



# **Configurazione ed esecuzione del backup protetti**

## **SnapManager Oracle**

NetApp  
October 04, 2023

# Sommario

- Configurazione ed esecuzione del backup protetti ..... 1
  - Utilizzo di SnapManager per Oracle per creare il profilo del database per un backup locale ..... 1
  - Utilizzo di Protection Manager per configurare un pool di risorse secondario ..... 2
  - Utilizzo di Protection Manager per configurare le pianificazioni di backup secondarie ..... 3
  - Utilizzo di Protection Manager per configurare un criterio di protezione di backup secondario ..... 4
  - Utilizzo di SnapManager per Oracle per creare il profilo del database e assegnare una policy di protezione ..... 6
  - Utilizzo di Protection Manager per il provisioning del nuovo set di dati ..... 7
  - Utilizzo di SnapManager per Oracle per creare un backup protetto ..... 8
  - Utilizzo di SnapManager per Oracle per confermare la protezione del backup ..... 9

# Configurazione ed esecuzione del backup protetti

È necessario configurare SnapManager e Protection Manager per supportare il backup del database sullo storage secondario. L'amministratore del database e l'amministratore dello storage devono coordinare le proprie azioni.

## Utilizzo di SnapManager per Oracle per creare il profilo del database per un backup locale

Gli amministratori del database utilizzano SnapManager per creare un profilo di database che verrà utilizzato per avviare un backup sullo storage locale su un sistema di storage primario. L'intero processo di creazione del profilo e di backup viene eseguito interamente in SnapManager, ma non in Gestione protezione.

Un profilo contiene le informazioni sul database gestito, incluse le credenziali, le impostazioni di backup e le impostazioni di protezione per i backup. Creando un profilo, non è necessario specificare i dettagli del database ogni volta che si esegue un'operazione sul database, ma fornire semplicemente il nome del profilo. Un profilo può fare riferimento a un solo database. Lo stesso database può essere referenziato da più profili.

1. Accedere al client SnapManager per Oracle.
2. Nella struttura dei repository SnapManager, fare clic con il pulsante destro del mouse sull'host che si desidera associare al profilo e selezionare **Crea profilo**.
3. Nella pagina Profile Configuration Information (informazioni configurazione profilo), immettere le seguenti informazioni e fare clic su **Next** (Avanti).
  - Nome profilo: Payroll\_prod
  - Password del profilo: Payroll123
  - Commento: Database Payroll di produzione
4. Nella pagina Database Configuration Information (informazioni configurazione database), immettere le seguenti informazioni e fare clic su **Next** (Avanti).
  - Nome database: PAYDB
  - SID del database: Payrolldb
  - Host database: Accettare l'impostazione predefinita

Poiché si sta creando un profilo da un host nella struttura del repository, SnapManager visualizza il nome host.

5. Nella seconda pagina Database Configuration Information (informazioni di configurazione del database), accettare le seguenti informazioni e fare clic su **Next** (Avanti):
  - Host account, che rappresenta l'account utente Oracle: oracle
  - Host Group, che rappresenta il gruppo Oracle: dba
6. Nella pagina Database Connection Information (informazioni connessione database), selezionare **Use database Authentication** (Usa autenticazione database) per consentire agli utenti di autenticarsi utilizzando le informazioni del database.

Per questo esempio, inserire le seguenti informazioni e fare clic su **Avanti**.

- SYSDBA Privileged User Name (Nome utente privilegiato SYSDBA), che rappresenta l'amministratore del database di sistema con privilegi amministrativi: SYS
- Password (SYSDBA password): oracle
- Porta per la connessione all'host del database: 1521

7. Nella pagina RMAN Configuration Information (informazioni configurazione RMAN), selezionare **Do not use RMAN** (non utilizzare RMAN) e fare clic su **Next** (Avanti).

Oracle Recovery Manager (RMAN) è uno strumento Oracle che consente di eseguire il backup e il ripristino dei database Oracle utilizzando il rilevamento a livello di blocco.

