ASM con SnapManager

È necessario conoscere i requisiti per l'utilizzo dei database di gestione automatica dello storage (ASM) con SnapManager. La conoscenza di questi requisiti può aiutare a evitare problemi con le specifiche ASMLib, le partizioni e i cloni, tra le altre cose.

- SnapManager (3.0.3 o versioni successive) utilizza il nuovo privilegio sysasm disponibile con Oracle 11gR2 invece del privilegio sysdba per amministrare un'istanza di Oracle ASM.

Se si utilizza il privilegio sysdba per eseguire comandi amministrativi sull'istanza di ASM, viene visualizzato un messaggio di errore. Il database utilizza il privilegio sysdba per accedere ai gruppi di dischi. Se ci si connette all'istanza ASM utilizzando il privilegio sysasm, si dispone dell'accesso completo a tutti i gruppi di dischi e alle funzioni di gestione di Oracle ASM disponibili.



Se si utilizza Oracle 10gR2 e 11gR1, è necessario continuare a utilizzare il privilegio sysdba.

- SnapManager (3.0.3 o versioni successive) supporta il backup di database memorizzati direttamente su gruppi di dischi ASM quando il gruppo di dischi contiene anche un volume ACFS (Automatic Cluster file System).

Questi file sono indirettamente protetti da SnapManager e potrebbero essere ripristinati con il contenuto rimanente di un gruppo di dischi ASM, ma SnapManager (3.0.3 o versione successiva) non supporta ACFS.



ACFS è una tecnologia di gestione dello storage per file system scalabile e multiplatforma disponibile con Oracle 11gR2. ACFS estende la funzionalità ASM per supportare i file dei clienti gestiti al di fuori del database Oracle.

- SnapManager (3.0.3 o versione successiva) supporta il backup dei file memorizzati nei gruppi di dischi ASM quando il gruppo di dischi contiene anche file OCR (Registro cluster Oracle) o file di dischi di voto; tuttavia, le operazioni di ripristino richiedono un metodo più lento, basato su host o PFSR (Partial-file Snap Restore).

Si consiglia di disporre di dischi OCR e di voto su gruppi di dischi che non contengono file di database.

- Ogni disco utilizzato per ASM deve contenere una sola partizione.
- La partizione che ospita i dati ASM deve essere allineata correttamente per evitare gravi problemi di performance.

Ciò implica che il LUN deve essere del tipo corretto e che la partizione deve avere un offset che è un multiplo di 4K byte.



Per ulteriori informazioni su come creare partizioni allineate a 4K, vedere l'articolo della Knowledge base 1010717.

- La configurazione ASM non è specificata come parte della specifica del clone.

Prima di aggiornare l'host a SnapManager (2.2 o versione successiva), è necessario rimuovere manualmente le informazioni di configurazione ASM nelle specifiche dei cloni create con SnapManager 2.1.

- SnapManager 3.1, 3.1p1 e 3.2 o versioni successive supportano ASMLib 2.1.4.
- SnapManager 3.1p4 o versioni successive supportano ASMLib 2.1.4, 2.1.7 e 2.1.8.

## Periferiche di partizione supportate

È necessario conoscere i diversi dispositivi di partizione supportati in SnapManager.

La seguente tabella fornisce informazioni sulle partizioni e su come attivarle per i diversi sistemi operativi:

<b>Sistema operativo</b>	<b>Partizione singola</b>	<b>Partizione multipla</b>	<b>Dispositivi senza partizione</b>	<b>File system o dispositivi RAW</b>
Red Hat Enterprise Linux 5x o.  Oracle Enterprise Linux 5 volte	Sì	No	No	ext3*
Red Hat Enterprise Linux 6 x  Oracle Enterprise Linux 6 volte	Sì	No	No	ext3 o ext4*
SUSE Linux Enterprise Server 11	Sì	No	No	ext3*
SUSE Linux Enterprise Server 10	No	No	Sì	ext3***
Red Hat Enterprise Linux 5x o versione successiva  Oracle Enterprise Linux 5x o versioni successive	Sì	No	Sì	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4OR  SUSE Linux Enterprise Server 11	Sì	No	Sì	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4 o versione successiva  SUSE Linux Enterprise Server 11	Sì	No	No	ASM senza ASMLib**

Per ulteriori informazioni sulle versioni dei sistemi operativi supportate, fare riferimento alla matrice di interoperabilità.

## Supporto per ASMLib

SnapManager supporta diverse versioni di ASMLib, sebbene vi siano diversi fattori da considerare quando si utilizza SnapManager con ASMLib.

SnapManager supporta ASMLib 2.1.4, 2.1.7 e 2.1.8. Tutte le operazioni SnapManager possono essere eseguite con ASMLib 2.1.4, 2.1.7 e 2.1.8.

Se è stato eseguito l'aggiornamento da ASMLib 2.1.4 ad ASM 2.1.7, è possibile utilizzare gli stessi profili e backup creati con ASMLib 2.1.4 per ripristinare i backup e creare i cloni.

Quando si utilizza SnapManager con ASMLib, è necessario considerare quanto segue:

- SnapManager 3.1 non supporta ASMLib 2.1.7.

SnapManager 3.1p4 o versioni successive supportano ASMLib 2.1.4, 2.1.7 e 2.1.8.

