



Amministrazione per UNIX

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 on October 04, 2023. Always check docs.netapp.com for the latest.

Sommario

Guida all'amministrazione per UNIX®	1
Panoramica del prodotto	1
Creare backup utilizzando copie Snapshot	28
Perché è necessario ridurre i file di log dell'archivio	29
Consolidamento dei log di archiviazione	29
Ripristino completo o parziale del database	29
Verificare lo stato del backup	30
Cloni di backup del database	30
Tieni traccia dei dettagli e genera report	30
Quali repository sono	31
Quali sono i profili	31
Quali sono gli stati operativi di SnapManager	33
In che modo SnapManager mantiene la sicurezza	34
Accesso e stampa della Guida in linea	35
Layout generali del database e configurazioni di storage consigliati	36
Limitazioni quando si lavora con SnapManager	48
Aggiornamento di SnapManager	55
Configurazione di SnapManager	67
Sicurezza e gestione delle credenziali	78
Gestione dei profili per backup efficienti	88
Backup del database	105
Pianificazione dei backup del database	139
Ripristino dei backup del database	144
Backup del database di cloning	184
Introduzione alla protezione dei dati in SnapManager	202
SnapManager per Oracle utilizza Protection Manager per proteggere un backup del database	219
Esecuzione delle operazioni di gestione	236
Configurazione di una notifica via email	239
Creazione di script e file di specifica delle attività per le operazioni SnapManager	246
Aggiornamento del nome del sistema di storage e del nome host del database di destinazione associati a un profilo	269
Mantenere la cronologia delle operazioni SnapManager	272
Riferimento al comando SnapManager per Oracle	275
Risoluzione dei problemi di SnapManager	387
Classificazioni dei messaggi di errore	419
Messaggi di errore	421

Guida all'amministrazione per UNIX®

Questa guida descrive come amministrare SnapManager 3.4.2 per Oracle in un ambiente UNIX dopo il completamento dell'implementazione, incluse le procedure di configurazione, aggiornamento e disinstallazione del prodotto, backup, ripristino e clonazione dei database.

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"

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.

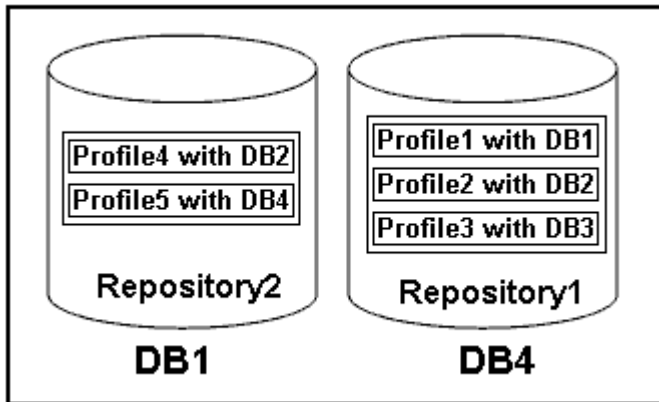
Quali sono i profili

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 Schedule 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. Nota: 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:

Sistema operativo	Partizione singola	Partizione multipla	Dispositivi senza partizione	File system o dispositivi RAW
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 initasm disk 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 initasm disks 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	Si	Acceso
File di dati	oradata_sid	Si	Spento
File di dati temporanei	oatemp_sid	Si	Spento
File di controllo	Oacntrl01_sid (multiplex) Oacntrl02_sid (multiplex)	Si	Spento
Registri di ripristino	Oralog01_sid (multiplex) Oralog02_sid (multiplex)	Si	Spento
Registri di archiviazione	oraarch_sid	Si	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	Si	Acceso
File di dati	oradata_dbname	Si	Spento
File di dati temporanei	ortamp_dbname	Si	Spento

Tipi di file	Nomi dei volumi	Volume dedicato per i tipi di file	Copie Snapshot automatiche
File di controllo	Oracntrl01_dbname (multiplex) Oracntrl02_dbname (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_dbname (multiplato) 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)

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) Oacntrl02_sid (multiplex)	Oracntrl01_sidlun (multiplex) Oracntrl02_sidlun (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_dbname (multiplato) 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 (multiplato)	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"

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.

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.

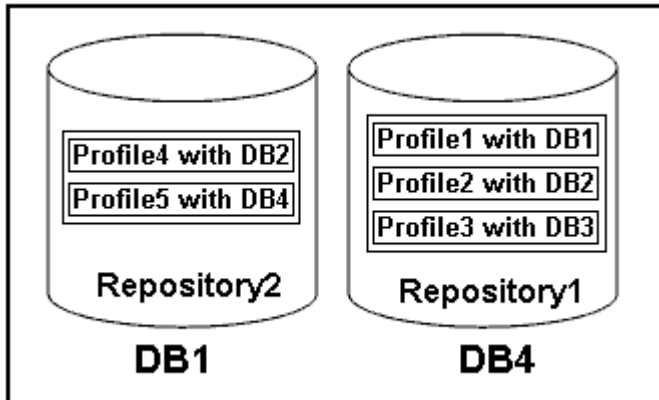
Quali sono i profili

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 Schedule 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.
Non riuscito	Operazione non riuscita. SnapManager ha eseguito automaticamente il processo di interruzione e ha pulito l'operazione. Nota: 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.Persistete` 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

Sistema operativo host	Percorso del file
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:

Sistema operativo	Partizione singola	Partizione multipla	Dispositivi senza partizione	File system o dispositivi RAW
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 initasm disk 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 initasm disks 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
```



```
# 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

Tipi di file	Nomi dei volumi	Volume dedicato per i tipi di file	Copie Snapshot automatiche
File di controllo	Oracntrl01_dbname (multiplex) Oracntrl02_dbname (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_dbname (multiplato) 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)

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) Oacntrl02_sid (multiplex)	Oracntrl01_sidlun (multiplex) Oracntrl02_sidlun (multiplex)	Sì	Spento
Registri di ripristino	Oralog01_dbname (multiplato) 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) 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
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"

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.

Aggiornamento di SnapManager

Puoi eseguire l'aggiornamento alla versione più recente di SnapManager per Oracle da

una qualsiasi delle versioni precedenti. È possibile aggiornare tutti gli host SnapManager contemporaneamente o eseguire un aggiornamento in sequenza, che consente di aggiornare gli host in modo sfalsato, host per host.

Preparazione all'aggiornamento di SnapManager

L'ambiente in cui si desidera aggiornare SnapManager deve soddisfare i requisiti specifici di software, hardware, browser, database e sistema operativo. Per informazioni aggiornate sui requisiti, consulta la matrice di interoperabilità.

Prima di eseguire l'aggiornamento, assicurarsi di eseguire le seguenti attività:

- Completare le attività di preinstallazione richieste.
- Scarica il pacchetto di installazione più recente di SnapManager per Oracle.
- Installare e configurare la versione appropriata di SnapDrive per UNIX su tutti gli host di destinazione.
- Creare un backup del database repository SnapManager per Oracle esistente.

"Matrice di interoperabilità: support.netapp.com/NOW/products/interoperability"

Aggiornamento degli host SnapManager

È possibile aggiornare tutti gli host esistenti per utilizzare la versione più recente di SnapManager. Tutti gli host vengono aggiornati simultaneamente. Tuttavia, questo potrebbe causare il downtime di tutti gli host SnapManager e delle operazioni pianificate durante tale periodo.

1. Accedere al sistema host come utente root.
2. Dall'interfaccia della riga di comando (CLI), accedere alla posizione in cui è stato scaricato il file di installazione.
3. Se il file non è eseguibile, modificare le autorizzazioni: `chmod 544 netapp.smo*`
4. Arrestare il server SnapManager: `smo_server stop`
5. A seconda dell'host UNIX, installare SnapManager:

Se il sistema operativo è...	Quindi eseguire...
Solaris (SPARC64)	
Solaris (x86_64)	
AIX (PPC64)	
Linux x86	
Linux x64	

6. Nella pagina Introduzione, premere **Invio** per continuare.

Viene visualizzato il seguente messaggio: Existing SnapManager for Oracle Detected (rilevamento di un sistema esistente per Oracle rilevato).

7. Premere **Invio**.

8. Al prompt dei comandi, eseguire le seguenti operazioni:

- a. Premere **Invio** per accettare il valore predefinito per l'utente del sistema operativo.
- b. Inserire il valore corretto per il gruppo di sistemi operativi o premere **Invio** per accettare il valore predefinito.
- c. Inserire il valore corretto per il tipo di avvio del server o premere **Invio** per accettare il valore predefinito.

Viene visualizzato il riepilogo della configurazione.

9. Premere **Invio** per continuare.

Viene visualizzato il seguente messaggio: Disinstallazione di SnapManager esistente per Oracle avviata.

La disinstallazione viene completata e viene installata la versione più recente di SnapManager.

Attività post-aggiornamento

Dopo aver eseguito l'aggiornamento a una versione successiva di SnapManager, è necessario aggiornare il repository esistente. È inoltre possibile modificare la classe di conservazione del backup assegnata ai backup esistenti e identificare il processo di ripristino che è possibile utilizzare.



Dopo aver eseguito l'aggiornamento a SnapManager 3.3 o versioni successive, impostare sqlnet.authentication_services su NONE (NESSUNO) se si desidera utilizzare l'autenticazione del database (DB) come unico metodo di autenticazione. Questa funzione non è supportata per i database RAC.

Aggiornamento del repository esistente

Non è necessario aggiornare il repository esistente se si esegue l'aggiornamento da SnapManager 3.3.x a SnapManager 3.4 o versione successiva, ma per tutti gli altri percorsi di aggiornamento è necessario aggiornare il repository esistente in modo da poterlo accedere dopo l'aggiornamento.

- Il server SnapManager aggiornato deve essere stato avviato e verificato.
- Deve esistere un backup del repository esistente.
- Se si esegue l'aggiornamento da una versione precedente a SnapManager 3.1 a SnapManager 3.3 o successiva, è necessario prima eseguire l'aggiornamento a SnapManager 3.2.

Dopo aver eseguito l'aggiornamento a SnapManager 3.2, è possibile eseguire l'aggiornamento a SnapManager 3.3 o versione successiva.

- Dopo aver aggiornato il repository, non è possibile utilizzarlo con una versione precedente di SnapManager.

a. Aggiornare il repository esistente: `smo repository update -repository -dbname repository_service_name -host repository_host_name -login -username repository_user_name -port repository_port`

- Il nome utente del repository, il nome del servizio di repository e il nome host del repository possono essere costituiti da caratteri alfanumerici, un segno meno, un carattere di sottolineatura e un punto.
- La porta del repository può essere qualsiasi numero di porta valido. Le altre opzioni utilizzate durante l'aggiornamento del repository esistente sono le seguenti:
- L'opzione `force`
- L'opzione `noprompt`
- L'opzione silenziosa
- L'opzione dettagliata

```
smo repository update -repository -dbname SALESDB  
-host server1 -login -username admin -port 1521
```

+

Riavviare il server SnapManager per riavviare le pianificazioni associate.

Modifica della classe di conservazione del backup

Dopo l'aggiornamento, SnapManager assegna la classe di conservazione del backup predefinita ai backup esistenti. È possibile modificare i valori predefiniti della classe di conservazione per soddisfare i requisiti di backup.

La classe di conservazione del backup predefinita assegnata ai backup esistenti è la seguente:

Tipo di backup	Assegnazione della classe di conservazione dopo l'aggiornamento
I backup devono essere conservati per sempre	Senza limiti
Altri backup	Ogni giorno

Nota: è possibile eliminare i backup conservati per sempre senza modificare la classe di conservazione.

Se si esegue l'aggiornamento a SnapManager 3.0 o versioni successive, ai profili esistenti viene assegnato il valore maggiore dei due seguenti valori:

- Numero di conservazione precedente per il profilo
- Valori predefiniti per il conteggio di conservazione e la durata dei backup giornalieri, come specificato nel file `smo.config`
 - a. Modificare i valori assegnati a `Retain.hourly.count` e `Retain.hourly.duration` nel file `smo.config`.

È possibile immettere i seguenti valori:

- retain.hourly.count = 12
- retain.hourly.duration = 2

Informazioni correlate

[Parametri di configurazione di SnapManager](#)

Ripristinare i tipi di processo

Tutti i processi di ripristino non sono supportati in tutte le versioni di SnapManager per Oracle. Dopo aver aggiornato SnapManager, è necessario conoscere il processo di ripristino che è possibile utilizzare per ripristinare un backup.

I backup creati utilizzando SnapManager 3.0 o versioni successive possono essere ripristinati utilizzando processi di ripristino rapido e basato su file. Tuttavia, i backup creati utilizzando una versione precedente a SnapManager 3.0 possono essere ripristinati utilizzando solo il processo di ripristino basato su file.

È possibile determinare la versione di SnapManager utilizzata per creare il backup eseguendo il comando `-backup show`.

Informazioni correlate

[Che cos'è il ripristino del database](#)

Aggiornamento degli host SnapManager mediante aggiornamento in sequenza

SnapManager 3.1 supporta l'approccio di aggiornamento a rotazione che consente di aggiornare gli host in modo sfalsato, host per host.

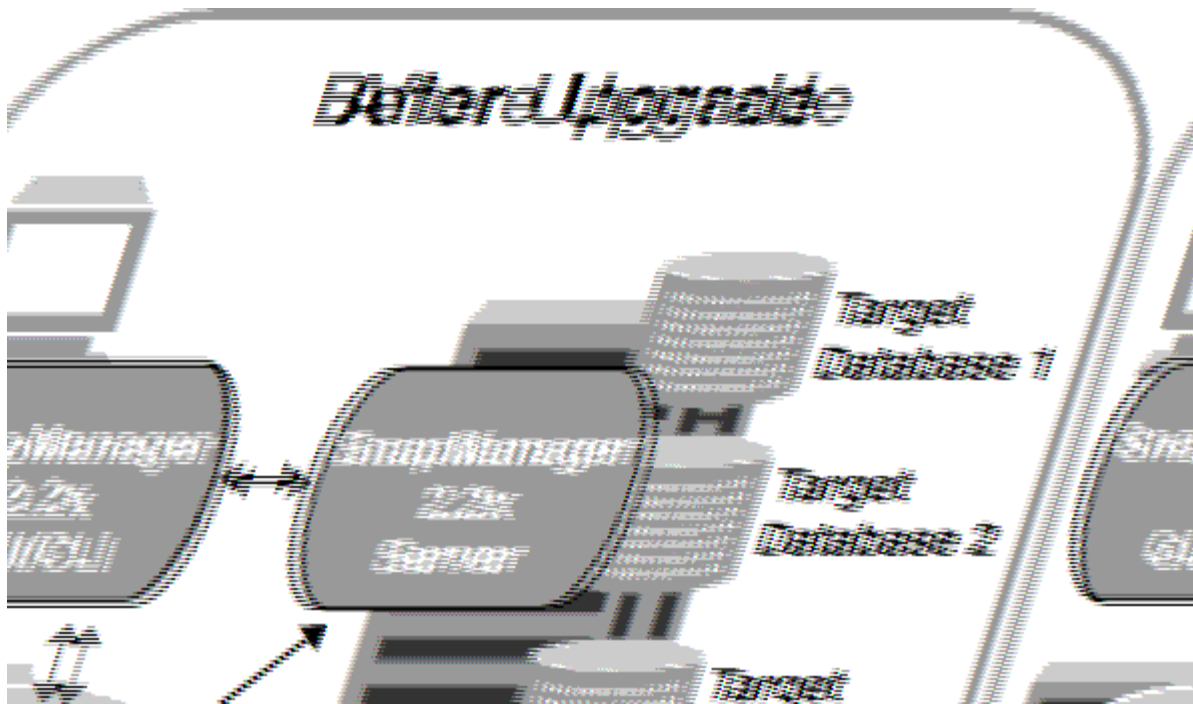
SnapManager 3.0 o versioni precedenti ti ha consentito di aggiornare tutti gli host contemporaneamente. Ciò ha comportato un downtime di tutti gli host SnapManager e delle operazioni pianificate durante l'operazione di aggiornamento.

L'upgrade a rotazione offre i seguenti vantaggi:

- Miglioramento delle prestazioni SnapManager grazie all'aggiornamento di un solo host alla volta.
- Possibilità di testare le nuove funzionalità in un host server SnapManager prima di aggiornare gli altri host.



È possibile eseguire l'aggiornamento in sequenza solo utilizzando l'interfaccia della riga di comando (CLI).



Una volta completato con successo l'aggiornamento a rotazione, SnapManager ospita, profili, pianificazioni, backup. Inoltre, i cloni associati ai profili dei database di destinazione vengono migrati dal database dei repository della versione precedente di SnapManager al database dei repository della nuova versione. I dettagli sulle operazioni eseguite utilizzando i profili, le pianificazioni, i backup e i cloni creati nella versione precedente di SnapManager sono ora disponibili nel database repository della nuova versione. È possibile avviare la GUI utilizzando i valori di configurazione predefiniti del file `user.config`. I valori configurati nel file `user.config` della versione precedente di SnapManager non vengono presi in considerazione.

Il server SnapManager aggiornato è ora in grado di comunicare con il database repository aggiornato. Gli host che non sono stati aggiornati possono gestire i database di destinazione utilizzando il repository della versione precedente di SnapManager e quindi utilizzare le funzionalità disponibili nella versione precedente.



Prima di eseguire l'aggiornamento in sequenza, è necessario assicurarsi che tutti gli host presenti nel database del repository possano essere risolti. Per informazioni su come risolvere gli host, consultare la sezione relativa alla risoluzione dei problemi nella *Guida all'amministrazione di SnapManager per Oracle per UNIX*.

Informazioni correlate

[Che cos'è un rollback](#)

[Risoluzione dei problemi di SnapManager](#)

Prerequisiti per l'esecuzione degli aggiornamenti in sequenza

Prima di eseguire un aggiornamento a rotazione, è necessario assicurarsi che l'ambiente soddisfi determinati requisiti.

- Se si utilizza una versione precedente a SnapManager 3.1 e si desidera eseguire un aggiornamento a rotazione a SnapManager 3.3 o versione successiva, è necessario prima eseguire l'aggiornamento alla versione 3.2 e poi alla versione più recente.

È possibile eseguire direttamente l'aggiornamento da SnapManager 3.2 a SnapManager 3.3 o versioni

successive.

- È necessario eseguire il backup degli script esterni utilizzati per eseguire la protezione esterna dei dati o la conservazione dei dati.
- La versione di SnapManager che si desidera aggiornare deve essere installata.



Se si esegue l'aggiornamento da una versione precedente a SnapManager 3.1 a SnapManager 3.3 o successiva, è necessario installare SnapManager 3.2 ed eseguire un aggiornamento in sequenza. Dopo aver eseguito l'aggiornamento alla versione 3.2, è possibile installare SnapManager 3.3 o versione successiva ed eseguire un altro aggiornamento a SnapManager 3.3 o versione successiva.

- È necessario installare la versione di SnapDrive per UNIX supportata con la versione di SnapManager alla quale si desidera eseguire l'aggiornamento.

La documentazione di SnapDrive contiene dettagli sull'installazione di SnapDrive.

- È necessario eseguire il backup del database del repository.
- La quantità di utilizzo del repository SnapManager deve essere minima.
- Se l'host da aggiornare utilizza un repository, le operazioni SnapManager non devono essere eseguite sugli altri host che utilizzano lo stesso repository.

Le operazioni pianificate o in esecuzione sugli altri host attendono il completamento dell'aggiornamento in sequenza.



Si consiglia di eseguire un aggiornamento in sequenza quando il repository è meno occupato, ad esempio durante il fine settimana o quando le operazioni non sono pianificate.

- I profili che puntano allo stesso database di repository devono essere creati con nomi diversi negli host del server SnapManager.

Se si utilizzano profili con lo stesso nome, l'aggiornamento in sequenza che coinvolge il database del repository non riesce senza preavviso.

- Le operazioni SnapManager non devono essere eseguite sull'host da aggiornare.



L'aggiornamento a rotazione viene eseguito più a lungo, in quanto aumenta il numero di backup degli host che vengono aggiornati insieme. La durata dell'aggiornamento può variare in base al numero di profili e backup associati a un determinato host.

"Documentazione sul sito di supporto NetApp: mysupport.netapp.com"

Esecuzione di un aggiornamento in sequenza su uno o più host

È possibile eseguire l'aggiornamento in sequenza su uno o più host server SnapManager utilizzando l'interfaccia a riga di comando (CLI). L'host del server SnapManager aggiornato viene quindi gestito solo con la versione successiva di SnapManager.

Assicurarsi che tutti i prerequisiti per l'esecuzione dell'aggiornamento in sequenza siano stati completati.

1. Per eseguire un aggiornamento rolling su un singolo host, immettere il seguente comando: `'Morepository rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-`

portrepo_port-upgradehosthost_with_target_database-force [-quiet | -verbose]'

Il seguente comando esegue l'aggiornamento in sequenza di tutti i database di destinazione montati su HostA e di un database di repository denominato repoA situato su repo_host:

```
smo repository rollingupgrade
  -repository
    -dbname repoA
    -host repo_host
    -login
    -username repouser
    -port 1521
  -upgradehost hostA
```

2. Per eseguire un aggiornamento rolling su più host, immettere il seguente comando: 'Smorepository rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-username-portrepo_port-upgradehosthost_with_target_database1,host_with_target_database2-force [-quiet | -verbose]



Per più host, immettere i nomi host separati da una virgola e assicurarsi di non includere spazio tra la virgola e il nome host successivo. Se si utilizza una configurazione Real Application Clusters (RAC), è necessario aggiornare manualmente tutti gli host associati al RAC. È possibile utilizzare -allhosts per eseguire l'aggiornamento in sequenza di tutti gli host.

Il seguente comando esegue l'aggiornamento in sequenza di tutti i database di destinazione montati sugli host, HostA e hostB e un database di repository denominato repoA situato su repo_host:

```
smo repository rollingupgrade
  -repository
    -dbname repoA
    -host repo_host
    -login
    -username repouser
    -port 1521
  -upgradehost hostA,hostB
```

3. Per eseguire un aggiornamento in sequenza su tutti gli host di un database del repository, immettere il seguente comando: 'Morepository rollingupgrade-repository-dbnamerepo_service_name-ostrepo_host-login-username_portrepo_port-allhosts-force [-quiet | -verbose]'

Dopo aver aggiornato correttamente il database del repository, è possibile eseguire tutte le operazioni SnapManager sul database di destinazione.

L'aggiornamento di SnapManager per Oracle conserva le credenziali utente basate su host, le credenziali utente del software Oracle e le credenziali utente di Oracle Recovery Manager (RMAN) della versione precedente di SnapManager per Oracle.

Il seguente comando esegue l'aggiornamento in sequenza di tutti i database di destinazione disponibili in

un database repository denominato repoA situato su repo_host:

```
smo repository rollinguupgrade
  -repository
    -dbname repoA
    -host repo_host
    -login
      -username repouser
      -port 1521
    -allhosts
```

- Se il server SnapManager si avvia automaticamente, è necessario riavviare il server per assicurarsi di poter visualizzare le pianificazioni.
- Se si aggiorna uno dei due host correlati, è necessario aggiornare il secondo host dopo l'aggiornamento del primo.

Ad esempio, se è stato creato un clone dall'host A all'host B o è stato montato un backup dall'host A all'host B, gli host A e B sono correlati tra loro. Quando si aggiorna l'host A, viene visualizzato un messaggio di avviso che richiede di aggiornare l'host B subito dopo l'aggiornamento dell'host A.



I messaggi di avviso vengono visualizzati anche se il clone viene cancellato o il backup viene dismontato dall'host B durante l'aggiornamento in sequenza dell'host A. Questo perché nel repository sono presenti metadati per le operazioni eseguite sull'host remoto.

Informazioni correlate

[Prerequisiti per l'esecuzione degli aggiornamenti in sequenza](#)

Che cos'è un rollback

L'operazione di rollback consente di ripristinare una versione precedente di SnapManager dopo l'esecuzione di un aggiornamento in sequenza.



Prima di eseguire un rollback, è necessario assicurarsi che tutti gli host presenti nel database del repository possano essere risolti.

Quando si esegue un rollback, vengono ripristinati i seguenti elementi:

- Backup creati, liberati ed eliminati utilizzando la versione di SnapManager da cui si esegue il rollback
- Cloni creati da un backup creato utilizzando la versione di SnapManager da cui si sta eseguendo il rollback
- Credenziali del profilo modificate utilizzando la versione di SnapManager da cui si sta eseguendo il rollback
- Stato di protezione del backup modificato utilizzando la versione di SnapManager da cui si sta eseguendo il rollback

Le funzioni disponibili nella versione di SnapManager in uso, ma non disponibili nella versione a cui si sta eseguendo il rollback, non sono supportate. Ad esempio, quando si esegue un rollback da SnapManager 3.3 o versioni successive a SnapManager 3.1, la configurazione della cronologia per i profili in SnapManager 3.3 o

versioni successive non viene rollback ai profili in SnapManager 3.1. Questo perché la funzione di configurazione della cronologia non era disponibile in SnapManager 3.1.