8. Nella pagina Snapshot Naming Information, specificare una convenzione di denominazione per le istantanee associate a questo profilo selezionando Variables (variabili). L'unica variabile richiesta è la variabile **smid**, che crea un identificatore di snapshot univoco.

Per questo esempio, procedere come segue:

- Nell'elenco Variable Token (token variabile), selezionare la variabile **{usertext}** e fare clic su **Add** (Aggiungi).
- Inserire "payroll.techco.com\_" come nome host e fare clic su **OK**.
- Fare clic su **sinistra** fino a visualizzare il nome host subito dopo "smo" nella casella Format (formato).
- Fare clic su **Avanti**.

La convenzione di naming Snapshot di smo\_hostname\_smoprofile\_dbsid\_scope\_mode\_smid diventa "smo\_payroll.techco.com\_payroll\_prod2\_payrolldb\_f\_a\_x" (dove "f" indica un backup completo, "a" indica la modalità automatica e "x" rappresenta L'SMID univoco).

9. Nella pagina Perform operation (Esegui operazione), verificare le informazioni e fare clic su **Create** (Crea).
10. Fare clic su **Dettagli operazione** per visualizzare le informazioni sull'operazione di creazione del profilo e sull'idoneità al ripristino basato sul volume.

## Utilizzo di Protection Manager per configurare un pool di risorse secondario

Per supportare il backup del database sullo storage secondario, l'amministratore dello storage utilizza Gestione protezione per organizzare i sistemi di storage secondari abilitati con la licenza secondaria SnapVault in un pool di risorse per i backup.

Idealmente, i sistemi storage in un pool di risorse sono intercambiabili in termini di accettabilità come destinazioni per i backup. Ad esempio, quando si sviluppa la strategia di protezione per il database delle retribuzioni, l'amministratore dello storage ha identificato i sistemi storage secondari con performance e livelli di servizio simili, che sarebbero stati membri idonei dello stesso pool di risorse.

Sono già stati creati aggregati di spazio inutilizzato nei sistemi storage che si intende assegnare ai pool di risorse. In questo modo si garantisce uno spazio sufficiente per contenere i backup.

1. Accedere alla NetApp Management Console di Protection Manager.
2. Dalla barra dei menu, fare clic su **Data > Resource Pools**.

Viene visualizzata la finestra Resource Pools (pool di risorse).

3. Fare clic su **Aggiungi**.

Viene avviata la procedura guidata Aggiungi pool di risorse.

4. Completare la procedura guidata per creare il pool di risorse **paydb\_backup\_resource**.

Utilizzare le seguenti impostazioni:

- Nome: Utilizzare **paydb-backup\_resource**
- Soglie di spazio (utilizzare le impostazioni predefinite):
  - Soglie di utilizzo dello spazio: Attivate
  - Soglia quasi completa (per pool di risorse): 80%
  - Soglia completa (per il pool di risorse): 90%

## Utilizzo di Protection Manager per configurare le pianificazioni di backup secondarie

Per supportare il backup del database sullo storage secondario, l'amministratore dello storage utilizza Protection Manager per configurare una pianificazione di backup.

Prima di configurare la pianificazione per i backup secondari, l'amministratore dello storage consegna al partner DBA le seguenti informazioni:

- La pianificazione che il DBA desidera seguire per i backup secondari.

In questo caso, i backup una volta al giorno si verificano alle 19:00. Inoltre, i backup una volta alla settimana vengono eseguiti il sabato alle 1:00.

- a. Accedere alla console di gestione NetApp di Protection Manager.
- b. Dalla barra dei menu, fare clic su **Policy > Protection > Schedules**.

Viene visualizzata la scheda programmi della finestra Criteri di protezione.

- c. Selezionare il programma giornaliero **giornaliero alle 20:00** nell'elenco dei programmi.
- d. Fare clic su **Copy** (Copia).