- Dopo aver eseguito un aggiornamento rolling da SnapManager 3.1 a 3.2, i backup creati utilizzando ASMLib 2.1.7 funzionano solo se il repository viene rollback a SnapManager 3.1 e ASMLib 2.1.7 viene rollgrade a ASMLib 2.1.4.
- Dopo aver eseguito un aggiornamento a rotazione da SnapManager 3.1 a 3.2, i backup creati utilizzando ASMLib 2.1.7 non funzionano se il repository viene rollback a SnapManager 3.1 con ASMLib 2.1.7.

Il rollback ha esito positivo, ma i profili e i backup non possono essere utilizzati.

## Supporto per database ASM senza ASMLib

Per impostazione predefinita, SnapManager supporta ASM senza ASMLib. Il requisito di base è che i dispositivi utilizzati per i gruppi di dischi ASM devono essere partizionati.

Quando ASMLib non è installato, le autorizzazioni dei dispositivi relative ai gruppi di dischi ASM vengono modificate in root:disk quando si eseguono le seguenti operazioni:

- Riavviare l'host
- Ripristinare un database dallo storage primario utilizzando VBSR (Volume-Based SnapRestore)
- Ripristinare un database dallo storage secondario

È possibile impostare le autorizzazioni appropriate per il dispositivo assegnando true alla variabile di configurazione `oracleasm.support.without.asmlib` in `smo.conf`. I dispositivi relativi ai gruppi di dischi ASM vengono aggiunti o rimossi dal file `initasmdisks` ogni volta che vengono aggiunti o rimossi nuovi dispositivi dall'host. Il file `initasmdisks` si trova in `/etc/initasmdisks`.

Ad esempio, se si imposta `oracleasm.support.without.asmlib=true` e si esegue un montaggio di backup, i nuovi dispositivi vengono aggiunti agli `initasmdisks`. Quando l'host viene riavviato, le autorizzazioni e la proprietà del dispositivo vengono mantenute dagli script di avvio.



Il valore predefinito per `oracleasm.support.without.asmlib` è false.

### Informazioni correlate

[Periferiche di partizione supportate](#)

## Script supportati

Gli script `asmmain.sh` e `asmquerydisk.sh` consentono di modificare l'utente, il gruppo e l'utente della griglia, tutti utilizzati per eseguire query sui dischi ASM. Gli script devono essere sempre eseguiti dalla directory principale.

`asmmain.sh` è il file di script principale chiamato da qualsiasi operazione che aggiunga o elimini dispositivi. Lo script `asmmain.sh` chiama un altro script internamente, che deve essere eseguito dalla directory principale che dispone di credenziali oracle Grid. Questo script interroga i dispositivi del gruppo di dischi ASM, quindi aggiunge tali voci nel file `initasmdisk` con l'autorizzazione e la proprietà dei dispositivi. È possibile modificare i permessi e la proprietà di questo file in base al proprio ambiente e al modello regex utilizzato per la corrispondenza solo con `/dev/mapper/*p1`.

Lo script `asmquerydisk.sh` viene utilizzato per eseguire query nell'elenco dei dischi, utilizzato per creare il gruppo di dischi ASM. È necessario assegnare valori a `ORACLE_BASE`, `ORACLE_HOME` e `ORACLE_SID`, a seconda della configurazione.

Gli script si trovano in `/opt/NetApp/smo/plugins/emplies/noasmLib`. Tuttavia, questi script devono essere spostati in `/opt/NetApp/smo/plugins/noasmLib` prima di avviare il server SnapManager per Oracle sull'host.

## Limitazioni dell'utilizzo di script per supportare un database ASM senza ASMLib

È necessario conoscere alcune limitazioni all'utilizzo di script per supportare un database ASM senza ASMLib.

- Gli script forniscono una soluzione alternativa per qualsiasi versione del kernel, ma solo se ASMLib non è installato.
- Le autorizzazioni per gli script devono essere impostate in modo che sia possibile accedervi da utenti root, grid, oracle o equivalenti.
- Gli script non supportano il ripristino da una posizione secondaria.

## Implementazione ed esecuzione degli script

È possibile implementare ed eseguire gli script `asmmain.sh` e `asmquerydisk.sh` per supportare i database ASM senza ASMLib.

Questi script non seguono la sintassi pre-scripts o post-scripts e il workflow viene chiamato quando `initasmdisks` è attivato. È possibile modificare qualsiasi elemento correlato alle impostazioni di configurazione negli script. Si consiglia di verificare se tutti gli script funzionano come previsto eseguendo una rapida esecuzione a secco.



Questi script non danneggiano il sistema in caso di guasti né influiscono sul sistema. Questi script vengono eseguiti per aggiornare i dischi relativi ad ASM in modo che dispongano delle autorizzazioni e della proprietà appropriate, in modo che i dischi siano sempre sotto il controllo dell'istanza di ASM.

1. Creare i gruppi di dischi ASM con i dischi partizionati.
2. Creare il database Oracle sui GRUPPI DI DISCHI.
3. Arrestare il server SnapManager per Oracle.





In un ambiente RAC, è necessario eseguire questo passaggio su tutti i nodi RAC.

4. Modificare il file `smo.conf` in modo da includere i seguenti parametri:

- a. `oracleasm.support.without.asmlib = true`
- b. `oracleasm.support.without.asmlib.ownership = true`
- c. `oracleasm.support.without.asmlib.username = nome utente dell'ambiente dell'istanza ASM`
- d. `oracleasm.support.without.asmlib.groupname = nome del gruppo dell'ambiente di istanze ASM`

Queste modifiche impostano i permessi solo per il percorso assoluto, il che significa che invece di partizione device, i permessi saranno impostati solo per il device `dm-*`.