Informazioni correlate

[Risoluzione dei problemi di SnapManager](#)

Limitazioni per l'esecuzione di un rollback

È necessario conoscere gli scenari in cui non è possibile eseguire un rollback. Tuttavia, per alcuni di questi scenari è possibile eseguire alcune attività aggiuntive prima di eseguire il rollback.

Gli scenari in cui non è possibile eseguire il rollback o eseguire le attività aggiuntive sono i seguenti:

- Se si esegue una delle seguenti operazioni dopo aver eseguito un aggiornamento in sequenza:
 - Creare un nuovo profilo.
 - Separare un clone.
 - Modificare lo stato di protezione del profilo.
 - Assegnare criteri di protezione, classe di conservazione o relazioni SnapVault e SnapMirror.

In questo scenario, dopo aver eseguito un rollback, è necessario rimuovere manualmente i criteri di protezione, la classe di conservazione o le relazioni SnapVault e SnapMirror assegnate.

- Modificare lo stato di montaggio del backup.

In questo scenario, è necessario prima modificare lo stato di montaggio e poi eseguire un rollback.

- Ripristinare un backup.
- Modificare la modalità di autenticazione dall'autenticazione del database all'autenticazione del sistema operativo.

In questo scenario, dopo aver eseguito un rollback, è necessario modificare manualmente la modalità di autenticazione dal sistema operativo al database.

- Se il nome host del profilo viene modificato
- Se i profili sono separati per creare backup del registro di archiviazione

In questo scenario, non è possibile eseguire il rollback a una versione precedente a SnapManager 3.2.

Prerequisiti per eseguire un rollback

Prima di eseguire un rollback, è necessario assicurarsi che l'ambiente soddisfi determinati requisiti.

- Se si utilizza SnapManager 3.3 o versione successiva e si desidera ripristinare una versione precedente a SnapManager 3.1, è necessario tornare alla versione 3.2 e quindi alla versione desiderata.
- È necessario eseguire il backup degli script esterni utilizzati per eseguire la protezione esterna dei dati o la conservazione dei dati.
- È necessario installare la versione di SnapManager in cui si desidera eseguire il rollback.



Se si desidera eseguire un rollback da SnapManager 3.3 o versione successiva a una versione precedente a SnapManager 3.1, è necessario installare SnapManager 3.2 ed eseguire un rollback. Dopo aver eseguito il rollback a 3.2, è possibile installare SnapManager 3.1 o versione precedente ed eseguire un altro rollback a tale versione.

- La versione di SnapDrive per UNIX supportata con la versione di SnapManager a cui si desidera eseguire il rollback deve essere installata.

Per informazioni sull'installazione di SnapDrive, consultare la documentazione di SnapDrive.

- È necessario eseguire il backup del database del repository.
- Se l'host da ripristinare utilizza un repository, le operazioni SnapManager non devono essere eseguite sugli altri host che utilizzano lo stesso repository.

Le operazioni pianificate o in esecuzione sugli altri host attendono il completamento del rollback.

- I profili che puntano allo stesso database del repository devono essere creati con nomi diversi negli host del server SnapManager.

Se si utilizzano profili con lo stesso nome, l'operazione di rollback che coinvolge il database del repository non riesce senza preavviso.

- Le operazioni SnapManager non devono essere eseguite sull'host che si desidera eseguire.

Se è in esecuzione un'operazione, è necessario attendere il completamento dell'operazione e prima di procedere con il rollback.



L'operazione di rollback viene eseguita per un periodo di tempo più lungo con l'aumentare del numero cumulativo di backup degli host che vengono rollback insieme. La durata del rollback può variare a seconda del numero di profili e backup associati a un determinato host.

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

Esecuzione di un rollback su uno o più host

È possibile eseguire un rollback su uno o più host server SnapManager utilizzando l'interfaccia della riga di comando (CLI).

Assicurarsi che tutti i prerequisiti per l'esecuzione di un rollback siano completi.

1. Per eseguire un rollback su un singolo host, immettere il seguente comando: `smrepository rollback-repository-dbnamerepo_service_name-hostrepo_host-login-username repo_username-portrepo_port-rollbackhosthost_with_target_database`

L'esempio seguente mostra il comando per eseguire il rollback di tutti i database di destinazione montati su HostA e di un database del repository denominato repoA situato sull'host del repository, repo_host:

```
smo repository rollback
  -repository
    -dbname repoA
    -host repo_host
    -login
      -username repouser
      -port 1521
    -rollbackhost hostA
```

2. Per eseguire un rollback su più host, immettere il seguente comando: Scorepository rollback-repository-dbnamerepo_service_name-hostrepo_host-login-username-portrepo_port-rollbackhosthost_with_target_database1,host_with_target_database2



Per più host, immettere i nomi host separati da una virgola e assicurarsi che non vi sia spazio tra la virgola e il nome host successivo.

Se si utilizza la configurazione RAC (Real Application Clusters), è necessario eseguire il rollback manuale di tutti gli host associati al RAC. È possibile utilizzare -allhosts per eseguire un rollback di tutti gli host.

Nell'esempio seguente viene illustrato il comando per eseguire il rollback di tutti i database di destinazione montati sugli host, HostA, hostB e un database di repository denominato repoA situato sull'host di repository, repo_host:

```
smo repository rollback
  -repository
    -dbname repoA
    -host repo_host
    -login
      -username repouser
      -port 1521
    -rollbackhost hostA,hostB
```

Gli host, i profili, le pianificazioni, i backup e i cloni associati ai profili dei database di destinazione per l'host vengono ripristinati nel repository precedente.

Informazioni correlate

[Prerequisiti per eseguire un rollback](#)

Attività di post-rollback

Per visualizzare le pianificazioni create nella versione precedente del database del repository, è necessario eseguire alcuni passaggi aggiuntivi dopo il rollback di un database del repository e il downgrade dell'host SnapManager da SnapManager 3.2 a SnapManager 3.0.

1. Accedere a `cd /opt/NetApp/smo/Repository`.

La directory dei repository potrebbe contenere due file per ciascun repository. Il nome del file con il numero viene creato utilizzando SnapManager 3.1 o versione successiva e il nome del file con il trattino (-) viene creato utilizzando SnapManager 3.0.

I nomi dei file potrebbero essere i seguenti:

- Repository SMO300A SMOREPO1 10.72.197.141 1521
- repository-smo300a-smorepo1-10.72.197.141-1521

2. Sostituire il segno del numero (n.) nel nome del file con il trattino (-).

Il nome del file con il numero (n.), ora contiene il trattino (-): Repository-SMO300a-SMOREPO1-10.72.197.141-1521.

Configurazione di SnapManager


Dopo aver installato SnapManager, è necessario eseguire alcune attività di configurazione aggiuntive a seconda dell'ambiente in uso.


Parametri di configurazione di SnapManager

SnapManager fornisce un elenco di parametri di configurazione che è possibile modificare in base alle proprie esigenze. I parametri di configurazione vengono memorizzati nel file `smo.config`. Tuttavia, il file `smo.config` potrebbe non contenere tutti i parametri di configurazione supportati. È possibile aggiungere i parametri di configurazione, a seconda dei requisiti.


La seguente tabella elenca tutti i parametri di configurazione SnapManager supportati e spiega anche quando utilizzare questi parametri:

Parametri	Descrizione
<ul style="list-style-type: none">• retain.hourly.count• retain.hourly.duration• retain.monthly.count• retain.monthly.duration	<p>Questi parametri impostano il criterio di conservazione quando si crea un profilo. Ad esempio, è possibile assegnare i seguenti valori: Retain.Hourly.count = 12</p> <p>retain.hourly.duration = 2</p> <p>retain.monthly.count = 2</p> <p>retain.monthly.duration = 6</p>


restore.secondaryAccessPolicy	<p>Questo parametro definisce il modo in cui SnapManager può accedere ai dati sullo storage secondario quando non può essere ripristinato direttamente utilizzando Gestione protezione. Di seguito sono riportati i diversi modi per accedere ai dati sullo storage secondario:</p> <ul style="list-style-type: none"> • Diretto (impostazione predefinita) <p>Quando restore.secondaryAccessPolicy è impostato su Direct, SnapManager clona i dati sullo storage secondario, monta i dati clonati dallo storage secondario sull'host, quindi copia i dati dal clone nell'ambiente attivo.</p> <ul style="list-style-type: none"> • Indiretto <p>Se si assegna indiretto a restore.secondaryAccessPolicy, SnapManager copia i dati in un volume temporaneo sullo storage primario, monta i dati dal volume temporaneo all'host, quindi copia i dati dal volume temporaneo nell'ambiente attivo.</p> <p>Il metodo indiretto deve essere utilizzato solo se l'host non dispone di accesso diretto al sistema di storage secondario. Questo metodo richiede il doppio del tempo rispetto al metodo diretto, in quanto vengono create due copie dei dati.</p> <div data-bbox="850 1199 902 1255">  </div> <div data-bbox="966 1142 1425 1310"> <p>In una SAN (Storage Area Network) con NFS (Network file System) come protocollo, SnapManager non deve connettersi direttamente allo storage secondario per eseguire un ripristino.</p> </div>
Restore.tmporaryVolumeName	<p>Questo parametro assegna un nome al volume temporaneo. Quando SnapManager utilizza il metodo indiretto per il ripristino dei dati dallo storage secondario, richiede un volume scratch sullo storage primario per conservare una copia temporanea dei dati fino a quando non vengono copiati nei file di database e il database viene ripristinato. Non esiste alcun valore predefinito. Se non si specifica un valore, è necessario immettere un nome nel comando restore che utilizza il metodo indiretto. Ad esempio, è possibile assegnare i seguenti valori: restore.tmporaryVolumeName = smo_tmp_volume</p>

Retain.alwaysFreeExpiredBackups	<p>Questo parametro consente a SnapManager di liberare i backup quando scadono e quando viene eseguito un ripristino rapido, anche se la protezione dei dati non è configurata. Questo parametro libera i backup protetti in scadenza ed elimina i backup non protetti in scadenza. I valori che è possibile assegnare sono i seguenti:</p> <ul style="list-style-type: none"> • Vero <p>Se si assegna true a Retain.alwaysFreeExpiredBackups, SnapManager libera i backup scaduti indipendentemente dal fatto che i backup siano protetti.</p> <p>I backup vengono cancellati quando non sono protetti o se sono scadute anche le copie protette sullo storage secondario.</p> <ul style="list-style-type: none"> • Falso <p>Se si assegna false a Retain.alwaysFreeExpiredBackups, SnapManager libera i backup scaduti protetti.</p>
host.credentials.persistere	<p>Questo parametro consente a SnapManager di memorizzare le credenziali dell'host. Per impostazione predefinita, le credenziali dell'host non vengono memorizzate. Tuttavia, le credenziali host devono essere memorizzate se si dispone di uno script personalizzato che viene eseguito su un clone remoto e richiede l'accesso a un server remoto. È possibile abilitare la memorizzazione delle credenziali host assegnando true a host.credentials.persistere. SnapManager crittografa e salva le credenziali dell'host.</p>
RestorePlanMaxFilesvisualizzati	<p>Questo parametro consente di definire il numero massimo di file da visualizzare nell'anteprima di ripristino. Per impostazione predefinita, SnapManager visualizza un massimo di 20 file nell'anteprima di ripristino. Tuttavia, è possibile passare a un valore maggiore di 0. Ad esempio, è possibile assegnare il seguente valore:</p> <ul style="list-style-type: none"> • RestorePlanMaxFilesvisualizzati = 30 <div data-bbox="850 1801 906 1864">  </div> <p>Se si specifica un valore non valido, viene visualizzato il numero predefinito di file.</p>

<p>snapshot.list.timeout.min</p>	<p>Questo parametro consente di definire il tempo in minuti per il quale SnapManager deve attendere l'esecuzione del comando snap-list quando si eseguono operazioni SnapManager. per impostazione predefinita, SnapManager attende 30 minuti. Tuttavia, è possibile passare a un valore maggiore di 0. Ad esempio, è possibile assegnare il seguente valore:</p> <ul style="list-style-type: none"> • snapshot.list.timeout.min = 40 <div data-bbox="850 457 906 512" data-label="Image"> </div> <p>Se si specifica un valore non valido, viene utilizzato il valore predefinito.</p> <p>Per qualsiasi operazione SnapManager, se il tempo di esecuzione del comando snap-list supera il valore assegnato a snapshot.list.timeout.min, l'operazione non riesce e viene visualizzato un messaggio di errore di timeout.</p>
<p>PrunelfFileExistsInOtherDestination</p>	<p>Questo parametro di eliminazione consente di definire la destinazione dei file di log dell'archivio. I file di log dell'archivio sono memorizzati in più destinazioni. Durante l'eliminazione dei file di log dell'archivio, SnapManager deve conoscere la destinazione dei file di log dell'archivio. I valori che è possibile assegnare sono i seguenti:</p> <ul style="list-style-type: none"> • Se si desidera eliminare i file di log dell'archivio da una destinazione specifica, è necessario assegnare false a prunelfFileExistsInOtherDestination. • Se si desidera eliminare i file di log dell'archivio da una destinazione esterna, è necessario assegnare true a prunelfFileExistsInOtherDestination.

prune.archivelogs.backedup.from.otherdestination	<p>Questo parametro di eliminazione consente di rimuovere i file di log dell'archivio di cui è stato eseguito il backup dalle destinazioni del log dell'archivio specificate o di eseguire il backup da destinazioni esterne del log dell'archivio. I valori che è possibile assegnare sono i seguenti:</p> <ul style="list-style-type: none"> • Se si desidera eseguire la eliminazione dei file di log dell'archivio dalle destinazioni specificate e il backup dei file di log dell'archivio dalle destinazioni specificate utilizzando -prune-dest, è necessario assegnare false a <code>prune.archivelogs.backedup.from.otherdestination</code>. • Se si desidera eseguire la eliminazione dei file di log dell'archivio da destinazioni specificate e il backup dei file di log dell'archivio viene eseguito almeno una volta da una qualsiasi delle altre destinazioni, è necessario assegnare true a <code>prune.archivelogs.backedup.from.otherdestination</code>.
Maximum.archiveog.files.toprun.atatime	<p>Questo parametro di eliminazione consente di definire il numero massimo di file di log di archiviazione che è possibile rimuovere in un dato momento. Ad esempio, è possibile assegnare il seguente valore: <code>maximum.archiveog.files.toprun.atatime = 998</code></p> <div>  <p>Il valore che può essere assegnato a <code>maximum.archiveog.files.toprun.atatime</code> deve essere inferiore a 1000.</p> </div>
archivelogs.consolidate	<p>Questo parametro consente a SnapManager di liberare i backup duplicati del registro di archiviazione se si assegna true a <code>archivelogs.consolidate</code>.</p>
suffix.backup.label.with.logs	<p>Questo parametro consente di specificare il suffisso che si desidera aggiungere per differenziare i nomi delle etichette del backup dei dati e del backup del log di archiviazione. ad esempio, quando si assegnano i log al suffisso <code>backup.label.with.logs</code>, <code>_logs</code> viene aggiunto come suffisso all'etichetta di backup del log di archiviazione. L'etichetta di backup del log di archiviazione sarà quindi <code>arch_logs</code>.</p>

backup.archiveLogs.beyond.missingfiles	<p>Questo parametro consente a SnapManager di includere nel backup i file di log dell'archivio mancanti. I file di log dell'archivio che non esistono nel file system attivo non sono inclusi nel backup. Se si desidera includere tutti i file di log dell'archivio, anche quelli che non esistono nel file system attivo, è necessario assegnare true a backup.archiveLogs.beyond.missingfiles.</p> <p>È possibile assegnare false per ignorare i file di log dell'archivio mancanti.</p>
srvctl.timeout	<p>Questo parametro consente di definire il valore di timeout per il comando srvctl. Nota: Server Control (SRVCTL) è un'utilità per gestire le istanze RAC.</p> <p>Quando SnapManager impiega più tempo per eseguire il comando srvctl rispetto al valore di timeout, l'operazione SnapManager non riesce e viene visualizzato il seguente messaggio di errore: Errore: Timeout durante l'esecuzione del comando: Stato srvctl.</p>
Snapshot.restore.storageNameCheck	<p>Questo parametro consente a SnapManager di eseguire l'operazione di ripristino con copie Snapshot create prima della migrazione da Data ONTAP in 7-Mode a Clustered Data ONTAP. Il valore predefinito assegnato al parametro è false. Se è stata eseguita la migrazione da Data ONTAP in 7-Mode a Clustered Data ONTAP ma si desidera utilizzare le copie Snapshot create prima della migrazione, impostare snapshot.restore.storageNameCheck=true.</p>
services.common.disableAbort	<p>Questo parametro disattiva il cleanup in caso di errore di operazioni a esecuzione prolungata. È possibile impostare services.common.disableAbort=true. For esempio. Se si esegue un'operazione di clonazione che viene eseguita a lungo e poi non riesce a causa di un errore Oracle, potrebbe non essere necessario pulire il clone. Se si imposta services.common.disableAbort=true, il clone non verrà cancellato. È possibile risolvere il problema di Oracle e riavviare l'operazione di clonazione dal punto in cui si è verificato un errore.</p>

<ul style="list-style-type: none"> • backup.sleep.dnfs.layout • backup.sleep.dnfs.secs 	<p>Questi parametri attivano il meccanismo di sospensione nel layout Direct NFS (DNFS). Dopo aver creato il backup dei file di controllo utilizzando DNFS o un file system di rete (NFS), SnapManager tenta di leggere i file di controllo, ma i file potrebbero non essere trovati. per attivare il meccanismo di sospensione, assicurarsi che backup.sleep.dnfs.layout=true. Il valore predefinito è true.</p> <p>Quando si attiva il meccanismo di sospensione, è necessario assegnare il tempo di sospensione a backup.sleep.dnfs.secs. Il tempo di sospensione assegnato è espresso in secondi e il valore dipende dall'ambiente in uso. Il valore predefinito è 5 secondi.</p> <p>Ad esempio:</p> <ul style="list-style-type: none"> • backup.sleep.dnfs.layout=true • backup.sleep.dnfs.secs=2
<ul style="list-style-type: none"> • override.default.backup.pattern • new.default.backup.pattern 	<p>Se non si specifica l'etichetta di backup, SnapManager crea un'etichetta di backup predefinita. Questi parametri SnapManager consentono di personalizzare l'etichetta di backup predefinita. per consentire la personalizzazione dell'etichetta di backup, assicurarsi che il valore override.default.backup.pattern sia impostato su true. Il valore predefinito è false.</p> <p>Per assegnare il nuovo modello dell'etichetta di backup, è possibile assegnare parole chiave come nome del database, nome del profilo, ambito, modalità e nome host a new.default.backup.pattern. Le parole chiave devono essere separate utilizzando un carattere di sottolineatura. Ad esempio, new.default.backup.pattern=dbname_profile_hostnam e_scope_mode.</p> <div data-bbox="850 1486 906 1549">  </div> <div data-bbox="966 1465 1448 1570"> <p>Il timestamp viene incluso automaticamente alla fine dell'etichetta generata.</p> </div>

allow.underscore.in.clone.sid	<p>Oracle supporta l'utilizzo del carattere di sottolineatura nel clone SID di Oracle 11gR2. Questo parametro SnapManager consente di includere un carattere di sottolineatura nel nome del SID clone. Per includere un carattere di sottolineatura nel nome del SID clone, assicurarsi che il valore allow.underscore.in.clone.sid sia impostato su true. Il valore predefinito è true.</p> <p>Se si utilizza una versione di Oracle precedente a Oracle 11gR2 o se non si desidera includere un carattere di sottolineatura nel nome SID del clone, impostare il valore su false.</p>
oracle.parameters.with.comma	<p>Questo parametro consente di specificare tutti i parametri Oracle con virgola (,) come valore. Durante l'esecuzione di qualsiasi operazione, SnapManager utilizza oracle.parameters.with.comma per controllare tutti i parametri Oracle e ignorare la suddivisione dei valori.</p> <p>Ad esempio, se il valore di nls_Numeric_Characters=, specificare oracle.parameters.with.comma=nls_numeric_characters. Se sono presenti più parametri Oracle con virgola come valore, è necessario specificare tutti i parametri in oracle.parameters.with.comma.</p>

- ArchivedLogs.exclude
- ArchivedLogs.exclude.fileslike
- <db-unique-name>.archivedLogs.exclude.fileslike

Questi parametri consentono a SnapManager di escludere i file di log dell'archivio dai profili e dai backup se il database non si trova su un sistema di storage abilitato alla copia Snapshot e si desidera eseguire operazioni SnapManager su tale sistema di storage. **Nota:** prima di creare un, è necessario includere i parametri di esclusione nel file di configurazione profilo.

I valori assegnati a questi parametri possono essere una directory di primo livello o un punto di montaggio in cui sono presenti i file di log dell'archivio o una sottodirectory. Se viene specificata una directory di primo livello o un punto di montaggio e se la protezione dei dati è attivata per un profilo sull'host, tale punto di montaggio o directory non viene inclusa nel dataset creato in Protection Manager. Quando si desidera escludere dall'host più file di log di archiviazione, è necessario separare i percorsi dei file di log di archiviazione utilizzando le virgole.

Per escludere l'inclusione dei file di log di archiviazione nel profilo e il backup, è necessario includere uno dei seguenti parametri:

- ArchivedLogs.exclude per specificare un'espressione regolare per l'esclusione dei file di log di archivio da tutti i profili o backup.

I file di log dell'archivio corrispondenti all'espressione regolare sono esclusi da tutti i profili e i backup.

Ad esempio, puoi impostare archivedLogs.exclude =
/arch/logs/on/local/disk1/./, **/arch/logs/on/local/disk2/..** Per i database ASM, è possibile impostare archivedLogs.exclude =
/KHDB_ARCH_DEST/khdb/archiveog/., **KHDB_NONNAARCHTWO/khdb/archiveog/..**

- ArchivedLogs.exclude.fileslike per specificare un'espressione SQL per escludere i file di log dell'archivio da tutti i profili o backup.

I file di log dell'archivio corrispondenti all'espressione SQL sono esclusi da tutti i profili e i backup.

Ad esempio, puoi impostare archivedLogs.exclude.fileslike =
/arch/logs/on/local/disk1/%/, /arch/logs/on/local/disk2/%.

- <db-unique-name>.archivedLogs.exclude.fileslike per specificare un'espressione SQL per escludere i file di log dell'archivio solo dal profilo o dal backup creato per il database con il nome db-unique specificato.

Modifica dei parametri di configurazione

A seconda dell'ambiente in uso, è possibile modificare i valori predefiniti assegnati al parametro di configurazione.

I file di log dell'archivio corrispondenti all'espressione SQL sono esclusi dal profilo e dai backup.

Ad esempio, è possibile impostare

1. Aprire il file di configurazione dal seguente percorso predefinito:
percorso/proprietà di installazione predefinito/smo.config2/%.
default.archivedLogs.exclude.fileslike =
/arch/logs/on/local/disk1/%,/arch/logs/on/local/disk2/%.
2. Modificare i valori predefiniti dei parametri di configurazione.



È inoltre possibile aggiungere parametri di configurazione supportati che non sono inclusi nel file di configurazione e assegnarli valori.

3. Riavviare il server SnapManager per Oracle.

Configurazione di SnapDrive per UNIX per un ambiente Veritas SFRAC attivo/attivo

Se è stato incluso il parametro host-cluster-sw-restore-warn in snapdrive.conf e il valore è stato assegnato su, è necessario modificare il valore per supportare l'operazione di ripristino nell'ambiente Active/Active Veritas Storage Foundation per Oracle RAC (SFRAC).

Quando si utilizza l'ambiente Active/Active Veritas Storage Foundation for Oracle RAC (SFRAC), se il parametro host-cluster-sw-restore-warn è impostato su ON, viene visualizzato un messaggio di avviso e l'operazione di ripristino viene interrotta. Se si desidera eseguire l'operazione di ripristino in un ambiente Veritas SFRAC attivo/attivo, è necessario impostare host-cluster-sw-restore-warn su Off.

Per informazioni su snapdrive.conf, consultare la documentazione di SnapDrive.

1. Accedere come utente root.
2. Aprire il file snapdrive.conf utilizzando un editor di testo.
3. Impostare il valore di host-cluster-sw-restore-warn su Off.

Dopo la configurazione, riavviare il server SnapDrive per UNIX.

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

Configurazione di SnapManager per il supporto dell'ambiente Veritas SFRAC

Quando SnapManager è installato su Solaris, è possibile configurare SnapManager per supportare l'ambiente TRAC di Veritas Storage Foundation per Oracle.

- Sull'host devono essere installati Solaris, utility host e Veritas.
 - a. Creare un gruppo di dischi condivisi e un file system per SnapManager utilizzando SnapDrive per UNIX in modo che i file system siano montati contemporaneamente su entrambi i nodi dei cluster di applicazioni reali (RAC).

Per informazioni su come creare un gruppo di dischi e un file system condivisi, consultare la documentazione di SnapDrive.

- b. Installare e configurare il database Oracle da montare sui file system condivisi.
- c. Avviare un'istanza di database su un nodo qualsiasi del RAC.