Nell'elenco viene visualizzato un nuovo programma giornaliero, **Copy of Daily at 20:00**. È già selezionato.

- e. Fare clic su **Edit** (Modifica).

La scheda delle proprietà Modifica pianificazione giornaliera si apre nella scheda Pianificazione.

- f. Modificare il nome del programma in **Payroll Daily at 19.00**, aggiornare la descrizione, quindi fare clic su **Apply** (Applica).

Le modifiche vengono salvate.

- g. Fare clic sulla scheda **Eventi giornalieri**.

Il tempo di backup giornaliero corrente del programma è di 20:00 viene visualizzato.

- h. Fare clic su **Add** (Aggiungi) e immettere **7:00 PM** nel nuovo campo Time (ora), quindi fare clic su **Apply** (Applica).

Il tempo di backup giornaliero corrente della pianificazione è ora alle 19:00

- i. Fare clic su **OK** per salvare le modifiche e uscire dalla scheda delle proprietà.

Il nuovo programma giornaliero, **Payroll Daily at 19.00**, viene visualizzato nell'elenco dei programmi.

- j. Selezionare il programma settimanale **Domenica alle 20:00 più giornaliero** nell'elenco dei programmi.

- k. Fare clic su **Copy** (Copia).

Un nuovo programma settimanale, **Copia di domenica alle 20:00 più giornaliero**, viene visualizzato nell'elenco. È già selezionato.

- l. Fare clic su **Edit** (Modifica).

La scheda delle proprietà Modifica pianificazione settimanale si apre nella scheda Pianificazione.

- m. Modificare il nome del programma in **Payroll Saturday at 1 AM più Daily at 7 PM** e aggiornare la descrizione.

- n. Dall'elenco a discesa **Daily Schedule** (programma giornaliero), selezionare il programma giornaliero appena creato, **Payroll Daily at 19.00**.

Selezionando **Payroll Daily alle 19:00**, questo programma definisce il momento in cui le operazioni giornaliere si verificano quando il programma **Payroll Saturday alle 1:00 più giornaliero alle 19:00** viene applicato a una policy.

- o. Fare clic su **OK** per salvare le modifiche e uscire dalla scheda delle proprietà.

Il nuovo programma settimanale, **Payroll Saturday at 1 AM più Daily at 7 PM**, viene visualizzato nell'elenco dei programmi.

## Utilizzo di Protection Manager per configurare un criterio di protezione di backup secondario

Dopo aver configurato la pianificazione di backup, l'amministratore dello storage configura un criterio di backup storage protetto in cui includere tale pianificazione.

Prima di configurare il criterio di protezione, l'amministratore dello storage conferisce al partner DBA le seguenti informazioni:

- Durata della conservazione da specificare per lo storage secondario
- Tipo di protezione dello storage secondario richiesta

La policy di protezione creata può essere elencata in SnapManager per Oracle dal partner DBA e assegnata a un profilo di database per i dati da proteggere.

1. Accedere alla NetApp Management Console di Protection Manager.

2. Dalla barra dei menu, fare clic su **Criteri > protezione > Panoramica**.

Viene visualizzata la scheda Overview (Panoramica) della finestra Protection Policies (Criteri di protezione).

3. Fare clic su **Add Policy** (Aggiungi policy) per avviare la procedura guidata Add Protection Policy (Aggiungi policy di protezione).

4. Completare la procedura guidata seguendo questa procedura:

a. Specificare un nome di policy descrittivo.

Per questo esempio, inserire **dati TechCo Payroll: Backup** e una descrizione, quindi fare clic su **Avanti**.

b. Selezionare un criterio di base.

Per questo esempio, selezionare **Backup** e fare clic su **Avanti**.

c. Nella scheda delle proprietà nodo dati primario, accettare le impostazioni predefinite e fare clic su **Avanti**.