- 5. Modificare gli script dei plug-in disponibili in `/opt/NetApp/smo/plugins/emplies/noasmlib` per includere le impostazioni di configurazione negli script.
- 6. Copiare gli script in `/opt/NetApp/smo/plugins/noasmlib` prima di avviare il server SnapManager per Oracle sull'host.
- 7. Accedere alla directory `/opt/NetApp/smo` ed eseguire un'esecuzione a secco eseguendo il seguente script:  
`sh plugins/noasmlib/asmmain.sh`

Viene creato il file `etc/initasmdisks`, che è il file principale utilizzato.

È possibile confermare che il file `etc/initasmdisks` contenga tutti i dispositivi relativi al database ASM configurato, ad esempio:

```
chown -R grid:oinstall /dev/mapper/360a98000316b61396c3f394645776863p1
chmod 777 /dev/mapper/360a98000316b61396c3f394645776863p1
chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714239p1
chmod 777 /dev/mapper/360a980003754322f7a2b433469714239p1
chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714241p1
chmod 777 /dev/mapper/360a980003754322f7a2b433469714241p1
chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714243p1
chmod 777 /dev/mapper/360a980003754322f7a2b433469714243p1
```

- 8. Avviare il server SnapManager per Oracle.
- 9. Configurare SnapDrive per UNIX aggiungendo quanto segue al file `snapdrive.conf.disconnect-lun-before-vbsr=on`
- 10. Riavviare il server SnapDrive per UNIX.



In un ambiente RAC, è necessario eseguire i passaggi da 3 a 10 per tutti i nodi RAC.

Il file `/etc/initasmdisks` creato deve essere eseguito da uno degli script di avvio o da uno script appena definito in `rc3.d`. Il file `/etc/initasmdisks` deve essere sempre eseguito prima dell'avvio del servizio `oracleha`.

Esempio

```
# ls -ltr *ohasd*
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 S96ohasd ->
/etc/init.d/ohasd
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 K15ohasd ->
/etc/init.d/ohasd
```

Nell'esempio seguente, `sh -x/etc/initasmdisks` non sarà disponibile per impostazione predefinita ed è necessario aggiungerlo come prima riga della funzione `start_stack()` in uno script `ohasd`:

```
start_stack()
{
sh -x /etc/initasmdisks
# see init.ohasd.sbs for a full rationale case $PLATFORM in Linux
}
```

#### Supporto per database Oracle RAC ASM senza ASMLib

Se si utilizzano database Oracle RAC, i nodi RAC devono essere aggiornati con il file `initasmdisks` ogni volta che viene eseguita un'operazione nel nodo RAC master.

Se non è richiesta alcuna autenticazione per accedere ai nodi RAC dal nodo master, `asmmain.sh` esegue una copia sicura (SCP) dei dischi di `initasmsu` tutti i nodi RAC. Il file `initasmdisks` del nodo master viene chiamato ogni volta che viene eseguito il ripristino e lo script `asmmain.sh` può essere aggiornato per richiamare lo stesso script in tutti i nodi RAC.

Il file `/etc/initasmdisks` creato che deve essere eseguito da uno degli script di avvio o da uno script appena definito in `rc3.d`. Il file `/etc/initasmdisks` deve essere sempre eseguito prima dell'avvio del servizio `oracleha`.

#### Supporto per database Oracle 10g ASM senza ASMLib

Se si utilizza Oracle 10g, il comando `asmcmd` non è disponibile per l'elenco dei dischi. È possibile utilizzare la query `sql` per ottenere l'elenco dei dischi.

Lo script `disk_list.sql` è incluso negli script esistenti forniti nella directory degli esempi per supportare le query `sql`. Quando si esegue lo script `theasmquerydisk.sh`, lo script `disk_list.sql` deve essere eseguito manualmente. Le righe di script di esempio vengono aggiunte con i commenti nel file `asmquerydisk.sh`. Questo file può essere posizionato nella posizione `/home/grid` o in un'altra posizione a scelta.

#### Script di esempio per supportare database ASM senza ASMLib

Gli script di esempio sono disponibili nella directory `plugins/emesemes/noasmlib` della directory di installazione di SnapManager per Oracle.

##### `asmmain.sh`

```
#!/bin/bash
griduser=grid
```

```

gridgroup=oinstall

# Run the script which takes the disklist from the asmcmd
# use appropriate user , here grid user is being used to run
# asmcmd command.
su -c "plugins/noasmllib/asmdiskquery.sh" -s /bin/sh grid
cat /home/grid/disklist

# Construct the final file as .bak file with propre inputs
awk -v guser=$griduser -v ggroup=$gridgroup '/^\s*/dev\/mapper/ { print
"chown -R "guser":"ggroup" "$1; print "chmod 777 " $1; }'
/home/grid/disklist > /etc/initasmdisks.bak

# move the bak file to the actual file.
mv /etc/initasmdisks.bak /etc/initasmdisks

# Set full full permission for this file to be called while rebooting and
restore
chmod 777 /etc/initasmdisks

# If the /etc/initasmdisks needs to be updated in all the RAC nodes
# or /etc/initasmdisks script has to be executed in the RAC nodes, then
the following
# section needs to be uncommented and used.
#
# Note: To do scp or running scripts in remote RAC node via ssh, it needs
password less login
# for root user with ssh keys shared between the two nodes.
#
# The following 2 lines are used for updating the file in the RAC nodes:
# scp /etc/initasmdisks root@racnode1:/etc/initasmdisks
# scp /etc/initasmdisks root@racnode2:/etc/initasmdisks
#
# In order to execute the /etc/initasmdisks in other RAC nodes
# The following must be added to the master RAC node /etc/initasmdisks
file
# from the asmmain.sh script itself. The above scp transfer will make sure
# the permissions and mode for the disk list contents are transferred to
the other RAC nodes
# so now appending any command in the /etc/initasmsdisks will be retained
only in the master RAC node.
# The following lines will add entries to the /etc/initasmsdisks file in
master RAC node only. When this script is executed
# master RAC node, /etc/initasmdisks in all the RAC nodes will be
executed.
# echo 'ssh racnode1 /etc/initasmdisks' >> /etc/initasmdisks