"Documentazione sul sito di supporto NetApp: mysupport.netapp.com"

Assicurarsi che ASM scopra i dischi importati

Se si utilizza la gestione automatica dello storage (ASM) in un ambiente NFS, dopo l'installazione di SnapManager, è necessario assicurarsi che ASM sia in grado di rilevare i dischi importati da SnapManager. A tale scopo, aggiungere il percorso della directory ASM al parametro ASM_DISKSTRING.

È possibile utilizzare gli strumenti Oracle per modificare il parametro ASM_DISKSTRING. Per informazioni sulla modifica di ASM_DISKSTRING, consultare la documentazione Oracle.

Il percorso del disco ASM /opt/NetApp/smo/mnt///disk* deve essere aggiunto al percorso esistente definito nel parametro ASM_DISKSTRING. Ad esempio, se il percorso definito in ASM_DISKSTRING era /mnt/my-asm-disks/dir1/disk*, dopo aver aggiunto il percorso del disco ASM, il percorso aggiornato sarà '/mnt/my-asm-disks/dir1/disk*,/opt/NetApp/smo/mnt///disk*'.



Il parametro ASM_DISKSTRING deve corrispondere solo ai file del disco ASM e non ad altri file.

- Il primo asterisco (*) indica il nome generato da SnapManager per il punto di montaggio root.
- Il secondo * indica la directory all'interno del punto di montaggio.
- Il terzo * indica il nome del file NFS.

Se il disco è montato nelle directory sotto /opt/NetApp/smo/mnt/<smo-generated-name>/, è necessario assicurarsi che il simbolo * corrisponda alla topologia del file system NFS.

1. Se si utilizzano dischi ASM con NFS nell'ambiente NAS (Network Attached Storage), modificare il parametro ASM_DISKSTRING in modo che punti al percorso di directory ASM corrente.

Se il punto di montaggio dei dischi ASM è /mnt/my-asm-disks//**disk**, dopo aver modificato ASM_DISKSTRING, il percorso aggiornato è /opt/NetApp/smo/mnt/my-asm-disks-20081012/disk1.nfs. Il parametro ASM_DISKSTRING è nel formato /opt/NetApp/smo/mnt//**disk**.

- Il primo * corrisponde a my-asm-disks-20081012.
- Il disco* corrisponde a disk1.nfs. Dopo aver modificato il parametro ASM_DISKSTRING, i risultati del rilevamento dei dischi importati da SnapManager sono i seguenti:
- Il clone di ASM su NFS disk1 è /opt/NetApp/smo/mnt/-mnt-my-asm-disks-20081012/dir1/disk1.nfs.
- Il clone di ASM su NFS disk2 è /opt/NetApp/smo/mnt/-mnt-my-asm-disks-20081012/dir1/disk2.nfs. Il parametro ASM_DISKSTRING è nel formato /opt/NetApp/smo/mnt//**disk**.*
- Il primo * corrisponde a -mnt-my-asm-disks-20081012.
- Il secondo * corrisponde a dir1.
- Il terzo * corrisponde a disk1.nfs e disk2.nfs.

2. Se si utilizzano dischi ASM nell'ambiente SAN (Storage Area Network), a seconda dell'ambiente, eseguire una delle seguenti operazioni:

Se si utilizzano dischi ASM con...	Quindi...
ASMLib su FCP e iSCSI su Linux	Modificare l'autorizzazione del proprietario del software Oracle e del gruppo primario dell'utente utilizzando solo il dispositivo a caratteri. Il percorso ASM_DISKSTRING deve essere ASM_DISKSTRING = ORCL:*
FCP e iSCSI su AIX	Aggiungere il nome del percorso per il parametro ASM_DISKSTRING fino al percorso della directory ASM. Il percorso ASM_DISKSTRING deve essere ASM_DISKSTRING = /dev/hdsk/*, dove * indica il nome del disco ASM.
FCP e iSCSI su Solaris	Aggiungere il nome del percorso per il parametro ASM_DISKSTRING fino al percorso della directory ASM. Il percorso ASM_DISKSTRING deve essere ASM_DISKSTRING = /dev/rdisk/*, dove * indica il nome del disco ASM. +

"Documentazione Oracle: www.oracle.com/technetwork/indexes/documentation/index.html"

Sicurezza e gestione delle credenziali

È possibile gestire la sicurezza in SnapManager applicando autenticazione dell'utente e RBAC (role-based access control). Il metodo di autenticazione dell'utente consente di accedere a risorse come repository, host e profili. RBAC consente di limitare le operazioni che SnapManager può eseguire rispetto ai volumi e alle LUN contenenti i file di dati nel database.

Quando si esegue un'operazione utilizzando l'interfaccia della riga di comando (CLI) o l'interfaccia utente grafica (GUI), SnapManager recupera il set di credenziali per repository e profili. SnapManager salva le credenziali delle installazioni precedenti.

Il repository e i profili possono essere protetti con una password. Una credenziale è la password configurata per l'utente per un oggetto e la password non è configurata sull'oggetto stesso.

È possibile gestire l'autenticazione e le credenziali eseguendo le seguenti operazioni:

- Gestire l'autenticazione dell'utente tramite richieste di password sulle operazioni o utilizzando il comando `smo credential set`.

Impostare le credenziali per un repository, un host o un profilo.

- Visualizzare le credenziali che regolano le risorse a cui si ha accesso.
- Cancellare le credenziali di un utente per tutte le risorse (host, repository e profili).
- Eliminare le credenziali di un utente per le singole risorse (host, repository e profili).

È possibile gestire l'accesso in base al ruolo eseguendo le seguenti operazioni:

- Abilitare RBAC per SnapManager utilizzando SnapDrive.
- Assegnare gli utenti ai ruoli e impostare le funzionalità dei ruoli utilizzando la console di Operations Manager.
- Facoltativamente, abilitare SnapManager per memorizzare le password crittografate modificando il file `smo.config`.

Se Protection Manager è installato, l'accesso alle funzionalità è interessato nei seguenti modi:

- Se è installato Gestione protezione, quando si crea un profilo di database, SnapManager crea un dataset e inserisce nel dataset i volumi che contengono i file di database.

Dopo un'operazione di backup, SnapManager mantiene il contenuto del dataset sincronizzato con i file di database.

- Se Gestione protezione non è installato, SnapManager non può creare un dataset e non è possibile impostare la protezione sui profili.

Che cos'è l'autenticazione dell'utente

Oltre a utilizzare RBAC (Role-Based Access Control), SnapManager autentica l'utente utilizzando un accesso al sistema operativo sull'host in cui è in esecuzione il server SnapManager. È possibile attivare l'autenticazione dell'utente tramite la richiesta di password sulle operazioni o utilizzando il comando `smo credential set`.

I requisiti di autenticazione dell'utente dipendono da dove viene eseguita l'operazione.

- Se il client SnapManager si trova sullo stesso server dell'host SnapManager, l'utente viene autenticato dalle credenziali del sistema operativo.

Non viene richiesta una password perché si è già connessi all'host in cui è in esecuzione il server SnapManager.

- Se il client SnapManager e il server SnapManager si trovano su host diversi, SnapManager deve autenticare l'utente con entrambe le credenziali del sistema operativo.

Se non sono state salvate le credenziali del sistema operativo nella cache delle credenziali utente di SnapManager, SnapManager richiede le password per qualsiasi operazione. Se si immette il comando `smo credential set -host`, le credenziali del sistema operativo vengono salvate nel file della cache delle credenziali di SnapManager e SnapManager non richiede la password per alcuna operazione.

Se si è autenticati con il server SnapManager, si è considerati l'utente effettivo. L'utente effettivo per qualsiasi operazione deve essere un account utente valido sull'host su cui viene eseguita l'operazione. Ad esempio, se si esegue un'operazione di clonazione, dovrebbe essere possibile accedere all'host di destinazione per il clone.



SnapManager per Oracle potrebbe non autorizzare gli utenti creati nei servizi Active Directory centrali, come LDAP e ADS. Per garantire che l'autenticazione non abbia esito negativo, è necessario impostare l'opzione configurabile `auth.disableServerAuthorization` su `true`.

In qualità di utente efficace, è possibile gestire le credenziali nei seguenti modi:

- In alternativa, è possibile configurare SnapManager in modo che memorizzi le credenziali utente nel file delle credenziali utente di SnapManager.

Per impostazione predefinita, SnapManager non memorizza le credenziali host. Ad esempio, se si dispone di script personalizzati che richiedono l'accesso su un host remoto, è possibile modificare questa impostazione. L'operazione di clonazione remota è un esempio di un'operazione SnapManager che richiede le credenziali di accesso di un utente per un host remoto. Per fare in modo che SnapManager memorizzi le credenziali di accesso dell'host utente nella cache delle credenziali utente di SnapManager, impostare la proprietà `host.credentials.Persist` su `true` nel file `smo.config`.

- È possibile autorizzare l'accesso dell'utente al repository.
- È possibile autorizzare l'accesso degli utenti ai profili.
- È possibile visualizzare tutte le credenziali utente.
- È possibile cancellare le credenziali di un utente per tutte le risorse (host, repository e profili).
- È possibile eliminare le credenziali per le singole risorse (host, repository e profili).

Informazioni sul controllo degli accessi in base al ruolo

RBAC (role-based access control) consente di controllare chi ha accesso alle operazioni SnapManager. RBAC consente agli amministratori di gestire gruppi di utenti definendo ruoli e assegnando utenti a tali ruoli. Si consiglia di utilizzare RBAC SnapManager in ambienti in cui RBAC è già in uso.

RBAC include i seguenti componenti:

- Risorse: Volumi e LUN che conservano i file di dati che compongono il database.
- Funzionalità: Tipi di operazioni che possono essere eseguite su una risorsa.
- Utenti: Persone alle quali si concedono funzionalità.
- Ruoli: Un insieme di risorse e funzionalità consentite sulle risorse. Assegnare un ruolo specifico a un utente che deve eseguire tali funzionalità.

Attivare RBAC in SnapDrive. È quindi possibile configurare funzionalità specifiche per ruolo nell'interfaccia grafica utente o nell'interfaccia della riga di comando di Operations Manager Web. I controlli RBAC vengono eseguiti nel server DataFabric Manager.

La tabella seguente elenca alcuni ruoli e le attività tipiche, come impostato in Operations Manager.

Ruolo	Attività tipiche
Amministratore del database Oracle	<ul style="list-style-type: none"> • Creazione, manutenzione e monitoraggio di un database Oracle che risiede su un host • Pianificazione e creazione di backup del database • Garantire che i backup siano validi e possano essere ripristinati • Cloning di database

Ruolo	Attività tipiche
Amministratore del server	<ul style="list-style-type: none"> • Configurazione di aggregati e sistemi storage • Monitoraggio dei volumi per lo spazio libero • Provisioning dello storage su richiesta degli utenti • Configurazione e monitoraggio del mirroring del disaster recovery
Storage architect	<ul style="list-style-type: none"> • Prendere decisioni architetturali sullo storage • Pianificazione della crescita della capacità dello storage • Pianificazione delle strategie di disaster recovery • Delegare le funzionalità ai membri del team

Se RBAC è in uso (vale a dire che Operations Manager è installato e RBAC è attivato in SnapDrive), l'amministratore dello storage deve assegnare le autorizzazioni RBAC a tutti i volumi e i sistemi di storage per i file di database.

Controllo degli accessi basato sui ruoli

Il RBAC (Role-Based Access Control) di SnapManager viene attivato tramite SnapDrive. All'installazione di SnapDrive, RBAC viene disattivato per impostazione predefinita. Dopo aver attivato RBAC in SnapDrive, SnapManager esegue le operazioni con RBAC attivato.

Il file snapdrive.config in SnapDrive imposta molte opzioni, una delle quali attiva RBAC.

La documentazione di SnapDrive contiene dettagli su SnapDrive.

1. Aprire il file snapdrive.conf in un editor.
2. Abilitare RBAC modificando il valore del parametro rbac-method da nativo a dfm.

Il valore predefinito per questo parametro è nativo, che disattiva RBAC.

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

Definizione di ruoli e funzionalità di controllo degli accessi in base al ruolo

Dopo aver attivato RBAC (role-based access control) per SnapManager utilizzando SnapDrive, è possibile aggiungere utenti e funzionalità RBAC ai ruoli per eseguire operazioni SnapManager.

È necessario creare un gruppo nel server Data Fabric Manager e aggiungerlo ai sistemi di storage primario e secondario. Eseguire i seguenti comandi:

- il gruppo dfm crea smo_grp
- il gruppo dfm aggiunge smo_grpprimary_storage_system
- il gruppo dfm aggiunge smo_grpsecondary_storage_system

È possibile utilizzare l'interfaccia Web di Operations Manager o l'interfaccia a riga di comando del server Data Fabric Manager (CLI) per modificare le funzionalità e i ruoli RBAC.

La tabella elenca le funzionalità RBAC necessarie per eseguire le operazioni SnapManager:

Operazioni SnapManager	Funzionalità RBAC richieste quando la protezione dei dati non è attivata	Funzionalità RBAC richieste quando è attivata la protezione dei dati
Creazione del profilo o aggiornamento del profilo	SD.Storage.Read (smo_grp)	SD.Storage.Read (dataset SMO_Profile)
Protezione del profilo	DFM.Database.Write (smo_grp) SD.Storage.Read (smo_grp) SD.Config.Read (smo_grp) SD.Config.Write (smo_grp) SD.Config.Delete (smo_GRP) GlobalDataProtection	Nessuno
Creazione del backup	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Write (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.Snapshot.Delete (dataset SMO_Profile)
Creazione del backup (con DBverify)	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.snapshot.Clone (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Write (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.Snapshot.Delete (dataset SMO_Profile) SD.snapshot.Clone (set di dati SMO_Profile)

Operazioni SnapManager	Funzionalità RBAC richieste quando la protezione dei dati non è attivata	Funzionalità RBAC richieste quando è attivata la protezione dei dati
Creazione di backup (con RMAN)	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.snapshot.Clone (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Write (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.Snapshot.Delete (dataset SMO_Profile) SD.snapshot.Clone (set di dati SMO_Profile)
Ripristino del backup	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.snapshot.Clone (smo_grp) SD.Snapshot.Restore (smo_GRP)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Write (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.Snapshot.Delete (dataset SMO_Profile) SD.snapshot.Clone (set di dati SMO_Profile) SD.Snapshot.Restore (dataset SMO_Profile)
Eliminazione del backup	SD.Snapshot.Delete (smo_grp)	SD.Snapshot.Delete (dataset SMO_Profile)
Verifica del backup	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.Snapshot.Clone (set di dati SMO_Profile)

Operazioni SnapManager	Funzionalità RBAC richieste quando la protezione dei dati non è attivata	Funzionalità RBAC richieste quando è attivata la protezione dei dati
Montaggio di backup	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.Snapshot.Clone (set di dati SMO_Profile)
Dismount del backup	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (set di dati SMO_Profile)
Creazione di cloni	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.snapshot.Clone (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.snapshot.Clone (set di dati SMO_Profile)
Eliminare i cloni	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (set di dati SMO_Profile)
Suddivisione dei cloni	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.snapshot.Clone (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Storage.Write (smo_grp)	SD.Storage.Read (dataset SMO_Profile) SD.Snapshot.Read (dataset SMO_Profile) SD.snapshot.Clone (set di dati SMO_Profile) SD.Snapshot.Delete (dataset SMO_Profile) SD.Storage.Write (dataset SMO_Profile)

Per ulteriori informazioni sulla definizione delle funzionalità RBAC, consultare la *Guida all'amministrazione di Gestione operazioni di Unified Manager di OnCommand*.

1. Accedere alla console di Operations Manager.
2. Dal menu Setup, selezionare **Roles** (ruoli).
3. Selezionare un ruolo esistente o crearne uno nuovo.
4. Per assegnare le operazioni alle risorse di storage del database, fare clic su **Add Capabilities** (Aggiungi funzionalità).

5. Nella pagina Edit Role Settings (Modifica impostazioni ruolo), per salvare le modifiche apportate al ruolo, fare clic su **Update** (Aggiorna).

Informazioni correlate

"OnCommand Unified Manager Operations Manager Administration Guide:

mysupport.netapp.com/documentation/productsatoz/index.html"

Memorizzazione di password crittografate per script personalizzati

Per impostazione predefinita, SnapManager non memorizza le credenziali host nella cache delle credenziali utente. Tuttavia, è possibile modificare questa impostazione. È possibile modificare il file smo.config per consentire l'archiviazione delle credenziali dell'host.

Il file smo.config si trova in <default installation location>/properties/smo.config

1. Modificare il file smo.config.
2. Impostare host.credentials.persistere su true.

Autorizzare l'accesso al repository

Oltre al RBAC (role-based access control), SnapManager consente di impostare le credenziali per gli utenti del database per accedere al repository. Utilizzando le credenziali, è possibile limitare o impedire l'accesso agli host, ai repository, ai profili e ai database di SnapManager.

Se si impostano le credenziali utilizzando il comando credential set, SnapManager non richiede la password.

È possibile impostare le credenziali utente quando si installa SnapManager o versioni successive.

1. Immettere il seguente comando:

```
'set di credenziali mo -repository -dbname repo_service_name -host repo_host -login -username  
repo_username [-password repo_password] -port repo_port'
```

Autorizzazione dell'accesso ai profili

Oltre al RBAC (role-based access control), SnapManager consente di impostare una password per un profilo per impedire accessi non autorizzati.

1. Immettere il seguente comando: 'Set di credenziali MO -profile -name profile_name [-password password]'

Informazioni correlate

[Il comando smo credential set](#)

Visualizzazione delle credenziali dell'utente

È possibile elencare gli host, i profili e i repository a cui si ha accesso.

1. Per elencare le risorse a cui si ha accesso, immettere questo comando: `smo credential list`

Esempio di visualizzazione delle credenziali utente

In questo esempio vengono visualizzate le risorse a cui si dispone dell'accesso.

```
smo credential list
```

```
Credential cache for OS user "user1":  
Repositories:  
Host1_test_user@SMOREPO/hotspur:1521  
Host2_test_user@SMOREPO/hotspur:1521  
user1_1@SMOREPO/hotspur:1521  
Profiles:  
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)  
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)  
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]  
Hosts:  
Host2  
Host5
```

Informazioni correlate

[Il comando `smo credential list`](#)

Cancellazione delle credenziali utente per tutti gli host, i repository e i profili

È possibile cancellare la cache delle credenziali per le risorse (host, repository e profili). In questo modo vengono eliminate tutte le credenziali delle risorse per l'utente che esegue il comando. Dopo aver cancellato la cache, è necessario autenticare nuovamente le credenziali per accedere a queste risorse protette.

1. Per cancellare le credenziali, immettere il comando `smo credential clear` dall'interfaccia utente di SnapManager oppure selezionare **Amministratore > credenziali > Cancella cache** dall'interfaccia utente di SnapManager.
2. Uscire dalla GUI di SnapManager.

NOTA:

- Se la cache delle credenziali è stata cancellata dalla GUI di SnapManager, non è necessario uscire dalla GUI di SnapManager.
- Se la cache delle credenziali è stata cancellata dall'interfaccia utente di SnapManager, è necessario riavviare l'interfaccia utente di SnapManager.

- Se il file di credenziale crittografato è stato eliminato manualmente, è necessario riavviare nuovamente l'interfaccia grafica di SnapManager.
3. Per impostare nuovamente le credenziali, ripetere la procedura per impostare le credenziali per il repository, l'host del profilo e il profilo. Per ulteriori informazioni sulla nuova impostazione delle credenziali utente, fare riferimento a "impostazione delle credenziali dopo la cancellazione della cache delle credenziali".

Informazioni correlate

[Il comando smo credential clear](#)

Impostazione delle credenziali dopo la cancellazione della cache delle credenziali

Dopo aver cancellato la cache per rimuovere le credenziali utente memorizzate, è possibile impostare le credenziali per gli host, i repository e i profili.

È necessario assicurarsi di impostare le stesse credenziali utente per il repository, l'host del profilo e il profilo forniti in precedenza. Durante l'impostazione delle credenziali utente viene creato un file di credenziali crittografato.

Il file delle credenziali si trova in `/root/.netapp/smo/3.3.0`.

Dall'interfaccia grafica utente (GUI) di SnapManager, se non è presente alcun repository in Repository, attenersi alla seguente procedura:

1. Fare clic su **Tasks > Add Existing Repository** (Aggiungi repository esistente) per aggiungere un repository esistente.
2. Per impostare le credenziali per il repository, attenersi alla seguente procedura:
 - a. Fare clic con il pulsante destro del mouse sul repository e selezionare **Apri**.
 - b. Nella finestra Repository Credentials Authentication (autenticazione credenziali repository), immettere le credenziali utente.
3. Per impostare le credenziali per l'host, attenersi alla seguente procedura:
 - a. Fare clic con il pulsante destro del mouse sull'host sotto il repository e selezionare **Open** (Apri).
 - b. Nella finestra host Credentials Authentication (autenticazione credenziali host), immettere le credenziali dell'utente.
4. Per impostare le credenziali per il profilo, procedere come segue:
 - a. Fare clic con il pulsante destro del mouse sul profilo sotto l'host e selezionare **Open** (Apri).
 - b. Nella finestra Profile Credentials Authentication (autenticazione credenziali profilo), immettere le credenziali dell'utente.

Eliminazione delle credenziali per le singole risorse

È possibile eliminare le credenziali di una qualsiasi delle risorse protette, ad esempio un profilo, un repository o un host. In questo modo è possibile rimuovere le credenziali di una sola risorsa, invece di cancellare le credenziali dell'utente per tutte le risorse.

Informazioni correlate

[Il comando smo credential delete](#)

Eliminazione delle credenziali utente per i repository

È possibile eliminare le credenziali in modo che un utente non possa più accedere a un determinato repository. Questo comando consente di rimuovere le credenziali per una sola risorsa, invece di cancellare le credenziali dell'utente per tutte le risorse.

1. Per eliminare le credenziali di un repository per un utente, immettere il comando: 'Mo credential delete -repository-dbname repo_service_name-host repo_host-login -username repo_username-port repo_port'

Eliminazione delle credenziali utente per gli host

È possibile eliminare le credenziali di un host in modo che un utente non possa più accedervi. Questo comando consente di rimuovere le credenziali per una sola risorsa, invece di cancellare tutte le credenziali dell'utente per tutte le risorse.

1. Per eliminare le credenziali host per un utente, immettere il seguente comando: 'Mo credential delete -host -name host_name-Username-Username'

Eliminazione delle credenziali utente per i profili

È possibile eliminare le credenziali utente per un profilo in modo che un utente non possa più accedervi.

1. Per eliminare le credenziali del profilo per un utente, immettere il seguente comando: "MO credential delete -profile-name profile_name"

Gestione dei profili per backup efficienti

È necessario creare un profilo in SnapManager per il database sul quale si desidera eseguire un'operazione. Selezionare il profilo e quindi l'operazione che si desidera eseguire.

Attività correlate ai profili

È possibile eseguire le seguenti operazioni:

- Creare profili per consentire backup completi o parziali e backup su storage primario, secondario o anche terzo.

È inoltre possibile creare profili per separare i backup del registro di archiviazione dai backup del file di dati.

- Verificare i profili.
- Aggiornare i profili.
- Eliminare i profili.

Informazioni sui profili e sull'autenticazione

Quando si crea un profilo, è possibile specificare un database e scegliere uno dei seguenti metodi per connettersi al database:

- Autenticazione Oracle con nome utente, password e porta
- Autenticazione del sistema operativo senza nome utente, password o porta.

Per l'autenticazione del sistema operativo, è necessario immettere le informazioni relative all'utente e al gruppo dell'account del sistema operativo.



Per utilizzare l'autenticazione del sistema operativo per i database dei cluster di applicazioni reali (RAC), il server SnapManager deve essere in esecuzione su ciascun nodo dell'ambiente RAC e la password del database deve essere la stessa per tutte le istanze Oracle in un ambiente RAC. SnapManager utilizza il nome utente e la password del database per connettersi a ogni istanza RAC nel profilo.

- Autenticazione del database quando `sqlnet.authentication_services` è impostato SU NESSUNO. SnapManager utilizza quindi il nome utente e la password del database per tutte le connessioni al database di destinazione.



Per utilizzare l'autenticazione del database per un'istanza di Automatic Storage Management (ASM), è necessario immettere il nome utente e la password utilizzati per accedere all'istanza di ASM.

È possibile impostare `sqlnet.authentication_services` su NONE solo nei seguenti ambienti:

Layout del database	Versione di Oracle	È supportata l'autenticazione del database per il database di destinazione	L'autenticazione del database è supportata per l'istanza ASM
Qualsiasi database non ASM e non RAC	Oracle 10g e Oracle 11g (meno di 11.2.0.3)	Sì	No
Database ASM standalone su UNIX	Oracle 11.2.0.3 e versioni successive	Sì	Sì
Istanza ASM sul database RAC su UNIX	Oracle 11.2.0.3	No	No
Database RAC su NFS	Oracle 11.2.0.3	Sì	No

Nota: dopo aver disattivato `sqlnet.authentication_services` e modificato il metodo di autenticazione in autenticazione del database, è necessario impostare `sqlnet.authentication_services` su NONE.