In questo esempio, viene applicata la pianificazione di backup locale configurata in SnapManager. Qualsiasi pianificazione di backup locale specificata utilizzando questo metodo viene ignorata.

d. Nella scheda delle proprietà connessione dati primari a backup, selezionare una pianificazione di backup.

Per questo esempio, selezionare **Payroll Saturday at 1 AM più Daily at 7 PM** come programma di backup, quindi fare clic su **Next**.

In questo esempio, la pianificazione selezionata include sia la pianificazione settimanale che quella giornaliera precedentemente configurate.

e. Nella scheda delle proprietà Backup policy, specificare il nome del nodo di backup e i tempi di conservazione per i backup giornalieri, settimanali o mensili.

Per questo esempio, specificare una conservazione giornaliera del backup di 10 giorni e una conservazione settimanale del backup di 52 settimane. Dopo aver completato ogni scheda delle proprietà, fare clic su **Avanti**.

Una volta completati tutti i fogli delle proprietà, la procedura guidata Aggiungi criterio di protezione visualizza un riepilogo del criterio di protezione che si desidera creare.

5. Fare clic su **fine** per salvare le modifiche.

La policy di protezione **TechCo Payroll Data: Backup** è elencata tra le altre policy configurate per Protection Manager.

Il partner DBA può ora utilizzare SnapManager per Oracle per elencare e assegnare questa policy durante la creazione del profilo di database per i dati da proteggere.

# Utilizzo di SnapManager per Oracle per creare il profilo del database e assegnare una policy di protezione

È necessario creare un profilo in SnapManager per Oracle, attivare la protezione nel profilo e assegnare un criterio di protezione per creare un backup protetto.

Un profilo contiene informazioni sul database gestito, incluse le credenziali, le impostazioni di backup e le impostazioni di protezione per i backup. Dopo aver creato un profilo, non è necessario specificare i dettagli del database ogni volta che si esegue un'operazione. Un profilo può fare riferimento a un solo database, ma lo stesso database può essere referenziato da più profili.

1. Accedere al client SnapManager per Oracle.
2. Nella struttura dei repository, fare clic con il pulsante destro del mouse sull'host e selezionare **Create Profile** (Crea profilo).
3. Nella pagina Profile Configuration Information (informazioni configurazione profilo), inserire i dettagli del profilo e fare clic su **Next** (Avanti).

È possibile inserire le seguenti informazioni:

- Nome del profilo: Payroll\_prod2
  - Password del profilo: Payroll123
  - Commento: Database Payroll di produzione
4. Nelle pagine Database Configuration Information (informazioni configurazione database), immettere i dettagli del database e fare clic su **Next** (Avanti).

È possibile inserire le seguenti informazioni:

- Nome database: PAYDB
  - SID del database: Payrolldb
  - Host database: Accettare l'impostazione predefinita. Poiché si sta creando un profilo da un host nella struttura del repository, SnapManager visualizza il nome host.
  - Host account, che rappresenta l'account utente Oracle: oracle
  - Host Group, che rappresenta il gruppo Oracle: dba
5. Nella pagina Database Connection Information (informazioni connessione database), fare clic su **Use database Authentication** (Usa autenticazione database) per consentire agli utenti di autenticarsi utilizzando le informazioni del database.
  6. Inserire i dettagli di connessione al database e fare clic su **Avanti**.

È possibile inserire le seguenti informazioni:

- SYSDBA Privileged User Name (Nome utente privilegiato SYSDBA), che rappresenta l'amministratore del database di sistema con privilegi amministrativi: SYS
  - Password (SYSDBA password): oracle
  - Porta per la connessione all'host del database: 1521
7. Nella pagina RMAN Configuration Information (informazioni di configurazione RMAN), fare clic su **Do not use RMAN** (non utilizzare RMAN) e fare clic su **Next** (Avanti).



Oracle Recovery Manager (RMAN) è uno strumento Oracle che consente di eseguire il backup e il ripristino dei database Oracle utilizzando il rilevamento a livello di blocco.