```

```
# echo 'ssh racnode2 /etc/initasm disks' >> /etc/initasm disks
```

### asmquerydisk.sh

```
#!/bin/bash
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/grid/product/11.2.0.3/grid
export ORACLE_SID=+ASM
export PATH=$ORACLE_HOME/bin:$PATH

# Get the Disk List and save this in a file called dglist.
asmcmd lsdsk > /home/grid/disklist

# In oracle 10g the above used command 'asmcmd' is not available so use
SQL
# query can be used to take the disk list. Need to uncomment the following
# line and comment the above incase oracle 10g is being in use.
# The disk_list.sql script is availbe in this noasm lib examples folder
itself
# which can be modified as per customer needs.
# sqlplus "/as sysdba" @/home/grid/disk_list.sql > /home/grid/disklist
```

### disk\_list.sql

```
# su - oracle
-bash-4.1$ cat disk_list.sql
select path from v$asm_disk;
exit
-bash-4.1$
```

## Requisiti per l'utilizzo di database con NFS e SnapManager

È necessario conoscere i requisiti per l'utilizzo dei database con NFS (Network file System) e SnapManager. I consigli includono l'esecuzione come root, il caching degli attributi e i collegamenti simbolici.

- È necessario eseguire SnapManager come root; SnapManager deve essere in grado di accedere ai file system che contengono file di dati, file di controllo, log di ripristino online, log di archiviazione e la home page del database.

Impostare una delle seguenti opzioni di esportazione NFS per garantire che root possa accedere ai file system:

- root=nome host
- rw=nome host, anon=0

- È necessario disattivare il caching degli attributi per tutti i volumi che contengono file di dati del database, file di controllo, log di ripristino e archiviazione e home page del database.

Esportare i volumi utilizzando le opzioni noac (per Solaris e AIX) o actimeo=0 (per Linux).

- È necessario collegare i file di dati del database dallo storage locale a NFS per supportare i collegamenti simbolici solo a livello di mount point.

## Layout di volumi di database di esempio

Per informazioni sulla configurazione del database, fare riferimento ai layout dei volumi del database di esempio.

### Database a istanza singola

Tipi di file	Nomi dei volumi	Volume dedicato per i tipi di file	Copie Snapshot automatiche
Binari Oracle	orabin_host name	Sì	Acceso
File di dati	oradata_sid	Sì	Spento
File di dati temporanei	oatemp_sid	Sì	Spento
File di controllo	Oacntrl01_sid (multiplex) Oacntrl02_sid (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_sid (multiplex) Oralog02_sid (multiplex)	Sì	Spento
Registri di archiviazione	oraarch_sid	Sì	Spento

### Real Application Clusters (RAC)

Tipi di file	Nomi dei volumi	Volume dedicato per i tipi di file	Copie Snapshot automatiche
Binari Oracle	orabin_host name	Sì	Acceso
File di dati	oradata_dbname	Sì	Spento
File di dati temporanei	ortamp_dbname	Sì	Spento

<b>Tipi di file</b>	<b>Nomi dei volumi</b>	<b>Volume dedicato per i tipi di file</b>	<b>Copie Snapshot automatiche</b>
File di controllo	Oracntrl01_dbname (multiplex)  Oracntrl02_dbname (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_dbname (multiplex)  Oralog02_dbname (multiplex)	Sì	Spento
Registri di archiviazione	oraarch_dbname	Sì	Spento
File del cluster	oracrs_clustername	Sì	Acceso

#### **Singola istanza di un database ASM (Automatic Storage Management)**

<b>Tipi di file</b>	<b>Nomi dei volumi</b>	<b>Nomi LUN</b>	<b>Volume dedicato per i tipi di file</b>	<b>Copie Snapshot automatiche</b>
Binari Oracle	orabin_host name	orabin_host namelun	Sì	Acceso
File di dati	oradata_sid	oradata_sidlun	Sì	Spento
File di dati temporanei	oatemp_sid	Oratemp_sidlun	Sì	Spento
File di controllo	Oacntrl01_sid (multiplex)  Oacntrl02_sid (multiplex)	Oracntrl01_sidlun (multiplex)  Oracntrl02_sidlun (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_dbname (multiplex)  Oralog02_dbname (multiplex)	Oralog01_dbnamelu n (multiplex)  Oralog02_dbnamelu n (multiplex)	Sì	Spento
Registri di archiviazione	oraarch_sid	Oraarch_sidlun	Sì	Spento

## Database RAC ASM

Tipi di file	Nomi dei volumi	Nomi LUN	Volume dedicato per i tipi di file	Copie Snapshot automatiche
Binari Oracle	orabin_host name	orabin_host namelun	Sì	Acceso
File di dati	oradata_sid	oradata_sidlun	Sì	Spento
File di dati temporanei	oatemp_sid	Oratemp_sidlun	Sì	Spento
File di controllo	Oacntrl01_sid (multiplex)	Oracntrl01_sidlun (multiplex)	Sì	Spento
	Oacntrl02_sid (multiplex)	Oracntrl02_sidlun (multiplex)		
Registri di ripristino	Oralog01_dbname (multiplex)	Oralog01_dbnamelu n (multiplex)	Sì	Spento
	Oralog02_dbname (multiplex)	Oralog02_dbnamelu n (multiplex)		
Registri di archiviazione	oraarch_sid	Oraarch_sidlun	Sì	Spento
File del cluster	oracrs_clustername	oracrs_clusternamel un	Sì	Acceso

## Limitazioni quando si lavora con SnapManager

È necessario conoscere gli scenari e le limitazioni che potrebbero influire sull'ambiente.