Se si accede a un profilo per la prima volta, è necessario inserire la password del profilo. Dopo aver immesso le credenziali, è possibile visualizzare i backup del database all'interno del profilo.

Informazioni correlate

[Quali sono i profili](#)

Creazione di profili

Durante la creazione dei profili, è possibile assegnare un account utente del database Oracle specifico al profilo. È possibile impostare il criterio di conservazione per il profilo, attivare la protezione del backup sullo storage secondario per tutti i backup utilizzando questo profilo e impostare il numero di conservazione e la durata per ciascuna classe di conservazione.

Se non si forniscono i valori dei parametri -login, -password e -port del database, la modalità di autenticazione del sistema operativo utilizza le credenziali predefinite.

Durante la creazione di un profilo, SnapManager esegue un controllo dell'idoneità al ripristino per determinare il meccanismo di ripristino che può essere utilizzato per ripristinare il database. Se il database si trova su un qtree e il volume padre non è idoneo per un ripristino rapido o basato su volume, l'analisi potrebbe essere errata.

SnapManager (3.2 o versione successiva) consente di separare i file di log dell'archivio dai file di dati durante la creazione di un nuovo profilo o l'aggiornamento di un profilo esistente. Dopo aver separato il backup utilizzando il profilo, è possibile creare solo il backup dei file di dati o il backup del database solo log di archiviazione. È possibile utilizzare il nuovo profilo o il profilo aggiornato per creare il backup contenente sia i file di dati che i file di log dell'archivio. Tuttavia, non è possibile utilizzare il profilo per creare il backup completo o ripristinare le impostazioni.

Profili per la creazione di backup completi e parziali

È possibile creare profili per creare il backup completo del database contenente i file di dati, i file di controllo e i file di log dell'archivio e il backup parziale del database contenente file di dati o tablespace specifici, tutti i file di controllo e tutti i file di log dell'archivio. SnapManager non consente di creare backup separati del registro di archiviazione utilizzando i profili creati per backup completi e parziali.

Profili per la creazione di backup solo file di dati e backup solo archivio

Quando si crea un nuovo profilo, è possibile includere -separate-archivelog-backups per separare il backup del registro di archiviazione dal backup del file di dati. È inoltre possibile aggiornare il profilo esistente per separare il backup del registro di archiviazione dal backup del file di dati.

Utilizzando le nuove opzioni del profilo per separare i backup del registro di archiviazione, è possibile eseguire le seguenti operazioni SnapManager:

- Creare un backup del registro di archiviazione
- Eliminare un backup del registro di archiviazione
- Montare un backup del registro di archiviazione
- Liberare un backup del registro di archiviazione

Durante la creazione del profilo per separare i backup del log di archiviazione dal backup dei file di dati, se i file di log di archiviazione non esistono nel database per cui è stato creato il profilo, nel file system attivo non esiste un messaggio di avviso file di log archiviato. Vengono visualizzate le versioni dei file di log archiviati precedenti al file di log di <archive log thread version> non incluse nel backup. Anche se si creano backup per questo database, i file di log dell'archivio non sono disponibili nei backup del database.



Se si verifica un errore durante la creazione di un profilo, utilizzare il comando smosystem dump. Dopo aver creato un profilo, se si verifica un errore, utilizzare i comandi smoooperation dump e smoprofile dump.

1. Per creare un profilo con nome utente, password e porta (autenticazione Oracle), immettere il seguente comando: 'Mo profile create -profileprofile [-profile-passwordprofile_password] -repository -dbnamerepo_dbname-hostrepo_host-portrepo_port-login-username] [-durasn-nomeselloconto] [-nomeselloconto] [-nomesello] [-nomeselloconto] {} [-nomeselloconto]_nome_utente] [-nomeselloconto] [-nomeselloconto] } }]_nomeselloconto] [-nomeselloconto] [-nomeselloconto]_nome_nome_utente] [-nomeselloconto] [-nomeselloconto]nomeselloconto] [-nomeselloconto]_nome_nomeselloconto] [-nomeselloconto] [-nomeselloconto]_nome_nome_utente]_nomeselloconto]

Le altre opzioni per questo comando sono le seguenti:

'[-force] [-noprompt]

'[quiet | verbose]



Per gli ambienti RAC (Real Application Clusters), quando si crea un nuovo profilo, è necessario fornire il valore del parametro db_unique_name come db_dbname.

È inoltre possibile includere altre opzioni durante la creazione dei profili, a seconda di come si desidera accedere al database.

Se...	Quindi...
Si desidera utilizzare l'autenticazione del sistema operativo per creare il profilo	<p>Specificare le variabili per un account del sistema operativo nel gruppo DBA (in genere l'account utilizzato per installare Oracle). Invece di aggiungere il nome utente, la password e la porta, specificare quanto segue:</p> <ul style="list-style-type: none"> • -osaccountaccount_name come nome dell'account del sistema operativo • -osgrouposgroup come gruppo associato all'account del sistema operativo
Si desidera utilizzare l'autenticazione dell'istanza di Automatic Storage Management (ASM) per creare il profilo	<p>Specificare le credenziali per l'autenticazione dell'istanza ASM.</p> <ul style="list-style-type: none"> • -Asmusernameasmintance_username è il nome utente utilizzato per accedere all'istanza di ASM. • -Asmpasswordasminstance_password è la password utilizzata per accedere all'istanza di ASM.

<p>Si desidera utilizzare l'autenticazione del database per creare un profilo</p>	<p>Specificare i dettagli di accesso al database. Se la password contiene caratteri speciali come punto esclamativo (!), simbolo del dollaro (\$) o accento grave (`), SnapManager non consente di creare il profilo autenticato dal database dall'interfaccia della riga di comando (CLI).</p>
<p>Stai utilizzando un catalogo come repository di Oracle Recovery Manager (RMAN)</p>	<p>Specificare le seguenti opzioni e variabili:</p> <ul style="list-style-type: none"> • -tnsnametnsname come nome tnsname definito nel file tnsnames.ora. • -Login -username nome utente come nome utente richiesto per la connessione al catalogo RMAN. <p>Se non specificato, SnapManager utilizza le informazioni di autenticazione del sistema operativo. Non è possibile utilizzare l'autenticazione del sistema operativo con i database RAC.</p> <ul style="list-style-type: none"> • -Passwordpassword come password RMAN necessaria per la connessione al catalogo RMAN.
<p>Il file di controllo viene utilizzato come repository RMAN</p>	<p>Specificare l'opzione -controlfile.</p>
<p>Specificare un criterio di conservazione del backup per i backup</p>	<p>Specificare il numero di conservazione o la durata di una classe di conservazione o entrambi. La durata è espressa in unità della classe (ad esempio, ore per ora, giorni per giorno).</p> <ul style="list-style-type: none"> • -hourly è la classe di conservazione oraria, per la quale [-count n] [-duration m] sono rispettivamente il conteggio di conservazione e la durata di conservazione. • -daily è la classe di conservazione giornaliera, per la quale [-count n] [-durationm] sono rispettivamente il conteggio di conservazione e la durata di conservazione. • -settimanale è la classe di conservazione settimanale, per la quale [-count n] [-duration m] sono rispettivamente il conteggio di conservazione e la durata di conservazione. • -mensile è la classe di conservazione mensile, per la quale [-count n] [-durationm] sono rispettivamente il conteggio e la durata della conservazione.

Si desidera attivare la protezione di backup per il profilo

Specificare le seguenti opzioni e variabili:

- -protect consente la protezione del backup.

Se si utilizza Data ONTAP in 7-Mode, questa opzione crea un set di dati dell'applicazione nel server DFM (Data Fabric Manager) e aggiunge membri correlati al database, al file di dati, ai file di controllo e ai registri di archiviazione. Se il dataset esiste già, lo stesso dataset viene riutilizzato quando viene creato un profilo.

- il criterio -protection-policy consente di specificare il criterio di protezione.

Se si utilizza Data ONTAP in 7-Mode e SnapManager è integrato con Protection Manager, è necessario specificare uno dei criteri di Protection Manager.



Per elencare i possibili criteri di protezione, utilizzare il comando `Protection-policy list`.

Se si utilizza Clustered Data ONTAP, selezionare *SnapManager_cDOT_Mirror* o *SnapManager_cDOT_Vault*.



L'operazione di creazione del profilo non riesce nei seguenti scenari:

- Se si utilizza Clustered Data ONTAP ma si seleziona il criterio Gestione protezione
 - Se si utilizza Data ONTAP in 7-Mode ma si seleziona il criterio *SnapManager_cDOT_Mirror* o *SnapManager_cDOT_Vault*
 - Se è stata creata una relazione SnapMirror ma è stata selezionata la policy *SnapManager_cDOT_Vault* o è stata creata una relazione SnapVault, ma è stata selezionata la policy *SnapManager_cDOT_Mirror*
 - Se non è stata creata una relazione SnapMirror o SnapVault ma è stata selezionata la policy *SnapManager_cDOT_Vault* o *SnapManager_cDOT_Mirror*
- -noprotect indica di non proteggere i backup del database creati utilizzando il profilo. **Nota:** se -Protect viene specificato senza -Protection-policy, il dataset non avrà una policy di protezione. Se viene specificato -Protect e -Protection-policy non viene impostato al

Si desidera attivare la notifica via email per lo stato di completamento delle operazioni del database

Specificare le seguenti opzioni e variabili:

- -summary-notification consente di configurare una notifica email di riepilogo per più profili in un database repository.
- -notification consente di ricevere una notifica via email per lo stato di completamento dell'operazione del database per un profilo.
- -success-email_email_address2 consente di ricevere una notifica via email sull'operazione di database eseguita correttamente utilizzando un profilo nuovo o esistente.
- -failure-email_email_address2 consente di ricevere una notifica via email sull'operazione di database non riuscita eseguita utilizzando un profilo nuovo o esistente.
- -subject_subject_text specifica il testo dell'oggetto della notifica e-mail durante la creazione di un nuovo profilo o di un profilo esistente. Se le impostazioni di notifica non sono configurate per il repository e si tenta di configurare le notifiche di profilo o di riepilogo utilizzando l'interfaccia CLI, nel registro della console viene registrato il seguente messaggio:
"MO-14577: Notification Settings Not configured" (Impostazioni di notifica non configurate).

Se sono state configurate le impostazioni di notifica e si tenta di configurare la notifica di riepilogo utilizzando l'interfaccia CLI senza attivare la notifica di riepilogo per il repository, nel log della console viene visualizzato il seguente messaggio: "MO-14575: Summary notification Configuration not available for this repository__ ** _"

<p>Si desidera eseguire il backup dei file di log dell'archivio separatamente dai file di dati</p>	<p>Specificare le seguenti opzioni e variabili:</p> <ul style="list-style-type: none"> • <code>-separate-archivelog-backups</code> consente di separare il backup del log di archiviazione dal backup del file di dati. • <code>-retain-archivelog-backups</code> imposta la durata di conservazione per i backup del registro di archiviazione. Specificare una durata di conservazione positiva. <p>I backup del registro di archiviazione vengono conservati in base alla durata della conservazione del registro di archiviazione. I backup dei file di dati vengono conservati in base alle policy di conservazione esistenti.</p> <ul style="list-style-type: none"> • <code>-protect</code> consente di proteggere i backup dei log di archiviazione. • <code>-protection-policy</code> imposta il criterio di protezione sui backup del registro di archiviazione. <p>I backup del registro di archiviazione sono protetti in base alla policy di protezione del registro di archiviazione. I backup dei file di dati sono protetti in base alle policy di protezione esistenti.</p> <ul style="list-style-type: none"> • <code>-include-with-online-backups</code> include il backup del log di archiviazione insieme al backup del database online. <p>Questa opzione consente di creare insieme un backup dei file di dati online e un backup dei registri di archiviazione per la clonazione. Quando questa opzione è impostata, ogni volta che si crea un backup dei file di dati online, i backup dei registri dell'archivio vengono creati immediatamente insieme ai file di dati.</p> <ul style="list-style-type: none"> • <code>-no-include-with-online-backups</code> non include il backup del log di archiviazione insieme al backup del database.
<p>È possibile raccogliere i file dump dopo l'operazione di creazione del profilo riuscita</p>	<p>Specificare l'opzione <code>-dump</code> alla fine del comando di creazione del profilo.</p>

Quando si crea un profilo, SnapManager analizza i file nel caso in cui si desideri eseguire un'operazione di ripristino basata su volume sui file specificati nel profilo.

Informazioni correlate

[Come raccogliere i file dump](#)

Naming delle copie Snapshot

È possibile specificare una convenzione o un modello di denominazione per descrivere le copie Snapshot correlate al profilo creato o aggiornato. È inoltre possibile includere testo personalizzato in tutti i nomi delle copie Snapshot.

È possibile modificare il modello di denominazione della copia Snapshot quando si crea un profilo o dopo averlo creato. Il modello aggiornato si applica solo alle copie Snapshot che non si sono ancora verificate; le copie Snapshot esistenti mantengono il modello Snapname precedente.

Gli esempi seguenti mostrano i due nomi delle copie Snapshot presi per un volume. La seconda copia Snapshot elencata ha *F_H_1* al centro del nome. "1" indica che si tratta della prima copia Snapshot acquisita nel set di backup. La prima copia Snapshot elencata è la più recente e ha un "2", il che significa che è la seconda copia Snapshot acquisita. La copia Snapshot "1" include i file di dati; la copia Snapshot "2" include i file di controllo. Poiché le copie Snapshot del file di controllo devono essere eseguite dopo la copia Snapshot del file di dati, sono necessarie due copie Snapshot.

```
smo_profile_sid_f_h_2_8ae482831ad14311011ad14328b80001_0
smo_profile_sid_f_h_1_8ae482831ad14311011ad14328b80001_0
```

Il modello predefinito include il valore smid richiesto, come illustrato di seguito:

* Schema predefinito: smo_{profilo}_{db-sid}_{ambito}_{modalità}_{smid} * esempio:
smo_my_profile_rac51_f_h_2_8abc01e915a55ac50115a55acc8d0001_0'

È possibile utilizzare le seguenti variabili nel nome della copia Snapshot:

Nome della variabile	Descrizione	Valore di esempio
smid (obbligatorio)	L'ID univoco SnapManager è l'unico elemento richiesto quando si crea un nome per la copia Snapshot. Questo ID garantisce la creazione di un nome Snapshot univoco.	8abc01e915a55ac50115a55acc8d0001_0
Classe (opzionale)	Classe di conservazione associata al backup per il profilo e indicata da oraria (h), giornaliera (d), settimanale (w), mensile (m) o illimitata (u).	d
Commento (opzionale)	Commento associato al backup per il profilo. Gli spazi in questo campo verranno convertiti in caratteri di sottolineatura una volta completato il nome della copia Snapshot.	sample_comment_spaces_replace d

Data (opzionale)	Data in cui viene eseguito il backup per il profilo. Se necessario, i valori delle date vengono aggiunti a zero. (aaaammgg)	20070218
db-host (opzionale)	Nome host del database associato al profilo da creare o aggiornare.	my_host
db-name (opzionale)	Nome del database associato alla copia Snapshot creata.	rac5
db-sid (opzionale)	sid del database associato alla copia Snapshot creata.	rac51
Etichetta (opzionale)	Etichetta associata al backup del profilo.	sample_label
Mode (opzionale)	Specifica se il backup viene completato online (h) o offline (c).	h
Profilo (opzionale)	Nome del profilo associato al backup creato.	profilo personale
Scopo (opzionale)	Specifica se il backup è completo (f) o parziale (p).	f
Ora (opzionale)	Ora in cui viene eseguito il backup per il profilo. I valori di tempo per questa variabile utilizzano l'orologio a 24 ore e vengono aggiunti degli zeri, se necessario. Ad esempio, 5:32 e 8 secondi vengono visualizzati come 053208 (hhmmss).	170530
Fuso orario (opzionale)	Fuso orario specificato per l'host del database di destinazione.	EST
Testo utente (opzionale)	Testo personalizzato che è possibile inserire.	prod

Nota: SnapManager per Oracle non supporta il simbolo dei due punti (:) nelle forme lunghe dei nomi delle copie Snapshot.

Ridenominazione dei profili

SnapManager consente di rinominare il profilo quando lo si aggiorna. Le funzionalità SnapManager impostate sul profilo e le operazioni che è possibile eseguire prima della

ridenominazione vengono conservate per il profilo rinominato.

- Durante la ridenominazione del profilo, assicurarsi che non siano in esecuzione operazioni SnapManager.

È possibile rinominare il profilo sia dall'interfaccia della riga di comando (CLI) di SnapManager che dall'interfaccia grafica utente (GUI). Durante l'aggiornamento del profilo, SnapManager verifica e aggiorna il nome del profilo nel repository.



SnapManager non supporta la ridenominazione del profilo nella finestra di aggiornamento multiprofilo.

Quando si fornisce un nuovo nome profilo, il nuovo nome del profilo viene aggiunto nella cache delle credenziali lato client e il nome del profilo precedente viene rimosso. Quando si rinomina il profilo da un client, viene aggiornata la cache delle credenziali di solo quel client. Per aggiornare la nuova cache delle credenziali con il nuovo nome del profilo, è necessario eseguire il comando `smo profile Sync` da ciascun client.

È possibile impostare la password per il profilo utilizzando il comando `smo credential set`.

Se il nome del profilo è stato incluso in un modello di denominazione della copia Snapshot, quando si rinomina un profilo, il nuovo nome del profilo viene aggiornato. Tutte le operazioni SnapManager eseguite sul profilo utilizzano il nuovo nome del profilo. I backup creati con il profilo precedente continuano ad avere il nome del profilo precedente e vengono utilizzati per eseguire altre operazioni SnapManager.

Se si esegue un aggiornamento in sequenza degli host server SnapManager, assicurarsi di eseguire l'aggiornamento completo prima di rinominare il profilo.

Il nuovo nome del profilo viene aggiornato solo dal client SnapManager da cui viene effettuata la richiesta. I client SnapManager connessi al server SnapManager non ricevono alcuna notifica in merito alla modifica del nome del profilo. È possibile controllare il log delle operazioni per conoscere la modifica apportata al nome del profilo.



Se un'operazione di backup pianificata inizia al momento della ridenominazione del profilo, l'operazione pianificata non riesce.

1. Immettere il seguente comando: `'Mo profile update -profileprofile [-new-profilenew_profile_name]'`

Modifica delle password del profilo

Per proteggere i profili esistenti nel repository, è necessario aggiornare le password dei profili. È possibile applicare questa password aggiornata quando si crea un backup utilizzando questo profilo.

1. Per aggiornare la password del profilo per un profilo esistente, immettere il seguente comando:

`'aggiornamento del profilo -nome_profilo -password-profilo'`

Informazioni correlate

[Il comando di aggiornamento del profilo smo](#)

Reimpostazione della password del profilo

È possibile reimpostare la password del profilo se non si ricorda la password fornita durante la creazione del profilo.

- Assicurarsi che il server SnapManager sia in esecuzione nel database del repository.
- È necessario disporre delle credenziali utente root dell'host su cui risiede il database del repository.
- È necessario assicurarsi che il profilo non sia in uso per alcuna operazione quando si ripristina la password per tale profilo.

È possibile reimpostare la password dall'interfaccia utente di SnapManager o dalla GUI. Durante la reimpostazione della password, SnapManager interroga il server SnapManager sull'host del repository per identificare il sistema operativo per l'host del repository. Immettere le credenziali dell'utente autorizzato per la connessione all'host del repository. Il server SnapManager autentica gli utenti con le proprie credenziali root nel database del repository. Una volta completata l'autenticazione, SnapManager ripristina la password del profilo sul server SnapManager con la nuova password.



SnapManager non mantiene la cronologia delle operazioni di reimpostazione della password.

1. Reimpostare la password del profilo immettendo il seguente comando: 'MO password reset -profileprofile [-profile-passwordprofile_password] [-repository-hostadmin-passwordadmin_password]'

Autorizzazione dell'accesso ai profili

Oltre al RBAC (role-based access control), SnapManager consente di impostare una password per un profilo per impedire accessi non autorizzati.

1. Immettere il seguente comando: 'Set di credenziali MO -profile -name profile_name [-password password]'

Informazioni correlate

[Il comando smo credential set](#)

Verifica dei profili in corso

È possibile verificare che un profilo esistente sia impostato correttamente. Quando si verifica un profilo, SnapManager verifica l'ambiente per il profilo specificato e verifica che il profilo sia impostato e che il database di questo profilo sia accessibile.

1. Per verificare se il profilo è impostato correttamente, immettere questo comando: `smo profile verify -profile profile_name`

Informazioni correlate

[Il comando di verifica del profilo smo](#)

Aggiornamento dei profili

È possibile aggiornare i profili per modificare la password del profilo, il numero di backup da conservare, l'accesso al database, l'autenticazione del sistema operativo per

l'autenticazione del database e viceversa e le informazioni sull'host. Se le informazioni relative alla password del database Oracle cambiano, è necessario modificarle anche nel profilo.

Se il criterio di protezione è attivato nel profilo, non è possibile modificarlo utilizzando SnapManager. L'amministratore dello storage deve modificare il criterio utilizzando la console di Protection Manager.

SnapManager (3.2 o versione successiva) consente di aggiornare il profilo per separare i backup del registro di archiviazione dai backup del file di dati utilizzando l'opzione -separate-archiveed-backups. È possibile specificare una durata di conservazione separata e un criterio di protezione per il backup del registro di archiviazione. SnapManager consente di includere il backup del registro di archiviazione insieme al backup del database online. È inoltre possibile creare un backup dei file di dati online e un backup dei log di archiviazione per la clonazione. Quando si crea un backup dei file di dati online, i backup dei registri di archiviazione vengono creati immediatamente insieme ai file di dati.

```
1. Immettere il seguente comando: smo profile update -profileprofile [-new-profilenew_profile_name] [-profile-passwordprofile_password] [-database-dbnamedb_dbname-host db_host [-siddb_sid] [-login -usernameadb_username -password db_password-port db_port] [-asminstance-asmusernameasminstance_username-asmpasswordasminstance_password]] [{-rman{-controlfile | {-login -usernameerman_username-password rman_password-tnsname rman_tnsname}}} | -remove-rman]-osaccountosaccount-osgrouposgroup [-retain [-hourly [-countn] [-durationm]] [-daily [-countn] [-durationm]] [-weekly [-countn] [-durationm]] [-monthly [-countn] [-durationm]]] [-commentcomment] [-snapname-patternpattern] [[-protect [-protection-policypolicy_name]]] [[-noprotect]] [-summary-notification] [-notification [-success-emailemail_address1, email_address2-subjectsubject_pattern] [-failure-emailemail_address1, email_address2-subjectsubject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hourshours | -daysdays | -weeksweeks| -monthsmonths [-protect [-protection-policypolicy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]
```

Le altre opzioni per questo comando sono le seguenti:


[-force] [-noprompt]

Se si desidera...	Quindi...
Modificare il profilo per utilizzare l'autenticazione del sistema operativo	<div>Invece di aggiungere il nome utente, la password e la porta, specificare quanto segue:</div> <ul style="list-style-type: none">-osaccountaccount_name come nome dell'account del sistema operativo-Osgrouposgroup come gruppo associato all'account del sistema operativo, in genere l'account utilizzato per installare Oracle

Se si desidera...	Quindi...
Utilizzare l'autenticazione dell'istanza di Automatic Storage Management (ASM) per creare il profilo	<p>Specificare le credenziali per l'autenticazione dell'istanza ASM.</p> <ul style="list-style-type: none"> • -Asmusernameasminstance_username è il nome utente utilizzato per accedere all'istanza di ASM. • -Asmpasswordasminstance_password è la password utilizzata per accedere all'istanza di ASM.
Utilizzare un catalogo come repository di Oracle Recovery Manager (RMAN) oppure rimuovere RMAN	<p>Specificare le seguenti opzioni e variabili:</p> <ul style="list-style-type: none"> • -tnsname tnsname come nome tnsname definito nel file tnsnames.ora. • -Login -username username come nome utente necessario per la connessione al catalogo RMAN. <p>Se non specificato, SnapManager utilizza le informazioni di autenticazione del sistema operativo. Non è possibile utilizzare l'autenticazione del sistema operativo con i database RAC (Real Application Clusters).</p> <ul style="list-style-type: none"> • -Passwordpassword come password RMAN necessaria per la connessione al catalogo RMAN. • -controlfile se si utilizza il file di controllo come repository RMAN. • -Remove-rman per rimuovere RMAN.