8. Nella pagina Snapshot Naming Information, specificare una convenzione di denominazione per le istantanee associate a questo profilo selezionando Variables (variabili).

La variabile smid crea un identificatore di snapshot univoco.

Effettuare le seguenti operazioni:

- a. Nell'elenco Variable Token (token variabile), selezionare usertext e fare clic su **Add** (Aggiungi).
- b. Inserire payroll.techco.com\_ come nome host e fare clic su **OK**.
- c. Fare clic su **sinistra** fino a visualizzare il nome host subito dopo smo nella casella Format (formato).
- d. Fare clic su **Avanti**.

La convenzione di naming Snapshot di smo\_hostname\_smoprofile\_dbsid\_scope\_mode\_smid diventa "smo\_payroll.techco.com\_payroll\_prod2\_payrolldb\_f\_a\_x" (dove "f" indica un backup completo, "a" indica la modalità automatica e "x" rappresenta L'SMID univoco).

9. Selezionare **Protection Manager Protection Policy**.

La **Protection Manager Protection Policy** consente di selezionare una policy di protezione configurata utilizzando la NetApp Management Console.

10. Selezionare **TechCo Payroll Data: Backup** come policy di protezione dalle policy di protezione recuperate da NetApp Management Console e fare clic su **Avanti**.
11. Nella pagina Perform operation (Esegui operazione), verificare le informazioni e fare clic su **Create** (Crea).
12. Fare clic su **Dettagli operazione** per visualizzare le informazioni sull'operazione di creazione del profilo e sull'idoneità al ripristino basato sul volume.
  - L'assegnazione di una policy di protezione della console di gestione NetApp al profilo del database crea automaticamente un set di dati non conforme, visibile all'operatore della console di gestione NetApp, con la convenzione di denominazione smo\_<hostname>\_<profilenome> o, in questo esempio, smo\_payroll.tech.com\_PAYDB.
  - Se il profilo non è idoneo per il ripristino del volume (chiamato anche "ripristino rapido"), si verifica quanto segue:
    - La scheda **risultati** indica che la creazione del profilo è riuscita e che si sono verificati degli avvisi durante l'operazione.
    - La scheda **Dettagli operazione** include un registro DI AVVISO che indica che il profilo non è idoneo per il ripristino rapido e spiega il motivo.

## Utilizzo di Protection Manager per il provisioning del nuovo set di dati

Una volta creato il set di dati smo\_paydb, l'amministratore dello storage utilizza Protection Manager per assegnare le risorse del sistema storage per il provisioning del nodo di backup del set di dati.

Prima di eseguire il provisioning del dataset appena creato, l'amministratore dello storage conferisce al partner DBA il nome del dataset specificato nel profilo.

In questo caso, il nome del dataset è `smo_payroll.tech.com_PAYDB`.

1. Accedere alla NetApp Management Console di Protection Manager.
2. Dalla barra dei menu, fare clic su **dati > dataset > Panoramica**.

Nella scheda dataset della finestra dataset viene visualizzato un elenco di set di dati che include il set di dati appena creato tramite SnapManager.

3. Individuare e selezionare il set di dati **smo\_payroll.tech.com\_PAYDB**.

Quando si seleziona questo set di dati, l'area del grafico visualizza il set di dati `smo_paydb` con il relativo nodo di backup senza provisioning. Lo stato di conformità viene contrassegnato come non conforme.

4. Con il set di dati `smo_paydb` ancora evidenziato, fare clic su **Edit** (Modifica).

NetApp Management Console di Protection Manager visualizza la finestra Edit Dataset (Modifica dataset) per il set di dati **smo\_payroll.tech.com\_PAYDB**. Il riquadro di navigazione della finestra visualizza le opzioni di configurazione per il nodo primario del dataset, la connessione di backup e il nodo di backup.

5. Dal riquadro di navigazione, individuare le opzioni per il nodo di backup del dataset e selezionare **provisioning/resource pool**.