### Limitazioni relative ai layout e alle piattaforme dei database

- SnapManager supporta i file di controllo su un file system in un gruppo di dischi ASM e non supporta i file di controllo sui dispositivi raw.
- SnapManager opera in un ambiente di clustering Microsoft (MSCS) ma non riconosce lo stato della configurazione MSCS (attiva o passiva) e non trasferisce la gestione attiva di un repository a un server di standby in un cluster MSCS.
- In Red Hat Enterprise Linux (RHEL) e Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 e 5.3, Il file system ext3 non è supportato quando si implementa Oracle su dispositivi raw utilizzando il multipathing dinamico (DMP) in un ambiente di i/o di rete multipath (MPIO).

Questo problema si verifica in SnapManager solo quando si utilizza SnapDrive 4.1 per UNIX o versioni precedenti.

- SnapManager su RHEL non supporta la partizione dei dischi utilizzando l'utilità **parted**.

Si tratta di un problema con l'utility RHEL **parted**.

- In una configurazione RAC, quando il nome di un profilo viene aggiornato dal nodo RAC A, il file di pianificazione per il profilo viene aggiornato solo per il nodo RAC A.

Il file di pianificazione per lo stesso profilo sul nodo RAC B non viene aggiornato e contiene le informazioni di pianificazione precedenti. Quando un backup pianificato viene attivato dal nodo B, l'operazione di backup pianificato non riesce perché il nodo B contiene il file di pianificazione precedente. Tuttavia, l'operazione di backup pianificata ha esito positivo dal nodo A, sul quale il profilo viene rinominato. È possibile riavviare il server SnapManager in modo da ricevere l'ultimo file di pianificazione per il profilo sul nodo B.

- Il database del repository potrebbe essere presente su un host a cui è possibile accedere utilizzando più indirizzi IP.

Se si accede al repository utilizzando più indirizzi IP, viene creato il file di pianificazione per ciascuno degli indirizzi IP. Se il backup della pianificazione viene creato per un profilo (ad esempio, il profilo A) sotto uno degli indirizzi IP (ad esempio, IP1), il file di pianificazione per solo quell'indirizzo IP viene aggiornato. Se si accede al profilo A da un altro indirizzo IP (ad esempio, IP2), il backup pianificato non viene elencato perché il file di pianificazione di IP2 non dispone di una voce per la pianificazione creata con IP1.

È possibile attendere che la pianificazione venga attivata da tale indirizzo IP e che il file di pianificazione venga aggiornato oppure riavviare il server.

### **Limitazioni relative alla configurazione SnapManager**

- SnapManager può essere configurato per catalogare i backup dei database con RMAN.

Se si utilizza un catalogo di ripristino RMAN, il catalogo di ripristino deve trovarsi in un database diverso da quello di cui è stato eseguito il backup.

- SnapDrive per UNIX supporta più di un tipo di file system e volume manager su determinate piattaforme.

Il file system e il gestore dei volumi utilizzati per i file di database devono essere specificati nel file di configurazione SnapDrive come file system e gestore dei volumi predefiniti.

- SnapManager supporta i database sui sistemi storage MultiStore con i seguenti requisiti:
  - È necessario configurare SnapDrive per impostare le password per i sistemi di storage MultiStore.
  - SnapDrive non può creare una copia Snapshot di un LUN o di un file che risiede in un qtree in un sistema di storage MultiStore se il volume sottostante non si trova nello stesso sistema di storage MultiStore.
- SnapManager non supporta l'accesso a due server SnapManager in esecuzione su porte diverse da un singolo client (entrambi dalla CLI o dalla GUI).

I numeri di porta devono essere gli stessi per gli host di destinazione e remoti.

- Tutte le LUN all'interno di un volume devono trovarsi a livello di volume o all'interno di qtree, ma non entrambe.

Questo perché se i dati risiedono sui qtree e si monta il volume, i dati all'interno dei qtree non sono protetti.

- Le operazioni SnapManager non riescono e non è possibile accedere alla GUI quando il database del repository non è attivo.



È necessario verificare che il database del repository sia in esecuzione quando si eseguono operazioni SnapManager.

- SnapManager non supporta la mobilità delle partizioni live (LPM) e la mobilità delle applicazioni live (LAM).
- SnapManager non supporta Oracle Wallet Manager e la crittografia trasparente dei dati (TDE).
- SnapManager non supporta le configurazioni MetroCluster in ambienti RDM (raw device mapping) perché le configurazioni MetroCluster devono ancora essere supportate dalla console di storage virtuale (VSC).