Se si desidera...	Quindi...
Modificare il criterio di conservazione del backup per i backup del database nel profilo	<p>Specificare il numero di conservazione o la durata di conservazione per una classe di conservazione o entrambi per modificare il criterio di conservazione. La durata è espressa in unità della classe (ad esempio, ore per ora, giorni per giorno).</p> <ul style="list-style-type: none"> • -hourly è la classe di conservazione oraria, per la quale [-countn] [-durationm]] sono rispettivamente il conteggio di conservazione e la durata di conservazione. • -daily è la classe di conservazione giornaliera, per la quale [-countn] [-durationm]] sono rispettivamente il conteggio di conservazione e la durata di conservazione. • -settimanale è la classe di conservazione settimanale, per la quale [-countn] [-durationm]] sono rispettivamente il conteggio di conservazione e la durata di conservazione. • -mensile è la classe di conservazione mensile, per la quale [-countn] [-durationm]] sono rispettivamente il numero di conservazione e la durata di conservazione.
Disattiva la protezione del backup per il profilo	<p>Specificare -noprotect per non proteggere i backup del database creati utilizzando il profilo. Per un profilo con -Protect attivato, se si desidera disattivare Protect, viene visualizzato un messaggio di avviso che indica che questa azione eliminerà il dataset e non sarà possibile ripristinare o clonare i backup per questo profilo.</p>

Se si desidera...	Quindi...
<p>Attivare le notifiche e-mail per lo stato di completamento delle operazioni del database</p>	<p>Specificare le seguenti opzioni e variabili:</p> <ul style="list-style-type: none"> • -summary-notification consente di configurare una notifica email di riepilogo per più profili in un database repository. • -notification consente di ricevere una notifica via email sullo stato di completamento dell'operazione del database per un profilo. • -success-emailemail_address2 consente di ricevere una notifica via email dopo il completamento di un'operazione di database eseguita correttamente utilizzando un profilo nuovo o esistente. • -failure-emailemail_address2 consente di ricevere una notifica via email su un'operazione di database non riuscita eseguita utilizzando un profilo nuovo o esistente. • -subjectsubject_text specifica il testo dell'oggetto per la notifica e-mail durante la creazione di un nuovo profilo o di un profilo esistente. Se le impostazioni di notifica non sono configurate per il repository e si sta tentando di configurare le notifiche di profilo o di riepilogo utilizzando l'interfaccia della riga di comando (CLI), nel log della console viene registrato il seguente messaggio: SMO-14577: Notification Settings Not configured (Impostazioni di notifica non configurate). <p>Se sono state configurate le impostazioni di notifica e si sta tentando di configurare la notifica di riepilogo utilizzando la CLI senza attivare la notifica di riepilogo per il repository, il seguente messaggio viene registrato nel log della console: SMO-14575: Configurazione della notifica di riepilogo non disponibile per questo repository__**_</p>

Se si desidera...	Quindi...
<p>Aggiornare il profilo per creare separatamente il backup dei file di log dell'archivio</p>	<p>Specificare le seguenti opzioni e variabili:</p> <ul style="list-style-type: none"> • <code>-separed-archivelog-backups</code> consente di creare un backup dei file di log dell'archivio separatamente dai file di database. <p>Dopo aver specificato questa opzione, è possibile creare un backup solo file di dati o un backup solo archivio. Impossibile creare un backup completo. Inoltre, non è possibile ripristinare le impostazioni del profilo separando il backup. SnapManager conserva i backup in base ai criteri di conservazione per i backup creati prima di eseguire il backup solo per l'archiviazione.</p> <ul style="list-style-type: none"> • <code>-retain-archivelog-backups</code> imposta la durata di conservazione per i backup del registro di archiviazione. <div data-bbox="922 1066 976 1129" style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px auto;">  </div> <p style="margin-left: 40px;">Se si aggiorna il profilo per la prima volta, è possibile separare i backup del registro di archiviazione dal backup dei file di dati utilizzando l'opzione <code>-separate-archivelog-backups</code>; è necessario specificare la durata di conservazione per i backup del registro di archiviazione utilizzando l'opzione <code>-retain-archivelog-backups</code>. L'impostazione della durata della conservazione è facoltativa quando si aggiorna il profilo in un secondo momento.</p> <ul style="list-style-type: none"> • <code>-Protect</code> crea un dataset applicativo nel server DFM (Data Fabric Manager) e aggiunge membri correlati al database, al file di dati, ai file di controllo e ai log di archiviazione. <p style="margin-left: 40px;">Se il dataset esiste, viene riutilizzato quando viene creato un profilo.</p> <ul style="list-style-type: none"> • <code>-protection-policy</code> imposta il criterio di protezione sui backup del registro di archiviazione. • <code>-include-with-online-backups</code> specifica che il backup del registro di archiviazione è incluso insieme al backup del database. • <code>-no-include-with-online-backups</code> specifica che il backup del file di log dell'archivio non è incluso con il backup del database.

Se si desidera...	Quindi...
Modificare il nome host del database di destinazione	Specificare -hostnew_db_host per modificare il nome host del profilo.
Raccogliere i file dump dopo l'operazione di aggiornamento del profilo	Specificare l'opzione -dump.

2. Per visualizzare il profilo aggiornato, immettere il seguente comando: `smo profile show`

Informazioni correlate

[Come raccogliere i file dump](#)

Eliminazione dei profili

È possibile eliminare un profilo in qualsiasi momento, a condizione che non contenga backup completi o riusciti. È possibile eliminare i profili che contengono backup liberati o cancellati.

1. Per eliminare un profilo, immettere il seguente comando: `smo profile delete -profile profile_name`

Informazioni correlate

[Il comando `smo profile delete`](#)

Backup dei database

SnapManager consente di eseguire il backup dei dati sulle risorse di storage locali utilizzando script di post-elaborazione proteggendo i backup su risorse di storage secondarie o terziarie. La scelta di eseguire il backup sullo storage secondario offre un layer aggiuntivo che preserva i dati in caso di disastro.

SnapManager consente inoltre agli amministratori dello storage di configurare i propri backup in base ai piani di policy. Utilizzando SnapManager, gli amministratori possono identificare i backup non conformi ai requisiti delle policy e correggerli immediatamente.

SnapManager offre le seguenti opzioni per eseguire il backup, il ripristino e il ripristino dei dati nel database:

- Eseguire il backup dell'intero database o di una parte di esso.
Se si esegue il backup di una parte di esso, specificare un gruppo di tablespace o un gruppo di file di dati.
- Eseguire il backup dei file di dati e archiviare i file di log separatamente.
- Eseguire il backup dei database nello storage primario (detto anche storage locale) e proteggerli eseguendo il backup su storage secondario o terzo (detto anche storage remoto).
- Pianificare backup di routine.

In che modo SnapManager (3.2 o versioni successive) differisce dalle versioni precedenti di

SnapManager

SnapManager (3.1 o versioni precedenti) consente di creare backup completi del database che contengono file di dati, file di controllo e file di log dell'archivio.

SnapManager (3.1 o versioni precedenti) gestisce solo i file di dati. I file di log dell'archivio vengono gestiti utilizzando soluzioni esterne a SnapManager.

SnapManager (3.1 o versioni precedenti) impone i seguenti limiti nella gestione dei backup del database:

- **Impatto delle performance**

Quando si esegue un backup completo del database online (quando il database è in modalità di backup), le prestazioni del database si riducono per il periodo di tempo fino alla creazione del backup. In SnapManager (3.2 o versioni successive), è possibile eseguire backup del database limitati e frequenti backup del registro di archiviazione. L'esecuzione di frequenti backup dei log di archiviazione consente di impedire che il database venga inserito in modalità di backup.

- **Ripristino e ripristino manuali**

Quando i file di log dell'archivio richiesti non esistono nel file system attivo, gli amministratori del database devono identificare il backup che contiene i file di log dell'archivio, montare i backup del database e ripristinare il database ripristinato. Questo processo richiede molto tempo.

- **Limiti di spazio**

Quando viene creato un backup del database, le destinazioni del registro di archiviazione diventano piene, causando la mancata risposta del database fino a quando non viene creato spazio sufficiente sullo storage. In SnapManager (3.2 o versioni successive), i file di log dell'archivio possono essere eliminati periodicamente dal file system attivo per liberare spazio.

Perché i backup dei log di archiviazione sono importanti

I file di log dell'archivio sono necessari per far avanzare il database dopo l'esecuzione di un'operazione di ripristino. Ogni transazione su un database Oracle viene acquisita nei file di log dell'archivio (se il database si trova in modalità di log dell'archivio). Gli amministratori del database possono ripristinare i backup del database utilizzando i file di log dell'archivio.

Vantaggi dei backup solo per l'archiviazione

- Fornisce una durata di conservazione separata per i backup di solo archiviazione

È possibile ridurre la durata della conservazione per i backup di solo archivio necessari per il ripristino.

- Protegge i backup solo archiviando in base alle policy di protezione dei log di archiviazione

È possibile selezionare criteri di protezione diversi per i backup solo di archiviazione in base ai requisiti.

- Migliora le performance del database

- Consolida i backup dei log di archiviazione

SnapManager consolida i backup dei log di archiviazione ogni volta che si esegue un backup liberando i backup dei log di archiviazione duplicati.

Quali sono i backup del database SnapManager

SnapManager consente di eseguire diverse attività di backup. È possibile assegnare classi di conservazione per specificare la durata di conservazione del backup; una volta raggiunto tale limite di tempo, il backup viene eliminato.

- Creare backup sullo storage primario
- Creare backup protetti sulle risorse di storage secondarie
- Verificare che i backup siano stati completati correttamente
- Visualizzare un elenco di backup
- Pianifica i backup utilizzando l'interfaccia grafica utente
- Gestire il numero di backup conservati
- Risorse di backup gratuite
- Montare e smontare i backup
- Eliminare i backup

SnapManager crea i backup utilizzando una delle seguenti classi di conservazione:

- Ogni ora
- Ogni giorno
- Settimanale
- Mensile
- Senza limiti

Protection Manager deve essere installato per utilizzare i criteri di protezione per la protezione dei backup. Un backup può avere uno dei seguenti stati di protezione: Non richiesto, non protetto o protetto.

Se vengono aggiunti nuovi file di dati al database, è necessario creare immediatamente un nuovo backup. Inoltre, se si ripristina un backup eseguito prima dell'aggiunta dei nuovi file di dati e si tenta di eseguire il ripristino a un punto successivo all'aggiunta dei nuovi file di dati, il processo di ripristino automatico potrebbe non riuscire. Consultare la documentazione Oracle per ulteriori informazioni sul processo di ripristino dei file di dati aggiunti dopo un backup.

Quali sono i backup completi e parziali

È possibile scegliere di eseguire il backup dell'intero database o solo di una parte di esso. Se si sceglie di eseguire il backup di una parte del database, è possibile scegliere di eseguire il backup di un gruppo di tablespaces o file di dati. È possibile scegliere di eseguire un backup separato di tablespaces e file di dati.

La seguente tabella elenca i vantaggi e le conseguenze di ogni tipo di backup:

Tipo di backup	Vantaggi	Svantaggi
Completo	Riduce al minimo il numero di copie Snapshot. Per i backup online, ogni tablespace è in modalità di backup per l'intero tempo dell'operazione di backup. SnapManager esegue una copia Snapshot per ogni volume utilizzato dal database, più una copia Snapshot per ogni volume occupato dai file di log.	Per i backup online, ogni tablespace è in modalità di backup per l'intero tempo dell'operazione di backup.
Parziale	Riduce al minimo la quantità di tempo che ogni tablespace trascorre in modalità di backup. SnapManager raggruppa le copie Snapshot necessarie in base allo spazio di tabella. Ogni tablespace si trova in modalità di backup solo per un tempo sufficiente a creare le copie Snapshot. Questo metodo di raggruppamento delle copie Snapshot riduce al minimo le scritture dei blocchi fisici nei file di log durante un backup online.	Il backup può richiedere la creazione di copie Snapshot di più tablespace nello stesso volume. Questo metodo può far sì che SnapManager crei più copie Snapshot di un singolo volume durante l'operazione di backup.

Nota: sebbene sia possibile eseguire un backup parziale, è necessario eseguire sempre un backup completo dell'intero database.

Tipi di backup e numero di copie Snapshot

Il tipo di backup (completo o parziale) influisce sul numero di copie Snapshot create da SnapManager. Per un backup completo, SnapManager crea una copia Snapshot di ciascun volume, mentre per un backup parziale, SnapManager crea una copia Snapshot di ciascun file tablespace.



Data ONTAP limita il numero massimo di copie Snapshot a 255 per volume. È possibile raggiungere questo valore massimo solo se si configura SnapManager in modo da conservare un elevato numero di backup, in cui ciascun backup è costituito da numerose copie Snapshot.

Per mantenere un pool adeguato di backup disponibili, senza raggiungere il limite massimo di copie Snapshot per volume, è necessario rimuovere i backup quando non sono più necessari. È possibile configurare il criterio di conservazione di SnapManager per rimuovere i backup riusciti dopo aver raggiunto una soglia specifica per una frequenza di backup specifica. Ad esempio, dopo che SnapManager ha creato quattro backup giornalieri, SnapManager rimuove i backup giornalieri creati il giorno precedente.

Le seguenti tabelle mostrano come SnapManager crea copie Snapshot in base al tipo di backup. L'esempio nelle tabelle presuppone che il database Z includa due volumi, ciascun volume include due tablespace (TS1 e TS2) e ogni tablespace include due file di database (ts1_1.dbf, ts1_2.dbf, ts2_1.dbf e ts2_2.dbf).

Queste tabelle mostrano come i due tipi di backup producono un numero diverso di copie Snapshot.

SnapManager crea copie Snapshot a livello di volume invece del livello di tablespace, il che di solito riduce il numero di copie Snapshot che deve creare.



Entrambi i backup creano anche copie Snapshot dei file di log.

Volumi nel database	Tablespace TS1 (include 2 file di database)	Tablespace TS2 (include 2 file di database)	Copie Snapshot create	Numero totale di copie Snapshot
/Vol/vol	TS1_1.dbf	TS2_1.dbf	1 per volume	2

Volumi nel database	Tablespace TS1 (include 2 file di database)	Tablespace TS2 (include 2 file di database)	Copie Snapshot create	Numero totale di copie Snapshot
/Vol/vol	TS1_1.dbf	TS2_1.dbf	2 per file	4

Backup online completi

Durante un backup online completo, SnapManager esegue il backup dell'intero database e crea copie Snapshot a livello di volume (non a livello di tablespace).

SnapManager crea due copie Snapshot per ogni backup. Se tutti i file necessari al database si trovano in un singolo volume, entrambe le copie Snapshot vengono visualizzate in tale volume.

Quando si specifica un backup completo, SnapManager esegue le seguenti operazioni:

1. Consente di attivare la modalità di backup online per l'intero database
2. Crea copie Snapshot di tutti i volumi contenenti file di database
3. Consente di estrarre il database dalla modalità di backup online
4. Forza uno switch di log e quindi archivia i file di log

In questo modo, le informazioni di ripristino vengono anche svuotate sul disco.

5. Genera file di controllo del backup
6. Crea una copia Snapshot dei file di log e dei file di controllo del backup

Quando si esegue un backup completo, SnapManager attiva l'intero database in modalità di backup online. Un singolo tablespace (ad esempio /vol/vola/ts1_1.dbf) si trova in modalità di backup online più lungo di alcuni tablespace o file di dati specificati.

Quando un database entra in modalità di backup, Oracle scrive interi blocchi nei registri e non scrive semplicemente il delta tra i backup. Poiché i database funzionano di più in modalità di backup online, la scelta di un backup completo comporta un carico maggiore sull'host.

Anche se l'esecuzione di backup completi comporta un carico maggiore sull'host, i backup completi richiedono meno copie Snapshot, con conseguente riduzione dei requisiti di storage.

Backup online parziali

Invece di eseguire un backup completo, è possibile scegliere di eseguire un backup parziale degli spazi delle tabelle in un database. Mentre SnapManager esegue una copia Snapshot dei volumi per *backup completi*, SnapManager esegue una copia Snapshot di ogni spazio tabella specificato per i backup *parziali*.

Poiché il livello tablespace è il livello più basso consentito da Oracle in modalità di backup, SnapManager elabora i backup a livello di tablespace, anche se si specifica un file di dati in uno spazio di tabella.

Con un backup parziale, ogni tablespace esiste in modalità di backup per un periodo di tempo più breve rispetto a un backup completo. Durante un backup online, il database è sempre disponibile per gli utenti; tuttavia, il database deve eseguire più lavoro e l'host deve eseguire più i/o fisico. Inoltre, poiché sta prendendo copie Snapshot di ogni tablespace specificato o di ogni tablespace contenente un file di dati specificato invece dell'intero volume, SnapManager utilizza più copie Snapshot.

SnapManager esegue copie Snapshot di tablespace o file di dati specifici. L'algoritmo di backup parziale è un loop che SnapManager ripete fino a quando non ha eseguito una copia Snapshot di ogni tablespace o file di dati specificato.



Sebbene sia possibile eseguire un backup parziale, si consiglia di eseguire sempre un backup completo dell'intero database.

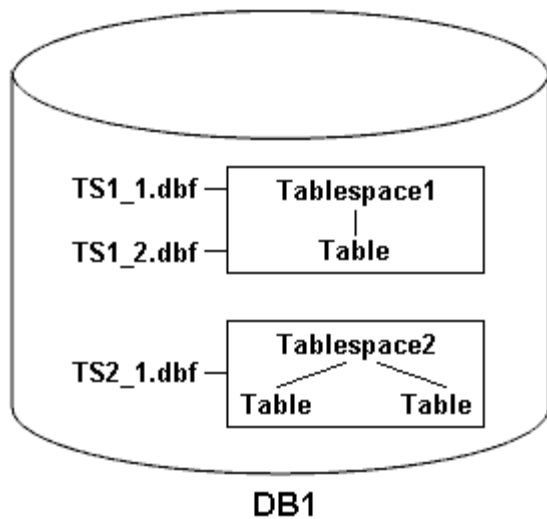
Durante un backup parziale, SnapManager esegue le seguenti azioni:

1. Posiziona lo spazio delle tabelle contenente i file di dati in modalità di backup.
2. Esegue una copia Snapshot di tutti i volumi utilizzati dallo spazio di tabella.
3. Elimina la tablespace dalla modalità di backup.
4. Continua questo processo fino a quando non viene eseguita una copia Snapshot di tutti i tablespace o file.
5. Forza uno switch di log e quindi archivia i file di log.
6. Genera file di controllo del backup.
7. Esegue una copia Snapshot dei file di log e dei file di controllo del backup.

Esempi di operazioni di backup, ripristino e ripristino

Sono disponibili informazioni su alcuni scenari di backup, ripristino e ripristino che è possibile utilizzare per raggiungere gli obiettivi di protezione dei dati.

L'illustrazione seguente mostra il contenuto dello spazio tabella:



Nell'illustrazione, Tablespace1 ha una tabella e due file di database associati. Tablespace2 dispone di due tabelle e di un file di database associato.

Le seguenti tabelle descrivono alcuni scenari completi e parziali di backup, ripristino e ripristino:

Esempi di operazioni complete di backup, ripristino e ripristino

Backup completo	Ripristinare	Ripristinare
SnapManager esegue un backup di tutto ciò che è contenuto nel database DB1, inclusi i file di dati, i log di archiviazione e i file di controllo.	Ripristino completo con file di controllo SnapManager ripristina tutti i file di dati, gli spazi delle tabelle e i file di controllo nel backup.	È possibile specificare una delle seguenti opzioni: <ul style="list-style-type: none"> • SCN - inserire un SCN, ad esempio 384641. • Data/ora - inserire una data e un'ora del backup, ad esempio 2005-11-25:19:06:22. • L'ultima transazione effettuata nel database.
Ripristino completo senza file di controllo SnapManager ripristina tutti i tablespaces e i file di dati, senza i file di controllo.	Ripristinare file di dati o tablespaces con file di controllo specificare una delle seguenti opzioni: <ul style="list-style-type: none"> • Tablespace • File di dati 	SnapManager ripristina i dati nell'ultima transazione effettuata nel database.

Esempi di operazioni parziali di backup, ripristino e ripristino

Backup parziale	Ripristinare	Ripristinare
<p>È possibile scegliere una delle seguenti opzioni:</p> <ul style="list-style-type: none"> • Tablespace <p>È possibile specificare Tablespace1 e Tablespace2 o solo uno di essi.</p> <ul style="list-style-type: none"> • File di dati <p>È possibile specificare tutti e tre i file di database (TS1_1.dbf, TS1_2.dbf e TS2_1.dbf), due o un file.</p> <p>Indipendentemente dall'opzione selezionata, il backup include tutti i file di controllo. I file di log dell'archivio sono inclusi nel backup parziale se il profilo non è abilitato a creare i backup del log dell'archivio separatamente.</p>	<p>Ripristino completo SnapManager ripristina tutti i file di dati, gli spazi delle tabelle e i file di controllo specificati nel backup parziale.</p>	<p>SnapManager ripristina i dati nell'ultima transazione eseguita nell'istanza del database.</p>
<p>Ripristino di file di dati o tablespace con file di controllo SnapManager ripristina una delle seguenti opzioni:</p> <ul style="list-style-type: none"> • Tutti i file di dati specificati • Tutti i tablespace specificati 	<p>Ripristino di file di dati o tablespace senza file di controllo SnapManager ripristina una delle seguenti opzioni:</p> <ul style="list-style-type: none"> • Tablespace <p>Specificare uno degli spazi delle tabelle. SnapManager ripristina solo gli spazi delle tabelle specificati. Se il backup contiene Tablespace1, SnapManager ripristina solo tale tablespace.</p> <ul style="list-style-type: none"> • File di dati <p>Specificare uno dei file di database. SnapManager ripristina solo i file di dati specificati. Se il backup contiene file di database (TS1_1.dbf e TS1_2.dbf), SnapManager ripristina solo questi file.</p>	<p>Ripristinare solo i file di controllo</p>

Informazioni sulla gestione del file di controllo e del file di log dell'archivio

SnapManager include i file di controllo e, facoltativamente, include i file di registro dell'archivio con ogni backup. I file di log dell'archivio vengono utilizzati per le operazioni di recovery.

Il database utilizza i file di controllo per identificare nomi, posizioni e dimensioni dei file di database. SnapManager include i file di controllo in ogni backup perché i file di controllo vengono utilizzati nel processo di ripristino.

Le modifiche apportate a un database vengono registrate utilizzando i log di ripristino online, che vengono poi archiviati e denominati log di ripristino archiviati (o log di archiviazione). SnapManager (3.2 o versioni successive) consente di eseguire il backup dei file di dati e di archiviare i file di registro separatamente con diverse frequenze e ritentimenti. SnapManager può eseguire backup solo dei registri di archiviazione o backup combinati di file di dati e registri di archiviazione. SnapManager offre una gestione automatica completa dei registri di archiviazione e non richiede alcun intervento manuale per il ripristino del database e consente inoltre di rimuovere i registri di archiviazione da una o più destinazioni dei registri di archiviazione dopo l'esecuzione del backup.



Per visualizzare gli spazi delle tabelle e i file di dati inclusi in un backup, utilizzare il comando `show di backup` o la finestra `Backup Properties`.

La seguente tabella illustra come SnapManager gestisce i file di log di archiviazione e controllo durante ciascuna operazione:

[options="header"]d

Tipo di operazione	File di controllo	Archiviare i file di log
Backup	Incluso con ogni backup	Può essere incluso con ogni backup
Ripristinare	Può essere ripristinato da solo o insieme ai tablespaces o ai file di dati	Può essere utilizzato per il processo di ripristino

Che cos'è la pianificazione del backup del database

È possibile pianificare, aggiornare e monitorare i backup dei database utilizzando la scheda `Schedule` (Pianificazione) dell'interfaccia utente grafica.

La seguente tabella affronta alcune domande comuni relative alla pianificazione:

Domanda	Risposta
Cosa accade ai backup pianificati quando il server SnapManager viene riavviato?	Quando il server SnapManager viene riavviato, riavvia automaticamente tutte le pianificazioni. Tuttavia, SnapManager non segue le occorrenze perse.