La finestra Edit Dataset (Modifica set di dati) visualizza un'impostazione per il criterio di provisioning predefinito e un elenco di pool di risorse disponibili.

6. Per questo esempio, selezionare il pool di risorse **paydb\_backup\_resource** e fare clic su **>**.

Il pool di risorse selezionato viene elencato nel campo "Pool di risorse per questo nodo".

7. Fare clic su **fine** per salvare le modifiche.

Protection Manager effettua automaticamente il provisioning del nodo di backup secondario con le risorse del pool di risorse `paydb_backup_resource`.

## Utilizzo di SnapManager per Oracle per creare un backup protetto

Quando si crea un backup per questo esempio, l'amministratore di database sceglie di creare un backup completo, di impostare le opzioni di backup e di selezionare la protezione sullo storage secondario. Sebbene il backup venga eseguito inizialmente sullo storage locale, poiché si basa su un profilo abilitato alla protezione, il backup viene quindi trasferito allo storage secondario in base alla pianificazione del criterio di protezione, come definito in Protection Manager.

1. Accedere al client SnapManager per Oracle.
2. Nella struttura ad albero del repository SnapManager, fare clic con il pulsante destro del mouse sul profilo contenente il database di cui si desidera eseguire il backup e selezionare **Backup**.

Viene avviata la procedura guidata di backup di SnapManager per Oracle.

3. Inserire `Production_payroll` come etichetta.

4. Inserire il backup del libro paga di produzione gennaio 19 come commento.
5. Selezionare **Auto** come tipo di backup che si desidera creare.

Ciò consente a SnapManager di determinare se eseguire un backup online o offline.

6. Selezionare **Daily** o **Weekly** come frequenza del backup.
7. Per confermare che il backup è in un formato valido per Oracle, selezionare la casella accanto a **verify backup** (verifica backup).

Questa operazione utilizza Oracle DBVerify per controllare il formato e la struttura del blocco.

8. Per forzare lo stato del database nella modalità appropriata (ad esempio, da aperto a montato), selezionare **Allow startup or shutdown of database, se necessario**, e fare clic su **Next** (Avanti).
9. Nella pagina Database, tablespace o file di dati per il backup, selezionare **Backup completo** e fare clic su **Avanti**.
10. Per proteggere il backup sullo storage secondario, selezionare **Protect the Backup** (protezione backup) e fare clic su **Next** (Avanti).
11. Nella pagina Perform operation (Esegui operazione), verificare le informazioni fornite e fare clic su **Backup**.
12. Nella pagina avanzamento, visualizzare lo stato di avanzamento e i risultati della creazione del backup.
13. Per visualizzare i dettagli dell'operazione, fare clic su **Dettagli operazione**.

## Utilizzo di SnapManager per Oracle per confermare la protezione del backup

Utilizzando SnapManager per Oracle, è possibile visualizzare un elenco di backup associati a un profilo, determinare se i backup sono stati abilitati per la protezione e visualizzare la classe di conservazione (giornaliera o settimanale, in questo esempio).

All'inizio, il nuovo backup in questo esempio viene mostrato come pianificato per la protezione, ma non ancora protetto (nell'interfaccia grafica utente di SnapManager e nell'output del comando di backup show). Dopo che l'amministratore dello storage ha verificato che il backup è stato copiato nello storage secondario, SnapManager modifica lo stato di protezione del backup da "Not Protected" (non protetto) a "Protected" (protetto) nell'interfaccia utente grafica e con il comando dell'elenco di backup.

1. Accedere al client SnapManager per Oracle.
2. Nella struttura ad albero del repository SnapManager, espandere il profilo per visualizzarne i backup.
3. Fare clic sulla scheda **Backup/cloni**.
4. Nel riquadro Report, selezionare **Dettagli backup**.
5. Visualizzare la colonna protezione e verificare che lo stato sia "protetto".

## 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.