### Limitazioni relative alla gestione del profilo

- Se si aggiorna il profilo per separare i backup del registro di archiviazione, non è possibile eseguire un'operazione di rollback sull'host.
- Se si abilita un profilo dalla GUI per creare backup del registro di archiviazione e in seguito si tenta di aggiornare il profilo utilizzando la finestra Multi Profile Update (aggiornamento multiprofilo) o la finestra Profile Update (aggiornamento profilo), non è possibile modificare tale profilo per creare un backup completo.
- Se si aggiornano più profili nella finestra Multi Profile Update (aggiornamento multiprofilo) e alcuni profili hanno l'opzione **Backup Archives separatamente** attivata e altri profili hanno l'opzione disattivata, l'opzione **Backup Archives separatamente** viene disattivata.
- Se si aggiornano più profili e alcuni profili hanno l'opzione **Backup Archives separatamente** attivata e altri profili hanno l'opzione disattivata, l'opzione **Backup Archives separatamente** nella finestra Multi Profile Update viene disattivata.
- Se si rinomina il profilo, non è possibile eseguire il rollback dell'host.

### Limitazioni relative alle operazioni di rollback o aggiornamento in corso

- Se si tenta di installare una versione precedente di SnapManager per un host senza eseguire l'operazione di rollback sull'host nel repository, potrebbe non essere possibile effettuare le seguenti operazioni:
  - Visualizzare i profili creati con versioni precedenti o successive di SnapManager per l'host.
  - Accesso a backup o cloni creati in versioni precedenti o successive di SnapManager.
  - Eseguire operazioni di rollback o upgrade rollback sull'host.
- Dopo aver separato i profili per creare i backup del registro di archiviazione, non è possibile eseguire un'operazione di rollback sul relativo repository host.

### Limitazioni relative alle operazioni di backup

- La creazione del backup potrebbe non riuscire se si eseguono contemporaneamente operazioni SnapManager sullo stesso host su un database ASM diverso.
- Durante il ripristino, se il backup è già stato montato, SnapManager non esegue nuovamente il montaggio e utilizza il backup già montato.

Se il backup viene montato da un altro utente e non si dispone dell'accesso al backup precedentemente montato, l'altro utente deve fornire l'autorizzazione.

Tutti i file di log dell'archivio dispongono dei permessi di lettura per gli utenti assegnati a un gruppo; se il backup viene montato da un altro gruppo di utenti, potrebbe non essere possibile accedere ai file di log dell'archivio. Gli utenti possono concedere manualmente l'autorizzazione ai file di registro dell'archivio montati, quindi riprovare l'operazione di ripristino o ripristino.

- SnapManager imposta lo stato di backup come "PROTECTED", anche quando una delle copie Snapshot

del backup del database viene trasferita al sistema di storage secondario.

- È possibile utilizzare il file delle specifiche delle attività per il backup pianificato solo da SnapManager 3.2 o versione successiva.
- Quando un'operazione di backup o clone viene eseguita simultaneamente sui database RAC 10gR2 e 11gR2 su ASM, una delle operazioni di backup o creazione dei cloni non riesce.

Questo errore è dovuto a una nota limitazione di Oracle.

- SnapManager integrato con Protection Manager supporta il backup di più volumi nello storage primario su un singolo volume nello storage secondario per SnapVault e qtree SnapMirror.

Il dimensionamento dinamico del volume secondario non è supportato. Per ulteriori informazioni, consultare la Provisioning Manager and Protection Manager Administration Guide for Use with DataFabric Manager Server 3.8.

- SnapManager non supporta il vaulting dei backup mediante lo script di post-elaborazione.
- Se il database del repository punta a più di un indirizzo IP e ciascun indirizzo IP ha un nome host diverso, l'operazione di pianificazione del backup viene eseguita correttamente per un indirizzo IP, ma non riesce per l'altro indirizzo IP.
- Dopo l'aggiornamento a SnapManager 3.4 o versioni successive, non è possibile aggiornare i backup pianificati con gli script di post-elaborazione che utilizzano SnapManager 3.3.1.

È necessario eliminare la pianificazione esistente e crearne una nuova.

### **Limitazioni relative alle operazioni di ripristino**

- Quando si utilizza un metodo indiretto per eseguire un'operazione di ripristino e i file di registro dell'archivio necessari per il ripristino sono disponibili solo nei backup dal sistema di storage secondario, SnapManager non riesce a ripristinare il database.

Questo perché SnapManager non può montare il backup dei file di log dell'archivio dal sistema di storage secondario.

- Quando SnapManager esegue un'operazione di ripristino del volume, le copie di backup del registro di archiviazione eseguite dopo il ripristino del backup corrispondente non vengono eliminate.

Quando i file di dati e la destinazione del file di log di archiviazione esistono sullo stesso volume, è possibile ripristinare i file di dati mediante un'operazione di ripristino del volume se non sono disponibili file di log di archiviazione nella destinazione del file di log di archiviazione. In questo scenario, le copie Snapshot del registro di archiviazione create dopo il backup dei file di dati vengono perse.

Non eliminare tutti i file di log dell'archivio dalla destinazione del log dell'archivio.

- In un ambiente ASM, se i file OCR (Oracle Cluster Registry) e di voting coesistono in un gruppo di dischi che contiene file di dati, l'operazione di anteprima del ripristino rapido visualizza la struttura di directory errata per il disco OCR e il disco di voting.

### **Limitazioni relative alle operazioni di cloni**

- Non è possibile visualizzare valori numerici compresi tra 0 e 100 per l'avanzamento dell'operazione di suddivisione del clone a causa della velocità con cui gli inode vengono rilevati ed elaborati dal sistema di storage che contiene il volume flessibile.

- SnapManager non supporta la ricezione di e-mail solo per le operazioni di suddivisione dei cloni riuscite.
- SnapManager supporta solo la suddivisione di un FlexClone.
- La clonazione del backup del database online del database RAC che utilizza la posizione esterna del file di log dell'archivio non riesce a causa di un errore di ripristino.