Domanda	Risposta
<p>Cosa succede quando si piangono due backup su due database contemporaneamente?</p>	<p>SnapManager avvia le operazioni di backup una alla volta e consente l'esecuzione dei backup in parallelo. Ad esempio, se un amministratore del database crea sei pianificazioni di backup giornaliere per sei profili di database diversi a 1:00, tutti e sei i backup vengono eseguiti in parallelo.</p> <p>Se si piangono più backup su un singolo profilo di database in un breve periodo di tempo, il server SnapManager esegue solo l'operazione di backup con la durata di conservazione più lunga.</p> <p>Prima di avviare un'operazione di backup, SnapManager determina quanto segue:</p> <ul style="list-style-type: none"> • Negli ultimi 30 minuti, un'altra pianificazione ha creato correttamente un backup, con una maggiore conservazione, per lo stesso profilo? • Entro i prossimi 30 minuti, un'altra pianificazione tenterà di creare un backup, con una maggiore conservazione, per lo stesso profilo? <p>Se la risposta a una delle due domande è sì, SnapManager salta il backup.</p> <p>Ad esempio, un amministratore di database potrebbe creare una pianificazione giornaliera, settimanale e mensile per un profilo di database, che viene pianificata per eseguire i backup alle 1:00. In quel giorno del mese in cui sono pianificati tre backup simultanei alle 1:00, SnapManager esegue solo l'operazione di backup in base alla pianificazione mensile.</p> <p>La finestra temporale di 30 minuti può essere modificata in un file di proprietà di SnapManager.</p>
<p>Con quale utente viene eseguita l'operazione di backup?</p>	<p>L'operazione viene eseguita sotto l'utente che ha creato la pianificazione. Tuttavia, è possibile modificare l'ID utente se si dispone di credenziali valide sia per il profilo del database che per l'host. Ad esempio, lanciando le proprietà di backup pianificato per la pianificazione di backup creata da Avida Davis, Stella Morrow può selezionare il proprio ID utente in Esegui questa operazione come utente per eseguire il backup pianificato.</p>

Domanda	Risposta
In che modo lo scheduler SnapManager interagisce con lo scheduler nativo del sistema operativo?	Sul server SnapManager, non è possibile visualizzare i backup pianificati tramite lo scheduler nativo del sistema operativo. Ad esempio, dopo aver creato un backup pianificato, non vengono visualizzate voci aggiuntive in cron.
Cosa succede se gli orologi nell'interfaccia grafica utente e nel server non sono sincronizzati?	<p>Gli orologi sul client e sul server non sono sincronizzati. Pertanto, è possibile pianificare un backup in cui l'ora di inizio sia in futuro sul client ma in passato sul server.</p> <p>Per i backup ricorrenti, il server continua a soddisfare la richiesta. Ad esempio, se il server riceve una richiesta di eseguire backup orari a partire dal 01/30/08 alle 15:00 ma l'ora attuale è alle 15:30 in quel giorno, il server esegue il primo backup alle 16:00 e continua a eseguire backup ogni ora.</p> <p>Tuttavia, per i backup una sola volta, il server gestisce la richiesta nel modo seguente:</p> <ul style="list-style-type: none"> • Se l'ora di inizio è compresa entro gli ultimi cinque minuti dall'ora corrente del server, SnapManager avvia immediatamente il backup. • Se l'ora di inizio è superiore a cinque minuti, SnapManager non avvia il backup. <p>Ad esempio, considerare il seguente scenario:</p> <ul style="list-style-type: none"> • L'orologio nell'host dell'interfaccia grafica è indietro di tre minuti rispetto all'ora effettiva. • L'ora corrente sul client è alle 8:58 • È possibile pianificare un backup una tantum alle 9:00 • È possibile pianificare un altro backup una tantum alle 8:30 <p>Quando il server riceve la prima richiesta, l'ora sul server è 9:01. Sebbene l'ora di inizio del backup sia passata, SnapManager esegue immediatamente il backup.</p> <p>Quando il server riceve la seconda richiesta, l'ora di inizio del backup è superiore a cinque minuti. Viene visualizzato un messaggio che indica che la richiesta di pianificazione non è riuscita perché l'ora di inizio è passata.</p> <p>È possibile modificare l'intervallo di cinque minuti in un file di proprietà di SnapManager.</p>

Domanda	Risposta
Cosa accade ai backup pianificati per un profilo quando questo viene cancellato?	Quando viene eliminato un profilo di database, il server SnapManager elimina i backup pianificati definiti per tale profilo.
Come si comportano i backup pianificati durante l'ora legale o quando si modifica l'ora del server SnapManager?	<p>Le pianificazioni dei backup di SnapManager vengono influenzate a causa dell'ora legale o quando si modifica l'ora del server SnapManager.</p> <p>Considerare le seguenti implicazioni in caso di modifica dell'ora del server SnapManager:</p> <ul style="list-style-type: none"> • Una volta attivata la pianificazione del backup, se l'ora del server SnapManager diminuisce, la pianificazione del backup non si attiva di nuovo. • Se l'ora legale inizia prima dell'ora di inizio pianificata, le pianificazioni di backup vengono attivate automaticamente. • Ad esempio, se ci si trova negli Stati Uniti e si pianificano backup orari alle 4:00 che dovrebbe avvenire ogni 4 ore, i backup si verificheranno alle 4:00, 8:00, 12:00, 4:00, 20:00, E mezzanotte nei giorni precedenti e successivi alle modifiche dell'ora legale di marzo e novembre. • Tenere presente quanto segue se i backup sono pianificati per le 2:30 ogni notte: <ul style="list-style-type: none"> ◦ Quando i clock tornano indietro di un'ora, poiché il backup è già attivato, il backup non si attiva di nuovo. ◦ Quando i clock vengono attivati in avanti di un'ora, il backup viene attivato immediatamente. Se ci si trova negli Stati Uniti e si desidera evitare questo problema, è necessario pianificare l'avvio dei backup al di fuori delle 2:00 alle 3:00 intervallo.

Creazione di backup del database

È possibile creare backup di interi database o porzioni di database, inclusi tablespaces, file di dati o file di controllo.

SnapManager offre funzionalità di copia Snapshot per i database in molti stack di storage lato host, tra cui NFS, ASM, Veritas e altri.



Per le configurazioni RAC (Real Application Clusters), SnapManager esegue il backup sul lato host nel profilo.

Gli amministratori possono facoltativamente registrare i backup con Oracle RMAN, che facilita l'utilizzo di RMAN per ripristinare e ripristinare il database con granularità più fini come i blocchi.

Durante la definizione del profilo, è possibile personalizzare i nomi delle copie Snapshot create dai backup di tale profilo. Ad esempio, è possibile inserire una stringa di prefissi DI SALT per indicare i backup High Operations.

Oltre a definire nomi univoci per le copie Snapshot create dai backup, è possibile creare etichette univoche per i backup stessi. Quando si crea un backup, è consigliabile fornire un nome per il backup in modo da poter identificare facilmente il backup utilizzando il parametro `-label`. Questo nome deve essere univoco per tutti i backup creati all'interno di un profilo specifico. Il nome può contenere lettere, numeri, caratteri di sottolineatura (`_`) e trattini (`-`). Non può iniziare con un trattino. Le etichette sono sensibili al maiuscolo/minuscolo. È possibile aggiungere informazioni quali variabili di ambiente del sistema operativo, data del sistema e tipo di backup.

Se non si fornisce un'etichetta, SnapManager crea un nome di etichetta predefinito nel formato `scope_mode_datestring`, dove `scope` è completo o parziale e `mode` è offline, online o automatico (la lettera `c` per cold, `h` per hot o `a` per automatic).

Da SnapManager 3.4, è possibile fornire una propria etichetta di backup sovrascrivendo l'etichetta di backup predefinita creata da SnapManager. Impostare il valore del parametro `override.default.backup.pattern` su `true` e specificare la nuova etichetta di backup nel parametro `new.default.backup.pattern`. Il modello di etichetta di backup può contenere parole chiave come nome del database, nome del profilo, ambito, modalità e nome host, che devono essere separate da un carattere di sottolineatura. Ad esempio, `new.default.backup.pattern=dbname_profile_hostname_scope_mode`.



Il timestamp verrà incluso automaticamente alla fine dell'etichetta generata.

Quando si inserisce un commento, è possibile includere spazi e caratteri speciali. Al contrario, quando si inserisce un'etichetta, non includere spazi o caratteri speciali.

Per ogni backup, SnapManager genera automaticamente un GUID, che è una stringa ESADECIMALE di 32 caratteri. Per determinare il GUID, eseguire il comando `backup list` con l'opzione `-verbose`.

È possibile creare un backup completo di un database mentre è online o offline. Per consentire a SnapManager di gestire il backup di un database indipendentemente dal fatto che sia online o offline, utilizzare l'opzione `-auto`.

Durante la creazione di un backup, se è stata attivata la funzione di eliminazione e la notifica di riepilogo è stata attivata nel profilo, vengono attivate due e-mail separate. Un'e-mail è per l'operazione di backup e l'altra per la potatura. È possibile correlare questi messaggi di posta elettronica confrontando il nome del backup e l'ID di backup contenuti in questi messaggi di posta elettronica.

È possibile creare un backup a freddo quando il database si trova nello stato di arresto. Se il database si trova in uno stato montato, impostarlo su shutdown ed eseguire il backup offline (cold backup).

SnapManager (3.2 o versione successiva) consente di eseguire il backup dei file di log dell'archivio separatamente dai file di dati, consentendo di gestire i file di log dell'archivio in modo efficiente.

Per creare separatamente i backup del registro di archiviazione, è necessario creare un nuovo profilo o aggiornare il profilo esistente per separare i backup del registro di archiviazione utilizzando l'opzione `-separate-archiviavelog-backups`. Utilizzando il profilo, è possibile eseguire le seguenti operazioni SnapManager:

- Creare un backup del registro di archiviazione.
- Eliminare un backup del registro di archiviazione.
- Montare un backup del registro di archiviazione.
- Liberare un backup del registro di archiviazione.

Le opzioni di backup variano a seconda delle impostazioni del profilo:

- L'utilizzo di un profilo non separato per eseguire separatamente i backup del registro di archiviazione consente di eseguire le seguenti operazioni:
 - Creare un backup completo.
 - Creare un backup parziale.
 - Specificare le destinazioni del registro di archiviazione di cui eseguire il backup per i file di registro di archiviazione.
 - Specificare le destinazioni del registro di archiviazione da escludere dal backup.
 - Specificare le opzioni di eliminazione per eliminare i file di log dell'archivio dalle destinazioni del log dell'archivio.
- L'utilizzo di un profilo separato per eseguire i backup del registro di archiviazione consente di effettuare le seguenti operazioni:
 - Creare un backup dei soli file di dati.
 - Creare un backup solo per l'archiviazione.
 - Durante la creazione di un backup dei soli file di dati, includere il backup del registro di archiviazione insieme al backup dei soli file di dati online per la clonazione.

Se sono stati inclusi i backup del registro di archiviazione insieme ai file di dati nella pagina **Impostazioni profilo** della procedura guidata **creazione profilo** dall'interfaccia grafica di SnapManager, inoltre, se non è stata selezionata l'opzione **Archivelog** nella procedura guidata **creazione backup**, SnapManager crea sempre il backup del registro di archiviazione insieme ai file di dati per tutti i backup online.

In tale situazione, dalla CLI di SnapManager, è possibile prendere in considerazione tutte le destinazioni del registro di archiviazione per il backup, ad eccezione delle destinazioni di esclusione specificate nel file di configurazione di SnapManager. Tuttavia, non è possibile eseguire l'eliminazione di questi file di log dell'archivio. Tuttavia, è ancora possibile utilizzare l'opzione `-archivelogs` per specificare la destinazione del file di log dell'archivio e per potare i file di log dell'archivio dalla CLI di SnapManager.

Se si sta creando il backup utilizzando l'opzione `-auto` e si specifica l'opzione `--archivelogs`, SnapManager crea un backup online o offline in base allo stato corrente del backup.

- SnapManager crea un backup offline quando il database non è in linea e non include i file di log dell'archivio nel backup.
- SnapManager crea un backup online che include i file di log dell'archivio quando il database è online.
- Durante la creazione del backup solo per l'archiviazione:
 - Specificare la destinazione del log di archiviazione di cui eseguire il backup insieme al backup solo archiviando
 - Specificare le destinazioni del registro di archiviazione da escludere dal backup solo dei registri di archiviazione
 - Specificare le opzioni di eliminazione per eliminare i file di log dell'archivio dalle destinazioni del log dell'archivio
- **Scenari non supportati**
 - Non è possibile creare il backup solo archivioinsieme a un backup solo file di dati offline.

- Non è possibile eseguire l'eliminazione dei file di log dell'archivio quando non viene eseguito il backup dei file di log dell'archivio.
- 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`.

Quando si specifica l'etichetta per il backup dei file di dati online con il backup del registro di archiviazione incluso, l'etichetta viene applicata per il backup dei file di dati e il backup del registro di archiviazione viene contrassegnato con il suffisso (`_logs`). Questo suffisso può essere configurato modificando il parametro `suffix.backup.label.with.logs` nel file di configurazione SnapManager.

Ad esempio, è possibile specificare il valore come `suffix.backup.label.with.logs=Arc` in modo che il valore predefinito `_logs` venga modificato in `_arc`.

Se non sono state specificate destinazioni del registro di archiviazione da includere nel backup, SnapManager include tutte le destinazioni del registro di archiviazione configurate nel database.

Se in una delle destinazioni mancano file di log di archiviazione, SnapManager ignora tutti i file di log di archiviazione creati prima dei file di log di archiviazione mancanti, anche se questi file sono disponibili in un'altra destinazione di log di archiviazione.

Durante la creazione dei backup del registro di archiviazione, è necessario specificare le destinazioni del file di registro di archiviazione da includere nel backup e impostare il parametro di configurazione in modo che i file di registro di archiviazione vengano inclusi sempre oltre i file mancanti nel backup.



Per impostazione predefinita, questo parametro di configurazione è impostato su `true` per includere tutti i file di log dell'archivio, oltre ai file mancanti. Se si utilizzano script di eliminazione dei log di archiviazione o si eliminano manualmente i file di log di archiviazione dalle destinazioni dei log di archiviazione, è possibile disattivare questo parametro, in modo che SnapManager possa ignorare i file di log di archiviazione e procedere ulteriormente con il backup.

SnapManager non supporta le seguenti operazioni SnapManager per i backup dei log di archiviazione:

- Clonare il backup del log di archiviazione
- Ripristinare il backup del registro di archiviazione
- Verificare il backup del registro di archiviazione

SnapManager supporta anche il backup dei file di log dell'archivio dalle destinazioni dell'area di ripristino flash.

1. Immettere il seguente comando: `smo backup create -profile_name {[full {online | offline | auto} [-retain {hourly | daily | settimanale | mensile | illimitato}] [-verify] | [-data [[filesfiles [files]] | [-tablespaces-tablespaces [-tablespaces] [-datalabellabellabel] {-}online | -verify-{sharly | untary [-]untary] | --untary [--untary] | -sharly -untary [---untary] | -untary [-untary] [-snapvaultlabelSnapVault_label][Protect | -noprotect | -protectnow] [-backup-destpath1 [,path2]] [-exclude-destpath1 [,path2]] [-prunelogs {-all | -untilSCNuntilSCN | -date yyyy-MM-dd:HH:mm:mm:--spune_praskspune | -}}-spuns | -spuna1-spunadeph] -}-spunadepune | -spuns | -spuns] -spunadepuns | -spuns | --spuns-spuns | -`

Se si desidera...	Quindi...
Creare un backup sullo storage secondario utilizzando la policy di protezione <i>SnapManager_cDOT_Vault</i>	Specificare -snapvaultlabel. È necessario fornire l'etichetta SnapMirror specificata nelle regole del criterio SnapMirror durante l'impostazione della relazione SnapVault come valore.
Specificare se si desidera eseguire un backup di un database online o offline, invece di consentire a SnapManager di gestire se è online o offline	Specificare -offline per eseguire un backup del database offline. Specificare -online per eseguire un backup del database online. + se si utilizzano queste opzioni, non è possibile utilizzare l'opzione -auto.
Specificare se si desidera consentire a SnapManager di eseguire il backup di un database indipendentemente dal fatto che sia online o offline	Specificare l'opzione -auto. Se si utilizza questa opzione, non è possibile utilizzare l'opzione --offline o -online.
Specificare se si desidera eseguire un backup parziale di file specifici	<div>Specify the -data-files option and then list the files, separated by commas. For example, list the file names f1, f2, and f3 after the option. + esempio per la creazione di un backup parziale dei file di dati su UNIX</div> <div>+</div> <div> <pre>smo backup create -profile nosepp -data -files /user/user.dbf -online -label partial_datafile_backup -verbose</pre> </div>

Se si desidera...	Quindi...
<p>Specificare se si desidera eseguire un backup parziale di spazi tabella specifici</p>	<div data-bbox="867 184 1461 747"> <p>Specify the <code>-data-tablespaces</code> option and then list the tablespaces, separated by commas. For example, use <code>ts1</code>, <code>ts2</code>, and <code>ts3</code> after the option.</p> <p>+ SnapManager supporta il backup degli spazi delle tabelle di sola lettura. Durante la creazione del backup, SnapManager modifica gli spazi delle tabelle di sola lettura in lettura/scrittura. Dopo aver creato il backup, gli spazi delle tabelle vengono modificati in sola lettura.</p> </div> <p>+ esempio per la creazione di un backup tablespace parziale</p> <p>+</p> <div data-bbox="867 1010 1455 1165"> <pre> smo backup create -profile nosepl -data -tablespaces tb2 -online -label partial_tablespace_bkup -verbose </pre> </div>
<p>Specificare se si desidera creare un'etichetta univoca per ciascun backup nel seguente formato: Full_hot_mybackup_label</p>	<div data-bbox="867 1270 1417 1350"> <p>For Linux, you might enter this example:</p> </div> <p>+</p> <div data-bbox="867 1514 1455 1665"> <pre> smo backup create -profile targetdbl_prof1 -label full_hot_my_backup_label -online -full -verbose </pre> </div>

Se si desidera...	Quindi...
<p>Specificare se si desidera creare il backup dei file di log dell'archivio separatamente dai file di dati</p>	<div data-bbox="844 157 1484 982" style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>Specify the following options and variables:</p> <p>** -archivelogs crea un backup dei file di log dell'archivio.</p> <p>** -backup-dest specifica le destinazioni del file di log di archiviazione di cui eseguire il backup.</p> <p>** -exclude-dest specifica le destinazioni del registro di archiviazione da escludere.</p> <p>** -label specifica l'etichetta per il backup del file di log dell'archivio.</p> <p>** -protect consente di proteggere i backup dei log di archiviazione. *Nota:* è necessario specificare l'opzione -backup-dest o -exclude-dest.</p> </div> <p>+ Fornendo entrambe queste opzioni insieme al backup, viene visualizzato un messaggio di errore che indica che è stata specificata un'opzione di backup non valida. Specificare una qualsiasi delle opzioni: -Backup-dest o exclude-dest.</p> <p>+ Esempio per la creazione di backup del file di log dell'archivio separatamente su UNIX</p> <p>+</p> <div data-bbox="844 1381 1484 1606" style="border: 1px solid #ccc; padding: 10px;"> <pre>smo backup create -profile nose p -archivelogs -backup-dest /mnt/archive_dest_2/ -label archivelog_bkup -verbose</pre> </div>

Se si desidera...	Quindi...
<p>Specificare se si desidera creare insieme il backup dei file di dati e dei file di log di archiviazione</p>	<div data-bbox="844 157 1484 577"> <p>Specify the following options and variables:</p> <p>** opzione <code>-data</code> per specificare i file di dati.</p> <p>** <code>-archivelogs</code> per specificare i file di log dell'archivio.</p> <p>Esempio di backup dei file di dati e di archiviazione dei file di log insieme su UNIX</p> </div> <p data-bbox="844 609 860 640">+</p> <div data-bbox="844 672 1484 945"> <pre>smo backup create -profile nosepl -data -online -archivelogs -backup-dest mnt/archive_dest_2 -label data_arch_backup -verbose</pre> </div>

Se si desidera...	Quindi...
<p>Specificare se si desidera eseguire la sregolazione dei file di log dell'archivio durante la creazione di un backup</p>	<div data-bbox="844 159 1481 457"> <p>Specify the following options and variables:</p> <p>** -prunelogs specifica di eliminare i file di log dell'archivio dalle destinazioni del log dell'archivio.</p> </div> <p>+ * -all specifica di eliminare tutti i file di log dell'archivio dalle destinazioni del log dell'archivio. * -Until-scnuntil-scn specifica di eliminare i file di log dell'archivio fino a quando non viene specificato un SCN. * -Until-dateyyyy-MM-dd:HH:mm:ss specifica di eliminare i file di log dell'archivio fino al periodo di tempo specificato. * l'opzione before consente di eliminare i file di log dell'archivio prima del periodo di tempo specificato (giorni, mesi, settimane, ore). * -prune-destprune_dest1,[prune_dest2 specifica di eliminare i file di log dell'archivio dalle destinazioni del log dell'archivio durante la creazione del backup. Nota: quando Flash Recovery Area (fra) è abilitata per i file di log dell'archivio, non è possibile eseguire la sunizzazione dei file di log dell'archivio.</p> <p>+ Esempio di eliminazione di tutti i file di log dell'archivio durante la creazione di un backup su UNIX</p> <p>+</p> <p>+</p> <p>+</p> <div data-bbox="844 1402 1481 1701"> <pre>smo backup create -profile nosepl -archivelogs -label archive_prunebackup1 -backup-dest /mnt/arc_1,/mnt/arc_2 -prunelogs -all -prune-dest /mnt/arc_1,/mnt/arc_2 -verbose</pre> </div>
<p>Specificare se si desidera aggiungere un commento sul backup</p>	<p>Specificare -comment seguito dalla stringa di descrizione.</p>

Se si desidera...	Quindi...
Specificare se si desidera forzare il database nello stato specificato per il backup, indipendentemente dallo stato in cui si trova attualmente	Specificare l'opzione -force.
Specificare se si desidera verificare il backup contemporaneamente alla creazione	Specificare l'opzione -verify.
Specificare se si desidera raccogliere i file dump dopo l'operazione di backup del database	Specificare l'opzione -dump alla fine del comando di backup create.

Esempio

```
smo backup create -profile targetdb1_prof1 -full -online -force -verify
```

Informazioni correlate

[Naming delle copie Snapshot](#)

[Creazione di script di pre-task, post-task e policy](#)

[Creazione di script di attività](#)

[Memorizzazione degli script delle operazioni](#)

[Il comando smo backup create](#)

[Protezione dei backup dei database su storage secondario o terzo](#)

Eliminazione dei file di log dell'archivio

Durante la creazione di un backup, è possibile eseguire l'eliminazione dei file di log dell'archivio dalle posizioni di log dell'archivio.

- Il backup dei file di log dell'archivio deve essere eseguito con l'operazione di backup corrente.

Se si specifica l'eliminazione insieme ad altri backup che non contengono file di log dell'archivio, i file di log dell'archivio non vengono eliminati.

- Il database deve essere in stato montato.

Se il database non si trova nello stato montato, immettere l'opzione -force insieme al comando backup.

Durante l'esecuzione di un'operazione di backup, è possibile specificare quanto segue:

- Scopo della potatura:
 - Eliminare tutti i file di log dell'archivio.

- Eliminare i file di registro dell'archivio fino al numero di modifica del sistema (SCN) specificato.
- Eliminare i file di log dell'archivio fino all'ora specificata.
- Eliminare i file di log dell'archivio prima del periodo di tempo specificato.
- Destinazione da cui è necessario rimuovere i file di log dell'archivio.



Anche quando l'eliminazione del file di log dell'archivio non riesce in una destinazione, SnapManager continua a rimuovere i file di log dell'archivio dalle altre destinazioni.

Prima di eliminare i file di log dell'archivio, SnapManager verifica quanto segue:

- Il backup dei file di log dell'archivio viene eseguito almeno una volta.
- I file di log dell'archivio vengono inviati al database Oracle DataGuard Standby, se presente.
- I file di log dell'archivio vengono acquisiti dal processo di acquisizione di Oracle Streams, se presente.

Se il backup dei file di log dell'archivio viene eseguito, inviato in standby e acquisito dal processo di acquisizione, SnapManager elimina tutti i file di log dell'archivio in una singola esecuzione. Tuttavia, se sono presenti file di log di archiviazione che non vengono sottoposti a backup, non vengono inviati in standby o non vengono acquisiti dal processo di acquisizione, SnapManager elimina i file di log di archiviazione uno per uno. L'eliminazione dei file di log dell'archivio in una singola esecuzione è più rapida rispetto all'eliminazione dei log dell'archivio uno per uno.

SnapManager può anche raggruppare i file di log dell'archivio ed eliminarli batch per batch. Ogni batch avrà un massimo di 998 file. Questo valore può essere configurato al di sotto di 998 utilizzando il parametro di configurazione `maximum.archive.log.files.toprune.atatime` nel file `smo.config`.

SnapManager utilizza i comandi di gestione ripristino Oracle per eliminare i file di log dell'archivio. Tuttavia, SnapManager non si integra con i criteri di conservazione e di eliminazione di RMAN.



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 non supporta l'eliminazione dei file di log dell'archivio nei seguenti scenari:

- I file di log dell'archivio si trovano nell'area di ripristino della flash.
- I file di log dell'archivio si trovano nel database Standby.
- I file di log dell'archivio sono gestiti da SnapManager e RMAN.
 - Immettere il seguente comando: `smo backup create -profile_name {[full {online | offline | auto} [-retain {hourly | [-daily | -settimanale | -mensile | -illimitato]} [-verify] | [-data [-filesfiles [files]] | [-tablespaces-tablespaces-tablespaces] [-datalabellabellabel] -settimanale | -{-}-online | -verify [-sharly] -verify [-sharly] | -sharly] -sharly | -sharing [--untary | -sharly] -sharly | --untary [- [-protect | -noprotect | -protectnow] [-backup-destpath1 [,path2]]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all | -untilSCNuntilSCN | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-mese | -giorni | -spacune_}}-spacune [-spacune] -}-spacune] -spacune-spacune [-spacune] --spacune] --spacune] -spaces] -spacune [-]`

Se si desidera...	Quindi...
File di log dell'archivio di Prune	<p>Specificare le seguenti opzioni:</p> <ul style="list-style-type: none"> • -prunelogs specifica l'eliminazione dei file di log dell'archivio durante la creazione di un backup. <ul style="list-style-type: none"> ◦ -all specifica l'eliminazione di tutti i file di log dell'archivio. ◦ -UntilSCN specifica l'eliminazione dei file di log dell'archivio fino al numero SCN specificato. ◦ -until-date specifica l'eliminazione dei log di archiviazione, inclusi data e ora specificate. ◦ -prima di {-mesi
-giorni	-settimane
-hours} specifica l'eliminazione dei file di log dell'archivio prima del periodo di tempo specificato.	Includere la destinazione da cui devono essere eliminati i file di log dell'archivio

Consolidamento dei backup dei log di archiviazione

SnapManager consolida i backup di solo archiviatore ogni volta che si esegue un backup liberando i backup duplicati di solo archiviatore. Per impostazione predefinita, il consolidamento è attivato.

SnapManager identifica i backup di solo archivio con file di log di archivio in altri backup e li libera di mantenere un numero minimo di backup di solo archivio con file di log di archivio univoci.

Se i backup di solo archivio vengono liberati dal consolidamento, questi vengono cancellati in base alla durata di conservazione del registro di archiviazione.

Quando il database si trova nello stato shutdown o nomount durante il consolidamento del log di archiviazione, SnapManager cambia il database nello stato mount.

Se il backup o l'eliminazione dei file di log dell'archivio non riesce, il consolidamento non viene eseguito. Il consolidamento dei backup di solo archiviatore viene seguito solo dopo aver eseguito correttamente i backup e le operazioni di eliminazione.

1. Per consentire il consolidamento dei backup di solo archiviazione, modificare il consolidamento dei parametri di configurazione e impostare il valore true nel file di configurazione SnapManager (smo.config).

Una volta impostato il parametro, vengono consolidati i backup di solo archivio.

Se il backup di sola archiviazione appena creato contiene gli stessi file di log dell'archivio in uno qualsiasi dei backup di sola archiviazione precedenti, i backup solo del log dell'archivio precedente vengono liberati.



SnapManager non consolida il backup del registro di archiviazione insieme al backup dei file di dati. SnapManager consolida il backup solo per l'archiviazione.



SnapManager consolida i backup del log di archiviazione anche quando l'utente elimina manualmente i file di log di archiviazione dalle destinazioni del log di archiviazione o quando i file di log di archiviazione sono corrotti e potrebbero essere inclusi nel backup.

2. Per disattivare il consolidamento dei backup del log di archiviazione, modificare il consolidamento dei parametri di configurazione e impostare il valore su false nel file di configurazione SnapManager (smo.config).

Pianificazione eliminazione file log archivio

Quando si crea un backup, è possibile pianificare l'eliminazione dei file di log dell'archivio in un momento specifico.

SnapManager consente di modificare periodicamente i file di log dell'archivio dal file system attivo.

1. Immettere il seguente comando: `smo schedule create -profile profile_name {[-full {-online | -offline | -auto}][-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]] | [-data [-filesfiles [files]] | [-tablespaces-tablespaces [-tablespaces]] {-online | -offline | -auto}][-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]] | [-archivelogs]} [-commentcomment] [-protect | -protectnow | -noprotect] [-backup-destpath1 [,path2]] [-exclude-destpath1 [,path2]] [-prunelogs{-all | -untilSCNuntilSCN | -before {-dateyyyy-MM-dd HH:mm:ss | -monthsmonths | -weeksweeks | -daysdays | -hourshours}} -prune-destprune_dest1,,prune_dest2] -schedule -nameschedule_name [-schedule-commentschedule_comment] -interval {-hourly | -daily | -weekly | -monthly | -onetimeonly} -cronstringcronstring-start-time {start-timestart_time <yyyy-MM-dd HH:mm>} -runasuser-runasuser [-force] [-quiet | -verbose]`

Se si desidera...	Quindi...
Schedule pruning dei file di log di archivio	<p>Specificare le seguenti opzioni:</p> <ul style="list-style-type: none"> • -prunelogs per pianificare l'eliminazione dei file di log dell'archivio • -prune-dest per la eliminazione dei file di log dell'archivio dalle destinazioni del log dell'archivio
Includere un nome per la pianificazione	Specificare l'opzione -schedule-name.

Se si desidera...	Quindi...
Schedule pruning dei file di log di archivio a intervalli di tempo specifici	<p>Specificare l'opzione Interval (intervallo) e indicare se i file di log dell'archivio devono essere eliminati in base alle seguenti classi di intervalli:</p> <ul style="list-style-type: none"> • orario • giornaliero • settimanale • mensile • -onetimeonly
Aggiungere un commento sull'operazione di pianificazione	Specificare l'opzione -schedule-comment seguita dalla stringa di descrizione.
Specificare l'ora di inizio dell'operazione di pianificazione	Specificare l'opzione -start-time nel formato yyyy-mm-gg hh:mm.

Protezione dei backup dei log di archiviazione

Durante la creazione dei profili, è possibile attivare la protezione per i backup del registro di archiviazione in base ai criteri di protezione del registro di archiviazione.

1. Immettere il seguente comando: `smo profile create -profileprofile [-profile-passwordprofile_password] -repository-dbnamerepo_dbname-hostrepo_host -portrepo_port-login-usernamerepo_username-database-dbnamedb_dbname -hostdb_host [-siddb_sid] [-login-usernamepdb_username-passwordddb_password-portdb_port] [-rman {-controlfile | {-login-username rman_username-passwordrman_password-tnsnamerman_tnsname} }] -osaccountosaccount -osgrouposgroup [-retain [-hourly [-countn] [-durationm]] [-daily [-countn] [-durationm]] [-weekly [-countn] [-durationm]] [-monthly [-countn] [-durationm]]] [-commentcomment][-snapname-patternpattern][-protect [-protection-policypolicy_name]] [-summary-notification] [-notification [-success-emailemail_address1, email_address2-subjectsubject_pattern] [-failure-emailemail_address1, email_address2-subjectsubject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hourshours | -daysdays | -weeksweeks | -monthsmonths [-protect [-protection-policypolicy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]`

Se...	Quindi...
Si desidera eseguire il backup dei backup dei log di archiviazione separatamente e proteggere i file di log di archiviazione	<p>Specificare le seguenti opzioni:</p> <ul style="list-style-type: none"> • -separate-archivelog-backups consente di separare i file di log dell'archivio dai file di dati. • -protect assegna una policy di protezione separata per i backup del log di archiviazione del log. • -protection-policy assegna il criterio di protezione per i backup del log di archiviazione.

Che cos'è AutoSupport

La funzione AutoSupport consente al server SnapManager di inviare messaggi AutoSupport al sistema di storage al termine dell'operazione di backup.



SnapManager invia messaggi AutoSupport solo per le operazioni di backup riuscite.

È possibile attivare o disattivare AutoSupport assegnando i seguenti valori al parametro di configurazione `auto_support.ON` nel file di configurazione `smo.config`:

- TRUE - attiva AutoSupport
- FALSE - Disabilita AutoSupport



Per impostazione predefinita, AutoSupport è attivato in SnapManager.

Informazioni correlate

[Aggiunta di sistemi storage che operano in Clustered Data ONTAP all'host del server SnapManager](#)

[Abilitazione di AutoSupport in SnapManager](#)

[Disattivazione di AutoSupport in SnapManager](#)

Aggiunta di sistemi storage che operano in Clustered Data ONTAP all'host del server SnapManager

Per abilitare AutoSupport, è necessario aggiungere i sistemi storage che operano in Clustered Data ONTAP all'host del server SnapManager. In SnapManager 3.3 e versioni precedenti, AutoSupport era supportato solo sui sistemi storage che operavano in 7-Mode.

1. Aggiungere sistemi storage che operano in Clustered Data ONTAP all'host del server SnapManager.

Se...	Quindi eseguire il seguente comando...
La macchina virtuale per lo storage di amministrazione (SVM, precedentemente nota come Vserver) opera in Clustered Data ONTAP	set di configurazione SnapDrive -cserver nome_utente
SVM opera in Clustered Data ONTAP	set di configurazione SnapDrive -nome_utente_vserver

Abilitazione di AutoSupport in SnapManager

È necessario abilitare AutoSupport, in modo che i sistemi storage ricevano messaggi dal server SnapManager per ogni operazione di backup riuscita.

AutoSupport può essere attivato in due modi:

- Per impostazione predefinita, la nuova installazione di SnapManager non contiene il parametro `auto_support.ON` nel file di configurazione `smo.config`. Ciò significa che AutoSupport è attivato.
- È possibile configurare manualmente il parametro `auto_support.on`.
 - a. Arrestare il server SnapManager.
 - b. Nel file di configurazione `smo.config`, impostare il valore del parametro `auto_support.on` su `TRUE`.


```
auto_support.on=TRUE
```
 - c. Riavviare il server SnapManager.

Disattivazione di AutoSupport in SnapManager

È necessario disattivare AutoSupport se non si desidera che il sistema di storage riceva messaggi dal server SnapManager per ogni operazione di backup eseguita correttamente.

Per impostazione predefinita, AutoSupport è attivato se il file di configurazione non contiene il parametro `auto_support.on`. In questo scenario, è necessario aggiungere il parametro `auto_support.on` nel file di configurazione e impostare il valore su `FALSE`.

1. Arrestare il server SnapManager.
2. Nel file di configurazione `smo.config`, impostare IL valore del parametro `auto_support.on` su `FALSE`.

```
auto_support.on=FALSE
```

3. Riavviare il server SnapManager.

Verifica dei backup del database

È possibile utilizzare il comando di verifica del backup per verificare che i blocchi nel backup del database non siano corrotti. L'operazione di verifica richiama l'utilità Oracle Database Verify per ogni file di dati nel backup.

SnapManager consente di eseguire l'operazione di verifica in qualsiasi momento utile per l'utente e per gli utenti del sistema. È possibile eseguire la verifica subito dopo aver creato il backup. Specificare il profilo contenente il backup e l'etichetta o l'ID del backup creato.



È possibile specificare `-dump` per raccogliere i file dump dopo l'operazione di verifica del backup.

1. Immettere il seguente comando: `smo backup verify -profile profile_name [-label label | -idid] [-force] [-dump] [-quiet | -verbose]`

Informazioni correlate

[Il comando di verifica del backup smo](#)

Modifica del criterio di conservazione del backup

È possibile modificare le proprietà di un backup in modo che sia idoneo o non idoneo per l'eliminazione in base ai criteri di conservazione.

Quando si crea un backup, è possibile impostarne i criteri di conservazione. In un secondo momento, è possibile scegliere di conservare il backup per un periodo di tempo superiore a quello consentito dal criterio di conservazione oppure specificare che il backup non è più necessario e che il criterio di conservazione lo gestisca.

Informazioni correlate

[Il comando `smo backup update`](#)

Conservazione dei backup per sempre

È possibile specificare che un backup non deve essere idoneo per l'eliminazione da parte del criterio di conservazione per mantenere il backup a tempo indeterminato.

1. Per specificare che un backup deve essere conservato senza limiti, immettere questo comando: `smo backup update -profileprofile_name {-labellabel [data | -archivelogs] | -idid} -retain -unlimited`

Informazioni correlate

[Il comando `smo backup update`](#)

Assegnazione di backup con una classe di conservazione specifica

I DBA possono assegnare ai backup una classe di conservazione specifica di ogni ora, giornaliera, settimanale o mensile. L'assegnazione di una classe di conservazione specifica rende idonei all'eliminazione i backup eseguiti in base a questa modifica.

1. Per assegnare una classe di conservazione del backup specifica, immettere questo comando: `smo backup update -profileprofile_name {-labellabel [data | -archivefacts] | -idid | All} -retain [-hourly | -daily | -settimanale | -mensile]`

Modifica del comportamento predefinito del criterio di conservazione

Quando un backup scade in base al criterio di conservazione, SnapManager determina se eliminare il backup in base alle impostazioni di conservazione. L'eliminazione dei backup è il comportamento predefinito. È possibile modificare questo comportamento predefinito e scegliere di liberare i backup non protetti.

Per impostazione predefinita, SnapManager elimina o libera i backup a seconda che siano protetti o meno come segue:

- Per i backup protetti, SnapManager libera i backup locali quando scadono.
- Per i backup non protetti, SnapManager elimina i backup locali alla scadenza.

È possibile modificare questo comportamento predefinito.

Per i backup protetti, SnapManager non prende in considerazione quanto segue per determinare se eliminare la copia locale:

- Il backup sullo storage secondario non è riuscito o è in corso la protezione.

Ciò consente il trasferimento dei backup sullo storage secondario prima dell'applicazione del criterio di conservazione.

- La copia è stata successivamente eliminata dallo storage secondario.

a. Accedere alla seguente posizione predefinita:

percorso/proprietà di installazione smo predefinito/smo.config

b. Modificare il file smo.config.

c. Impostare la proprietà `Retain.alwaysFreeExpiredBackups` nel file smo.config su `true`.

Ad esempio, `Retain.alwaysFreeExpiredBackups = true`

Informazioni correlate

[Il comando `smo backup update`](#)

Liberare o eliminare i backup esenti dai criteri di conservazione

I backup con la classe di conservazione "illimitata" non possono essere cancellati o liberati direttamente. Per eliminare o liberare questi backup, è necessario prima assegnare un'altra classe di conservazione, ad esempio oraria, giornaliera, settimanale o mensile. Per eliminare o liberare un backup esente dal criterio di conservazione, è necessario prima aggiornare il backup per renderlo idoneo per l'eliminazione o liberarlo.

1. Per aggiornare il backup in modo che sia idoneo per l'eliminazione in base al criterio di conservazione, immettere il seguente comando: `smo backup update -profileprofile_name {-labellabel [data | -archivelogs] | -idid} -retain [-hourly | -daily | -weekly | -monthly]`
2. Dopo aver aggiornato il backup in modo che sia idoneo per l'eliminazione, è possibile eliminare il backup o liberare le risorse di backup.

- Per eliminare il backup, immettere il seguente comando: `smo backup delete -profileprofile_name {-labellabel [data | -archivelogs] | -idid | -all}`
- Per liberare le risorse di backup, invece di eliminare il backup, immettere questo comando: `smo backup free -profileprofile_name {-labellabel [data | -archivelogs] | -idid | -all} [-force] [-dump] [-quiet | -verbose]`

Informazioni correlate

[Il comando `smo backup update`](#)

Visualizzazione di un elenco di backup

È possibile controllare quali backup sono stati creati per un profilo e lo stato di backup utilizzando il comando `smo backup list`. Per ciascun profilo, il comando visualizza prima le informazioni relative al backup più recente, quindi continua fino a quando non vengono visualizzate le informazioni relative a tutti i backup.

1. Immettere il seguente comando: `smo backup list -profileprofile_name [-delimitercharacter] [data | -archivelogs] [-quiet | -verbose]`

Informazioni correlate

[Il comando `smo backup list`](#)

Visualizzazione dei dettagli del backup

È possibile visualizzare informazioni dettagliate su un particolare backup in un profilo utilizzando il comando `smo backup show`.

Il comando `smo backup show` visualizza le seguenti informazioni per ogni backup:

- L'ID di backup
- Se il backup ha avuto esito positivo o negativo
- Ambito del backup (completo, parziale, online o offline)
- Modalità di backup
- Stato del montaggio
- L'etichetta di backup
- Commento
- La data e l'ora di inizio e fine dell'operazione
- Informazioni sulla verifica del backup
- Classe di conservazione del backup
- Il nome del database e dell'host
- Il numero SCN (System Change Number) del checkpoint
- La SCN di fine backup (solo per backup online)
- I tablespace e i file di dati del database di cui è stato eseguito il backup
- File di controllo del database di cui è stato eseguito il backup

- L'archivio registra dal database di cui è stato eseguito il backup
- Il sistema di storage e i volumi in cui si trovano i file
- Le copie Snapshot eseguite e la loro posizione
- Lo stato delle risorse di storage principali
- Lo stato di protezione del backup
- Un elenco di copie sullo storage secondario, sotto forma di backup_copy ID - nome del nodo
- Modalità di backup

Se si specifica l'opzione `-verbose`, vengono visualizzate le seguenti informazioni aggiuntive:

- I cloni creati dal backup, se presenti
- Informazioni di verifica
- Se il backup è montato, SnapManager visualizza i punti di montaggio in uso

Per il backup del file di registro dell'archivio, vengono visualizzate le stesse informazioni dell'altro backup del database, ad eccezione delle seguenti informazioni:

- SCN del punto di verifica
- Fine SCN. Backup
- Tablespace
- File di controllo

Tuttavia, il backup del file di log dell'archivio contiene le seguenti informazioni aggiuntive:

- Il primo numero di modifica del backup
- Il numero di modifica successivo del backup
- Numero del thread
- Reimpostare l'ID dei log
- Incarnazione
- Nome del file di log

- Immettere il seguente comando: `smo backup show -profileprofile_name {-labellabel [data | -archivelogs] | -id id [-quiet | -verbose]}`

Informazioni correlate

[Il comando `smo backup show`](#)

Montaggio dei backup

SnapManager gestisce automaticamente il montaggio di un backup per renderlo disponibile all'host. È inoltre possibile montare i backup in scenari in cui si utilizza uno strumento esterno, ad esempio Oracle Recovery Manager (RMAN), per accedere ai file nel backup.

Se si utilizza RMAN, è necessario utilizzare l'operazione di montaggio per modificare lo stato di un backup (che consente l'accesso) e l'operazione di disinstallazione per modificare lo stato di un backup (che rimuove

l'accesso).

Il comando `smo backup mount` visualizza un elenco di percorsi in cui sono state montate le copie Snapshot costituite dal backup.

È possibile utilizzare l'opzione `-from-secondary` per montare il backup dallo storage secondario. Se non si utilizza questa opzione, SnapManager installa il backup dallo storage primario.

Specificare l'opzione `-copy-id` ogni volta che si specifica l'opzione `-from-secondary`. Se nel sistema di storage secondario sono presenti più backup, viene utilizzata l'opzione `-copy-id` per specificare quale copia di backup nello storage secondario utilizzare per montare il backup.⁶



Se si utilizza Data ONTAP in modalità 7, è necessario specificare un valore valido per l'opzione `-copy-id`. Tuttavia, se si utilizza Clustered Data ONTAP, l'opzione `-copy-id` non è richiesta.

Se si sta montando un backup del database su un host remoto, è necessario assicurarsi che le credenziali di Automatic Storage Management (ASM) siano le stesse su entrambi gli host.



È possibile raccogliere i file dump dopo un'operazione di montaggio di backup riuscita o non riuscita.

1. Per attivare un backup, immettere il seguente comando: `smo backup mount -profile profile_name {labellabel [data | -archivelogs] | -idid} [-host-host] [-from-secondary [-copy-id id]] [-dump] [-quiet | -verbose]`

Informazioni correlate

[Il comando di montaggio del backup smo](#)

Smontare i backup

SnapManager disinstalla automaticamente il backup per renderlo non disponibile sul server host. SnapManager consente inoltre di disinstallare se si utilizza uno strumento esterno, ad esempio Gestione ripristino Oracle (RMAN), per accedere ai file nel backup e modificare lo stato del backup per rimuovere l'accesso.

Se si dismonta un backup del database da un host remoto, assicurarsi che le credenziali di Automatic Storage Management (ASM) siano le stesse su entrambi gli host.

È possibile raccogliere i file dump dopo un'operazione di disinstallazione di backup riuscita o non riuscita.

L'operazione di disinstallazione potrebbe non riuscire con un messaggio di errore se il punto di montaggio è occupato, ad esempio `--[ERRORE] FLOW-11019: Errore in Disconnect: SD-10046: Non è possibile smontare il backup poiché il punto di montaggio è occupato con i seguenti percorsi di montaggio e PID: /Opt/NetApp/smo/mnt/-Nuse_nfsvrdb_Arch-20120427052319903_0 con PID 6598.`

È necessario identificare il PID della sessione che causa il guasto dell'operazione di disinstallazione. Interrompere la sessione eseguendo il seguente comando: `kill pid`

È quindi possibile eseguire l'operazione di disinstallazione.

1. Immettere il seguente comando: `smo backup unmount -profile profile_name {labellabel [data | -archivelogs] | -idid} [-quiet | -verbose] -dump-force-verbose`

Informazioni correlate

[Il comando smo backup unmount](#)

Liberare i backup

È possibile liberare i backup, eliminando le copie Snapshot senza eliminare i metadati di backup. Questa funzione libera lo spazio occupato dal backup. È possibile utilizzare il comando `smo backup free` per liberare i backup.

Affinché un backup possa essere liberato, è necessario assicurarsi di quanto segue:

- Backup riuscito
- Il backup non deve essere montato
- Il backup non ha cloni
- Il backup non deve essere conservato utilizzando una policy di conservazione illimitata
- Il backup non è già stato liberato

Se la protezione è attivata sul profilo e il criterio di protezione contiene connessioni dal nodo primario che utilizzano una relazione mirror, le copie Snapshot vengono eliminate sul nodo primario quando viene liberato un backup. Le copie Snapshot vengono eliminate anche dai nodi mirror quando si verifica il successivo trasferimento allo storage secondario.

Quando si libera un backup protetto, SnapManager richiede a Protection Manager di rimuovere le copie Snapshot locali per il backup. Se l'operazione senza backup viene eseguita correttamente per i backup protetti, le copie Snapshot vengono eliminate da Protection Manager in modo asincrono.

Stato di protezione	Stato locale	Azione sullo storage primario	Azione sullo storage secondario	Spiegazione
Non richiesto (da proteggere)	Esiste	Libera il backup	Non è richiesta alcuna azione	SnapManager libera il backup locale.
Liberato	Non è richiesta alcuna azione	Non è richiesta alcuna azione	Il backup locale è già stato liberato.	Non protetto
Esiste	Libera il backup	Non è richiesta alcuna azione	SnapManager libera il backup locale anche se sullo storage secondario non sono presenti copie.	Liberato
Non è richiesta alcuna azione	Non è richiesta alcuna azione	Il backup locale è già stato liberato.	Protetto	Esiste

Stato di protezione	Stato locale	Azione sullo storage primario	Azione sullo storage secondario	Spiegazione
Libera il backup	Nessuna azione richiesta; il backup su secondario rimane	SnapManager libera il backup locale. Le copie rimangono sullo storage secondario.	Liberato	Non è richiesta alcuna azione

È possibile specificare l'opzione `-dump` come parametro facoltativo per raccogliere i file dump dopo l'operazione senza backup riuscita o non riuscita.

1. Immettere il seguente comando: `smo backup free -profileprofile_name {-labellabel [data | -archive]logs} | -idid | -all} -force [-dump] [-quiet] [-force]`

Informazioni correlate

[Il comando `smo backup free`](#)

Eliminazione dei backup

È necessario eliminare i backup quando non sono più necessari, liberando così lo spazio occupato dai backup. Se si rimuovono i backup, si riduce la possibilità di raggiungere il limite di 255 copie Snapshot per volume.

- Assicurarsi che il backup non sia stato utilizzato per creare un clone.

Quando si elimina un backup protetto, SnapManager elimina il backup dallo storage secondario e dal repository SnapManager. La seguente tabella mostra le azioni eseguite sullo storage primario e secondario quando si elimina un backup locale:

Stato di protezione	Stato locale	Azione sullo storage primario	Azione sullo storage secondario	Spiegazione
Non richiesto (da proteggere)	Esiste	Elimina le copie Snapshot	Non è richiesta alcuna azione	SnapManager elimina il backup locale.
Liberato	Non è richiesta alcuna azione	Non è richiesta alcuna azione	Il backup locale è già stato liberato. Se si elimina un backup liberato, i metadati del backup vengono rimossi dal repository.	Non protetto

Stato di protezione	Stato locale	Azione sullo storage primario	Azione sullo storage secondario	Spiegazione
Esiste	Elimina le copie Snapshot	Non è richiesta alcuna azione	SnapManager elimina il backup locale indipendentemente dal fatto che sia stato protetto.	Liberato
Non è richiesta alcuna azione	Non è richiesta alcuna azione	Il backup locale è già stato liberato. Se si elimina un backup liberato, i metadati del backup vengono rimossi dal repository.	Protetto	Esiste
Elimina le copie Snapshot	SnapManager elimina il backup sullo storage secondario	SnapManager elimina il backup locale e le copie secondarie.	Liberato	Non è richiesta alcuna azione

Se si tenta di eliminare un backup protetto dallo storage secondario, le copie Snapshot potrebbero essere contrassegnate per l'eliminazione e successivamente eliminate da Protection Manager.

È possibile eliminare i backup conservati senza limiti senza modificare la classe di conservazione.

È possibile raccogliere i file dump dopo l'operazione di eliminazione del backup riuscita o non riuscita.

Se si desidera eliminare i backup del registro di archiviazione, è necessario verificare la durata di conservazione impostata per il backup del registro di archiviazione. Se il backup del registro di archiviazione rientra nella durata di conservazione e i file di registro di archiviazione sono necessari per il ripristino di un database ripristinato, non è possibile eliminare il backup del registro di archiviazione.