La clonazione non riesce perché Oracle non riesce a trovare e applicare i file di log dell'archivio per il ripristino dalla posizione del log dell'archivio esterno. Si tratta di un limite Oracle. Per ulteriori informazioni, vedere l'ID bug Oracle: 13528007. Oracle non applica il log di archiviazione dalla posizione non predefinita in "[Sito di supporto Oracle](#)". È necessario disporre di un nome utente e di una password Oracle metalink validi.

- SnapManager 3.3 o versioni successive non supporta l'utilizzo del file XML delle specifiche dei cloni creato nelle release precedenti a SnapManager 3.2.
- Se gli spazi delle tabelle temporanei si trovano in una posizione diversa da quella dei file di dati, un'operazione di clonazione crea gli spazi delle tabelle nella posizione dei file di dati.

Tuttavia, se gli spazi delle tabelle temporanei sono file gestiti Oracle (OMF) che si trovano in una posizione diversa da quella dei file di dati, l'operazione di clonazione non crea gli spazi delle tabelle nella posizione dei file di dati. Gli OMF non sono gestiti da SnapManager.

- SnapManager non riesce a clonare un database RAC se si seleziona l'opzione -resetlogs.

### **Limitazioni relative ai file di log e ai backup dell'archivio**

- SnapManager non supporta l'eliminazione dei file di log dell'archivio dalla destinazione dell'area di ripristino flash.
- SnapManager non supporta l'eliminazione dei file di log dell'archivio dalla destinazione di standby.
- I backup del registro di archiviazione vengono conservati in base alla durata della conservazione e alla classe di conservazione oraria predefinita.

Quando la classe di conservazione del backup del registro di archiviazione viene modificata utilizzando l'interfaccia utente grafica o l'interfaccia utente grafica di SnapManager, la classe di conservazione modificata non viene considerata per il backup, in quanto i backup del registro di archiviazione vengono conservati in base alla durata della conservazione.

- Se si eliminano i file di log dell'archivio dalle destinazioni del log dell'archivio, il backup del log dell'archivio non include i file di log dell'archivio precedenti al file di log dell'archivio mancante.

Se manca l'ultimo file di log dell'archivio, l'operazione di backup del log dell'archivio non riesce.

- Se si eliminano i file di log dell'archivio dalle destinazioni del log dell'archivio, l'eliminazione dei file di log dell'archivio non riesce.
- SnapManager consolida i backup del log di archiviazione anche quando si eliminano i file di log di archiviazione dalle destinazioni del log di archiviazione o quando i file di log di archiviazione sono corrotti.

### **Limitazioni relative alla modifica del nome host del database di destinazione**

Le seguenti operazioni SnapManager non sono supportate quando si modifica il nome host del database di destinazione:

- Modifica del nome host del database di destinazione dalla GUI di SnapManager.
- Eseguire il rollback del database del repository dopo aver aggiornato il nome host del database di

destinazione del profilo.

- Aggiornamento simultaneo di più profili per un nuovo nome host del database di destinazione.
- Modifica del nome host del database di destinazione quando è in esecuzione un'operazione SnapManager.

### **Limitazioni relative alla CLI o alla GUI di SnapManager**

- I comandi dell'interfaccia utente di SnapManager per l'operazione di creazione del profilo generati dall'interfaccia utente grafica di SnapManager non dispongono di opzioni di configurazione della cronologia.

Non è possibile utilizzare il comando di creazione del profilo per configurare le impostazioni di conservazione della cronologia dall'interfaccia utente di SnapManager.

- SnapManager non visualizza la GUI in Mozilla Firefox quando non è disponibile alcun ambiente di runtime Java sul client UNIX.
- Durante l'aggiornamento del nome host del database di destinazione utilizzando l'interfaccia utente di SnapManager, se sono presenti una o più sessioni GUI di SnapManager aperte, tutte le sessioni GUI di SnapManager aperte non rispondono.

### **Limitazioni relative a SnapMirror e SnapVault**

- Lo script di post-elaborazione SnapVault non è supportato se si utilizza Data ONTAP in 7-Mode.
- Se si utilizza ONTAP, non è possibile eseguire SnapRestore basato su volume (VBSR) sui backup creati nei volumi che hanno stabilito relazioni SnapMirror.

Ciò è dovuto a una limitazione di ONTAP, che non consente di interrompere la relazione quando si esegue un VBSR. Tuttavia, è possibile eseguire un VBSR sull'ultimo backup o sull'ultimo backup creato solo quando i volumi hanno relazioni SnapVault stabilite.

- Se si utilizza Data ONTAP in 7-Mode e si desidera eseguire un VBSR sui backup creati nei volumi con relazioni SnapMirror stabilite, è possibile impostare l'opzione `override-vbsr-snapmirror-check` su ON in SnapDrive per UNIX.

La documentazione di SnapDrive contiene ulteriori informazioni al riguardo.

- In alcuni scenari, non è possibile eliminare l'ultimo backup associato alla prima copia Snapshot quando il volume ha una relazione SnapVault stabilita.

È possibile eliminare il backup solo quando si rompe la relazione. Questo problema è dovuto a una restrizione ONTAP con copie Snapshot di base. In una relazione SnapMirror, la copia Snapshot di base viene creata dal motore SnapMirror e, in una relazione SnapVault, la copia Snapshot di base è il backup creato utilizzando SnapManager. Per ogni aggiornamento, la copia Snapshot di base indica il backup più recente creato utilizzando SnapManager.

### **Limitazioni relative ai database Data Guard Standby**

- SnapManager non supporta i database di standby di protezione dati logica.
- SnapManager non supporta i database di standby di Active Data Guard.
- SnapManager non consente backup online dei database di standby di Data Guard.
- SnapManager non consente backup parziali dei database di standby di Data Guard.

- SnapManager non consente il ripristino dei database di standby di Data Guard.
- SnapManager non consente l'eliminazione dei file di log dell'archivio per i database di standby Data Guard.
- SnapManager non supporta Data Guard Broker.

## Informazioni correlate

["Documentazione sul sito di supporto NetApp: mysupport.netapp.com"](http://mysupport.netapp.com)

## Limitazioni di SnapManager per Clustered Data ONTAP

Se si utilizza Clustered Data ONTAP, è necessario conoscere i limiti di alcune funzionalità e delle operazioni SnapManager.

Le seguenti funzionalità non sono supportate se si utilizza SnapManager su Clustered Data ONTAP:

- Funzionalità di protezione dei dati se SnapManager è integrato con il gestore unificato di OnCommand
- Database in cui un LUN appartiene a un sistema che esegue Data ONTAP in modalità 7 e l'altro LUN appartiene a un sistema che esegue Clustered Data ONTAP
- SnapManager per Oracle non supporta la migrazione di un Vserver, che non è supportato da Clustered Data ONTAP
- SnapManager per Oracle non supporta la funzionalità Clustered Data ONTAP 8.2.1 per specificare criteri di esportazione diversi per volumi e qtree

## Limitazioni relative al database Oracle

Prima di iniziare a lavorare con SnapManager, è necessario conoscere le limitazioni relative a Oracle Database.

Le limitazioni sono le seguenti:

- SnapManager supporta le versioni di Oracle 10gR2, 11gR1, 11gR2 e 12c, ma non supporta Oracle 10gR1 come repository o database di destinazione.
- SnapManager non supporta l'utilizzo di un indirizzo IP DI SCANSIONE al posto di un nome host.

SCAN IP è una nuova funzionalità di Oracle 11gR2.

- SnapManager non supporta Oracle Cluster file System (OCFS).
- Oracle 11g in un ambiente Direct NFS (DNFS) consente configurazioni aggiuntive del punto di montaggio nel file orafstab, ad esempio percorsi multipli per il bilanciamento del carico.

SnapManager non modifica il file orafstab. È necessario aggiungere manualmente le proprietà aggiuntive che si desidera utilizzare nel database clonato, nel file orafstab.

- Il supporto per Oracle Database 9i è obsoleto da SnapManager 3.2.
- Il supporto per Oracle Database 10gR2 (versioni precedenti alla 10.2.0.5) è obsoleto rispetto a SnapManager 3.3.1.



Identificare le diverse versioni dei database Oracle supportate facendo riferimento alla matrice di interoperabilità.

## Informazioni correlate

"Matrice di interoperabilità: [support.netapp.com/NOW/products/interoperability](https://support.netapp.com/NOW/products/interoperability)"

## Versioni obsolete del database Oracle

Il database Oracle 9i non è supportato da SnapManager 3.2 o versione successiva e il database Oracle 10gR2 (versione precedente alla 10.2.0.4) non è supportato da SnapManager 3.3.1 o versione successiva.

Se si utilizzano database Oracle 9i o 10gR2 (precedenti alla 10.2.0.4) e si desidera eseguire l'aggiornamento a SnapManager 3.2 o versioni successive, non è possibile creare nuovi profili; viene visualizzato un messaggio di avviso.

Se si utilizzano database Oracle 9i o 10gR2 (precedenti alla 10.2.0.4) e si desidera eseguire l'aggiornamento a SnapManager 3.2 o versioni successive, è necessario eseguire una delle seguenti operazioni:

- Aggiornare i database Oracle 9i o 10gR2 (precedenti alla 10.2.0.4) ai database Oracle 10gR2 (10.2.0.5), 11gR1 o 11gR2, quindi eseguire l'aggiornamento a SnapManager 3.2 o 3.3.

Se si esegue l'aggiornamento a Oracle 12c, è necessario eseguire l'aggiornamento a SnapManager 3.3.1 o versione successiva.



Il database Oracle 12c è supportato solo da SnapManager 3.3.1.

- Gestire i database Oracle 9i utilizzando una versione patch di SnapManager 3.1.

È possibile utilizzare SnapManager 3.2 o 3.3 se si desidera gestire i database Oracle 10gR2, 11gR1 o 11gR2 e utilizzare SnapManager 3.3.1 o versione successiva se si desidera gestire i database Oracle 12c insieme agli altri database supportati.

## Restrizioni per la gestione dei volumi

SnapManager ha alcune restrizioni di gestione dei volumi che potrebbero influire sull'ambiente.

È possibile disporre di più gruppi di dischi per un database; tuttavia, le seguenti limitazioni si applicano a tutti i gruppi di dischi per un determinato database:

- I gruppi di dischi per il database possono essere gestiti da un solo gestore di volumi.
- I dispositivi raw supportati da un volume manager logico non sono supportati per la protezione dei dati Oracle.

Il provisioning dei gruppi di dischi di storage raw e ASM (Automatic Storage Management) deve essere eseguito direttamente sui dispositivi fisici. In alcuni casi, è necessario eseguire il partizionamento.

- Un ambiente Linux senza gestione logica dei volumi richiede una partizione.

## Informazioni sul copyright

Copyright © 2023 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.