1. Verificare che le operazioni siano complete immettendo il seguente comando: `smo operation list -profileprofile_name-quiet-verbose`
2. Per eliminare un backup, immettere il seguente comando: `smo backup delete -profile_name [-label label [data | -archivelogs] | -idid | -all] [-force] [-dump] [-quiet | -verbose]`

Utilizzare l'opzione `-force` per forzare la rimozione del backup. Forzare la rimozione di un backup con operazioni incomplete potrebbe lasciare il backup in uno stato incoerente.

Pianificazione dei backup del database

SnapManager (3.2 o versioni successive) per Oracle consente di pianificare backup del database regolari durante le ore di lavoro fuori dalle ore di punta per mantenere performance elevate. Per pianificare un backup, è possibile creare un profilo che includa le informazioni del database e i criteri di conservazione, quindi impostare le pianificazioni per il backup.



È necessario pianificare i backup come utente root o come utente Oracle. Se si tenta di pianificare i backup come utente non esistente, SnapManager visualizza un messaggio di errore: Utente non valido: Nome utente: Impossibile creare il backup di pianificazione per un determinato utente

Di seguito sono riportate alcune delle attività correlate alla pianificazione:

- Pianificare un backup del database in modo che venga eseguito su base oraria, giornaliera, settimanale, mensile o una sola volta.
- Visualizzare un elenco di backup pianificati associati a un profilo.
- Aggiornare un backup pianificato.
- Sospendere temporaneamente un programma.
- Riprendere il programma sospeso.
- Eliminare un programma.



La casella di controllo **Esegui ora operazione menu** è disattivata quando viene eseguito un backup pianificato per tale pianificazione.

Creazione di pianificazioni di backup

È possibile pianificare un backup in base all'ora e alla frequenza adatte per i dati e l'ambiente.

Da SnapManager 3.2 per Oracle, è possibile pianificare i backup dei file di log dell'archivio separatamente. Tuttavia, è necessario utilizzare il profilo creato per separare i file di log dell'archivio.

Se sono stati pianificati i backup dei file di dati e dei file di registro dell'archivio contemporaneamente, SnapManager crea prima il backup dei file di dati.

Se si seleziona l'intervallo di pianificazione come -onetimonly, tutte le opzioni di eliminazione sono disponibili. Se si seleziona un intervallo di pianificazione diverso da -onetimonly, le opzioni di eliminazione -Until-SCN e -Until-date non sono supportate e viene visualizzato il seguente messaggio di errore: L'opzione di eliminazione del registro di archiviazione specificata, -Until-scn o -Until-date per l'intervallo di pianificazione orario non è valida. Specificare l'opzione -onetimeonly per l'intervallo di pianificazione oppure eseguire la riduzione dei registri di archiviazione utilizzando una qualsiasi delle opzioni all'opppure -before {-months | -days | -weeks | -hours}.

Quando si verifica un failover in un ambiente HACMP (High Availability Cluster Multiprocessing), è necessario riavviare il server SnapManager per Oracle in modo che l'indirizzo del servizio (virtuale) sia mappato all'host attivo e le pianificazioni SnapManager siano regolate sull'host SnapManager attivo. È possibile aggiungere queste informazioni negli script di failover HACMP di pre-elaborazione o post-elaborazione.



Se in un altro repository sono presenti lo stesso nome di profilo e pianificazione, l'operazione di pianificazione del backup non viene avviata in quel repository. L'operazione viene chiusa con il seguente messaggio: Operazione già in esecuzione.

1. Immettere il seguente comando: `smo schedule create -profile profile_name {[-full {-online | -offline | -auto}]{-retain [-hourly | -daily | -settimanale | -mensile | -illimitato] [-verify]] | [-data [-filesfiles [files] | [-tablespaces-tablespaces [-tablespaces] {-online | -offline | -verify [-shourly}}-sharily | -sharily | -verify [-sharily | -sharf]-sharily | -verify [-sharily | -sharily | -sharf]-sharf | -sharf]-sharf | -sh -Noprotect] [-backup-destpath1`

```
[,[path2]] [-exclude-destpath1 [,path2]] [-prunelogs{-all | -until-dateyyyy-MM-dd HH:mm:ss | -before {-months | -settimane | -giorni | -ore-}} -prune-tempistiche -tempistiche_<yyyy-MM-dd HH:mm> di_diraspa_inizio_{-timeschescheschedule | -tempistiche -tempistiche_di_inizio_di_tempistiche -} -tempistiche_di_di_inizio_di_{-}tempistiche_di_tempistiche_di_inizio_di_di_tempistiche [-tempistiche] -tempistiche] --tempistiche_di_di_tempistiche_di_di_di_di_tempistiche | --tempistiche di_di_di_di_inizio
```

Se si desidera...	Quindi...
Pianificare un backup di un database online o offline	Specificare -offline o -online per pianificare un backup del database offline o online. Se si specificano questi valori, non è possibile utilizzare -auto.
Lasciare che SnapManager gestisca la pianificazione di un database indipendentemente dal fatto che sia online o offline	Specificare -auto. Se si specifica -auto, non è possibile utilizzare --offline o -online.
Pianificare un backup dei file di dati	Specificare -data -files per elencare i file separati da virgole. Ad esempio, utilizzare i nomi dei file f1,f2,f3.
Pianificare un backup parziale di spazi tabella specifici	Specificare -tablespaces per elencare i tablespaces separati da virgole. Ad esempio, utilizzare ts1,ts2,ts3.
Pianificare il backup dei file di log dell'archivio	Specificare quanto segue: <ul style="list-style-type: none"> • -archiveed per pianificare il backup dei file di log dell'archivio • -backup-dest per pianificare le destinazioni dei file di log di archiviazione da includere nel backup • -exclude-dest per pianificare le destinazioni del registro di archiviazione da escludere dal backup
Specificare i valori della classe di conservazione	Specificare -retain e indicare se il backup deve essere conservato in base a una delle seguenti classi di conservazione: <ul style="list-style-type: none"> • orario • giornaliero • settimanale • mensile • -Unlimited SnapManager (numero illimitato): Il valore predefinito è orario.

Se si desidera...	Quindi...
Schedule pruning dei file di log di archivio	Specificare quanto segue: -Prunelogs per rimuovere i file di log dell'archivio durante la pianificazione di un backup -prune-dest per specificare la destinazione del log dell'archivio da cui vengono eliminati i file di log dell'archivio
Includere un nome per la pianificazione	Specificare -schedule-name.
Pianificare il backup del database a un intervallo di tempo specifico	Specificare l'opzione Interval (intervallo) e selezionare l'intervallo di tempo tra i seguenti, in base al quale creare i backup: <ul style="list-style-type: none"> • orario • giornaliero • settimanale • mensile • -onetimeonly
Configurare una pianificazione	Specificare -cronstring e includere le seguenti sette sottoespressioni che descrivono la singola opzione: <ul style="list-style-type: none"> • 1 si riferisce ai secondi. • 2 indica i minuti. • 3 si riferisce alle ore. • 4 si riferisce a un giorno in un mese. • 5 si riferisce al mese. • 6 si riferisce a un giorno in una settimana. • (Facoltativo) 7 si riferisce all'anno. Nota: se il backup è stato pianificato con orari diversi in -cronstring e -start-time, la pianificazione del backup viene sovrascritta e attivata da -start-time.
Aggiungere un commento sulla pianificazione del backup	Specificare -schedule-comment seguito dalla stringa di descrizione.
Specificare l'ora di inizio dell'operazione di pianificazione	Specificare -start-time nel formato yyyy-mm-gg hh:mm.

Se si desidera...	Quindi...
Modificare l'utente dell'operazione di backup pianificata durante la pianificazione del backup	Specificare -runasuser. L'operazione viene eseguita come utente (utente root o utente Oracle) che ha creato la pianificazione. Tuttavia, è possibile utilizzare il proprio ID utente, se si dispone di credenziali valide sia per il profilo del database che per l'host.
Attivare un'attività di pre-task o post-task dell'operazione di pianificazione del backup utilizzando il file XML delle specifiche di pre-task e post-task	Specificare l'opzione -taskspec e fornire il percorso assoluto del file XML delle specifiche delle attività per eseguire una pre-elaborazione o un'attività di post-elaborazione prima o dopo l'operazione di pianificazione del backup.

Aggiornamento di una pianificazione di backup

È possibile visualizzare un elenco delle operazioni pianificate e aggiornarle, se necessario. È possibile aggiornare la frequenza di pianificazione, l'ora di inizio della pianificazione, l'espressione crontstring e l'utente che ha pianificato il backup.

1. Per aggiornare la pianificazione di un backup, immettere il seguente comando: `smo schedule update -profile profile_name-schedule-nameschedulename [-schedule-commentschedule comment] -interval {-hourly | -daily | -weekly | -monthly | -onetimeonly} -start-timestarttime-cronstringcronstring-runasuserrunasuser [-quiet | -verbose]`

Visualizzazione di un elenco di operazioni pianificate

È possibile visualizzare un elenco di operazioni pianificate per un profilo.

1. Per visualizzare le informazioni relative all'operazione pianificata, immettere il seguente comando: `smo schedule list -profile profile_name[-quiet | -verbose]`

Sospensione delle pianificazioni di backup

SnapManager consente di sospendere una pianificazione di backup fino al ripristino della pianificazione di backup.

È possibile sospendere le pianificazioni attive. Se si tenta di sospendere la pianificazione di backup già sospesa, potrebbe venire visualizzato il messaggio di errore "Impossibile sospendere: Pianificare <schedulename> già in stato di sospensione".

1. Per sospendere temporaneamente la pianificazione del backup, immettere il seguente comando: `smo schedule suspend -profile profile_name-schedule-nameschedulename [-quiet | -verbose]`

Ripresa delle pianificazioni di backup

Gli amministratori hanno la possibilità di riprendere la pianificazione del backup sospeso.

Se si tenta di riprendere le pianificazioni attive, potrebbe venire visualizzato il messaggio di errore "Impossibile riprendere: Pianificazione <schedulename> già in stato di ripristino".

1. Per riprendere la pianificazione di backup sospesa, immettere il seguente comando: `smo schedule resume -profile profile_name-schedule-nameschedulename [-quiet | -verbose]`

Eliminazione delle pianificazioni di backup

È possibile eliminare le pianificazioni di backup quando non sono più necessarie.

1. Per eliminare la pianificazione di backup, immettere il seguente comando: `smo schedule delete -profile profile_name-schedule-nameschedulename [-quiet | -verbose]`

Ripristino dei backup del database

SnapManager per Oracle consente di ripristinare un database nello stato in cui si trovava quando è stata eseguita una copia Snapshot. Oltre al processo di ripristino basato su file, SnapManager supporta la tecnologia di ripristino rapido basata su volume, che riduce significativamente il tempo di ripristino rispetto ad altri metodi di ripristino. Poiché i backup vengono creati con maggiore frequenza, il numero di log da applicare viene ridotto, riducendo così il tempo medio di ripristino (MTTR) per un database.

Di seguito sono riportate alcune delle attività che è possibile eseguire in relazione al ripristino e al ripristino dei dati nei database:

- Eseguire un ripristino basato su file o un ripristino basato su volume, che è il metodo più rapido per ripristinare i backup del database ed è l'impostazione predefinita utilizzata da SnapManager.
- Ripristinare l'intero backup o parte di esso.

Se si ripristina una parte di esso, si specifica un gruppo di tablespace o un gruppo di file di dati. È inoltre possibile ripristinare i file di controllo insieme ai dati o solo i file di controllo stessi.

- Ripristinare i dati in base a un punto temporale o a tutti i registri disponibili, che memorizzano l'ultima transazione impegnata nel database.

Il punto temporale può essere un Oracle System Change Number (SCN) o una data e un'ora (yyyy-mm-dd:hh:mm:ss). SnapManager utilizza l'orologio a 24 ore.

- Ripristino dai backup sullo storage primario (backup locali).
- Ripristinare e ripristinare il backup utilizzando SnapManager oppure utilizzare SnapManager per ripristinare il backup e utilizzare un altro strumento, ad esempio Recovery Manager (RMAN), per ripristinare i dati.
- Ripristinare i backup da posizioni alternative.
- Ripristinare i backup protetti dallo storage secondario (backup remoti) e da una posizione alternativa utilizzando il file delle specifiche di ripristino.

È possibile ripristinare un backup eseguito da una versione precedente di SnapManager utilizzando SnapManager 3.0 e versioni successive.

SnapManager offre inoltre la possibilità di ripristinare i database di gestione automatica dello storage (ASM). Un gruppo di dischi ASM può essere condiviso da più database. Pertanto, non è possibile ripristinare una copia Snapshot precedente del gruppo di dischi, perché ripristinerebbe tutti i database. Le soluzioni tradizionali per le operazioni di ripristino passano attraverso l'host e richiedono che tutti i blocchi che costituiscono il database vengano spostati dal sistema di storage all'host e quindi di nuovo al sistema di storage. SnapManager elimina questo overhead offrendo la possibilità di ripristinare solo i dati richiesti all'interno del gruppo di dischi ASM senza passare attraverso l'host.

Gli amministratori possono eseguire operazioni di ripristino o ripristino utilizzando l'interfaccia grafica utente (GUI) di SnapManager o l'interfaccia a riga di comando (CLI).

Informazioni correlate

[Backup dei database](#)

[Il comando di ripristino del backup smo](#)

Che cos'è il ripristino del database

SnapManager consente di eseguire operazioni di backup e ripristino basate su volume o file.

La seguente tabella descrive i metodi di ripristino:

Processo di ripristino	Dettagli
Ripristini rapidi basati su volume (dallo storage primario)	SnapManager ripristina i file di dati di un database ripristinando un volume completo. Questo processo predefinito è il metodo più rapido per il ripristino del database.
Ripristini basati su file	Ripristino completo del file system lato storage (da primario o secondario): SnapManager esegue un ripristino completo del numero di unità logica (LUN).
Ripristino file lato storage: SnapManager esegue un singolo ripristino snap-file (SFSR) in un ambiente NAS o un ripristino snap-file parziale (PFSR) in un ambiente di gestione automatica dello storage (ASM). In un SFSR, vengono ripristinati i file o i LUN che rappresentano gli oggetti protetti. Un PFSR viene eseguito dal backup locale se i dettagli del file system e il layout del file system non sono stati modificati dopo l'esecuzione del backup precedente.	Ripristino della copia del file lato host (da primario o secondario): SnapManager clona il backup locale utilizzando un LUN o un FlexClone. Il clone viene montato e SnapManager copia i file host dal clone nel file system attivo.

Anche se l'impostazione predefinita è il processo di ripristino rapido, gli amministratori possono scegliere uno dei due tipi. Nel processo di ripristino rapido, SnapManager fornisce informazioni sulle condizioni che impediscono il completamento del processo di ripristino rapido e su quelle che potrebbero influire sul ripristino rapido, ma che gli amministratori possono ignorare se scelgono di continuare il processo.



Non è possibile ripristinare un backup dallo storage secondario, se il backup esiste anche nello storage primario.

Una volta completata l'operazione di ripristino rapido, SnapManager esegue le seguenti operazioni:

- Libera i backup più recenti (eseguiti dopo il ripristino del backup) nello stesso profilo, perché le copie Snapshot non esistono più sullo storage primario.
- Elimina tutte le copie Snapshot per i backup nello stesso profilo in cui le copie Snapshot venivano eliminate automaticamente dal processo di ripristino rapido.

In questo modo si evita che i backup vengano parzialmente liberati. Ad esempio, è stato creato prima Backup_A e poi Backup_B. Ciascuno di essi dispone di una copia Snapshot per i file di dati e di una per i registri di archiviazione. Dopo che SnapManager ha ripristinato Backup_A utilizzando il processo di ripristino rapido, SnapManager elimina automaticamente la copia Snapshot del file di dati da Backup_B. Poiché il log di archiviazione non viene ripristinato durante il processo di ripristino rapido, SnapManager deve eliminare la copia Snapshot dei log di archiviazione di Backup_B al termine del processo di ripristino rapido.

Ripristino rapido

Il ripristino rapido o basato su volume è così chiamato perché è il metodo di ripristino più veloce possibile. L'intero volume del sistema di storage viene reimpostato su una copia Snapshot. A livello di storage, questo ripristino è quasi istantaneo. Tuttavia, l'esecuzione di un ripristino di un volume può avere le seguenti conseguenze negative e pertanto deve essere utilizzata con cautela:

- L'intero volume lato storage viene invertito, tra cui:
 - File non considerati come parte del backup
 - Altri file, file system o LUN sul volume
- Tutte le copie Snapshot create dopo la copia Snapshot in cui viene eseguito il ripristino del volume vengono eliminate.

Ad esempio, non è più possibile ripristinare il backup di martedì se il volume è stato ripristinato il backup di lunedì.

- Le relazioni con i sistemi storage secondari vengono interrotte se la copia Snapshot ripristinata è precedente alla copia Snapshot di riferimento nella relazione.

Ripristino completo del file system lato storage

Un ripristino completo del file system lato storage viene eseguito quando non è possibile eseguire un ripristino del volume, ma è possibile ripristinare l'intero file system sul sistema storage.

Quando viene eseguito un ripristino del file system lato storage, si verifica quanto segue:

- In un ambiente SAN, tutte le LUN utilizzate dal file system (e se presenti nel gruppo di volumi sottostante) vengono ripristinate nel sistema di storage.
- In un ambiente NAS, ogni file nel file system viene ripristinato sul sistema di storage.

Per gli ambienti NAS, questo meccanismo di ripristino non offre ulteriori vantaggi rispetto al ripristino dei file lato storage.

Quando viene eseguito un ripristino del file system lato storage, a seconda della posizione di storage si verifica quanto segue:

- Quando SnapManager viene ripristinato dai sistemi di storage primari, i LUN (SAN) o i file (NAS) vengono ripristinati in posizione tramite SFSR.
- Quando SnapManager viene ripristinato dai sistemi di storage secondari, i LUN (SAN) o i file (NAS) vengono copiati dai sistemi di storage secondari di nuovo nel sistema di storage primario sulla rete.

Poiché il file system è completamente ripristinato, vengono ripristinati anche i file che non fanno parte del backup. È necessario eseguire un override se nel file system che si sta ripristinando sono presenti file che non fanno parte del ripristino.

Ripristino dei file sul lato storage

Talvolta, il ripristino del file dal lato dello storage viene eseguito quando non è possibile eseguire un ripristino del file system dal lato dello storage. In un ripristino dei file dal lato dello storage, i singoli file all'interno di un file system vengono ripristinati direttamente sui sistemi di storage.

Questo tipo di ripristino può essere eseguito solo in ambienti NFS.

Per gli ambienti ASM, il ripristino dei file sul lato storage può essere eseguito solo se si verificano le seguenti condizioni:

- Le estensioni dei file sottostanti non sono state modificate dopo l'esecuzione del backup (ad esempio, il file non è stato ridimensionato e il ribilanciamento del disco non si è verificato).
- Si sta eseguendo il ripristino dai sistemi storage primari. (Non è supportato durante il ripristino da sistemi storage secondari).

Quando viene eseguito un ripristino del file dal lato dello storage, si verifica quanto segue:

- Quando SnapManager ripristina i file NFS dai sistemi di storage primari, i singoli file vengono ripristinati utilizzando SFSR.
- Quando SnapManager ripristina i file NFS dai sistemi di storage secondari, i singoli file vengono copiati di nuovo nel sistema di storage primario sulla rete di storage.
- Quando si ripristinano i file ASM dai sistemi di storage primari, i singoli file vengono ripristinati ripristinando solo i byte nelle LUN sottostanti associate ai file da ripristinare (il resto dei byte nelle LUN rimane intatto). La tecnologia del sistema storage utilizzata per il ripristino parziale dei LUN è denominata PFSR.

Ripristino del file sul lato host

Un ripristino della copia del file lato host viene utilizzato come ultima risorsa negli ambienti SAN quando non è possibile eseguire il ripristino rapido, il ripristino del file system lato storage e il ripristino del file lato storage.

Il ripristino di una copia del file lato host richiede le seguenti operazioni:

- Clonazione dello storage
- Connessione dello storage clonato all'host
- Copia dei file dal file system clone nei file system attivi
- Disconnessione dello storage clone dall'host
- Eliminazione dello storage clone

Durante il ripristino dallo storage secondario, SnapManager tenta innanzitutto di ripristinare i dati direttamente dal sistema di storage secondario al sistema di storage primario (senza coinvolgere l'host). Se SnapManager non è in grado di eseguire questo tipo di ripristino (ad esempio, se in un file system sono presenti file che non fanno parte del ripristino), SnapManager eseguirà il ripristino della copia del file sul lato host. SnapManager offre due metodi per eseguire un ripristino della copia del file sul lato host dallo storage secondario. Il metodo SnapManager Selects viene configurato nel file `smo.config`.

- **Diretto:** SnapManager clona i dati sullo storage secondario, monta i dati clonati dal sistema di storage secondario sull'host e copia i dati dal clone nell'ambiente attivo. Questo è il criterio di accesso secondario predefinito.
- **Indiretto:** SnapManager copia prima i dati in un volume temporaneo sullo storage primario, quindi monta i dati dal volume temporaneo all'host, quindi copia i dati dal volume temporaneo nell'ambiente attivo. Questo criterio di accesso secondario deve essere utilizzato solo se l'host non dispone di accesso diretto al sistema di storage secondario. I ripristini con questo metodo richiedono il doppio del tempo rispetto al criterio di accesso secondario diretto, poiché vengono eseguite due copie dei dati.

La decisione di utilizzare il metodo diretto o indiretto è controllata dal valore del parametro `restore.secondaryAccessPolicy` nel file di configurazione `smo.config`. L'impostazione predefinita è `Direct` (diretto).

Indicazioni su quando è possibile utilizzare il ripristino rapido

Si applicano regole specifiche per l'utilizzo del ripristino rapido per ottenere performance di ripristino ottimali. In alcuni casi, non è possibile utilizzare il ripristino rapido.

Per ottenere prestazioni di ripristino ottimali (ripristino del volume o ripristino di un gruppo di dischi completo), è necessario rispettare le seguenti regole:

- Solo i ripristini completi dei backup completi sono idonei per il ripristino rapido.
- Solo i file di dati sono idonei per il ripristino rapido.
- I file di dati devono essere gli unici file di un volume a poter essere ripristinati rapidamente.

Sebbene i file di dati temporanei possano risiedere nel volume, i file di controllo, i log, i file pfile o altri file devono risiedere su un volume separato dai file di dati. È necessario configurare un database Oracle con file di dati su un volume separato da file di controllo, log archiviati e file di log online.

- I file di dati per un solo database devono essere presenti nel volume.
- È possibile utilizzare più file system, ma i file in questi file system devono essere file di dati per un solo database.
- Per i database ASM, ciascun database deve utilizzare il proprio gruppo di dischi ASM e il database ASM non può condividere lo storage con altri database ASM.



Per verificare se un backup creato in precedenza è ripristinabile utilizzando il ripristino rapido, è possibile utilizzare l'opzione `-preview` del comando `smo backup restore`.

Il processo di ripristino rapido non può essere utilizzato nei seguenti casi:

- Su backup parziali
- Sui backup dallo storage secondario, se il backup esiste anche sullo storage primario

Non è possibile ripristinarli utilizzando il ripristino basato su file o su volume.

- Backup protetti con SnapVault

Il processo di ripristino rapido non può essere utilizzato per i backup creati prima dell'ultimo backup protetto. Tuttavia, è possibile utilizzare il processo di ripristino rapido per i backup creati dopo l'ultimo backup protetto. Ad esempio, prendere in considerazione i backup A, B e C. B è l'ultimo backup da trasferire allo storage secondario utilizzando SnapVault. È possibile ripristinare rapidamente B e C, ma non è possibile ripristinare rapidamente A perché è stato creato prima dell'ultimo backup protetto. SnapVault ha bisogno di un SnapVault di riferimento per calcolare la differenza di tempo e inviarlo allo storage secondario al successivo trasferimento di un backup allo storage secondario. L'ultimo backup protetto funge da copia Snapshot di riferimento. Pertanto, l'utilizzo del processo di ripristino rapido impedisce a SnapVault di riconoscere la linea di base.

- FlexClone o cloni LUN che utilizzano copie Snapshot create dopo la copia Snapshot in cui viene eseguito il ripristino del volume

Ad esempio, i cloni possono essere il risultato di un backup successivo che viene montato o clonato da SnapManager.

- LUN che non fanno parte della copia Snapshot SnapDrive attiva

Non è possibile eseguire un ripristino rapido insieme ad altri tipi di ripristino per lo stesso backup. Ad esempio, se un volume di dati può essere ripristinato utilizzando il processo di ripristino rapido, ma un altro volume di dati non può essere ripristinato, nessuno dei due viene ripristinato utilizzando il processo di ripristino rapido. In questo caso, è possibile scegliere un ripristino basato su file.

Inoltre, è necessario considerare i seguenti punti relativi ai ripristini dei database:

- SnapManager non ripristina mai i log di archiviazione o di ripristino, ma monta il backup dei file di log di archiviazione e li utilizza per il ripristino.
- SnapManager non ripristina mai i file di controllo utilizzando il ripristino del volume.
- Se si desidera ripristinare i file di controllo e i file di dati, SnapManager esegue il ripristino in due fasi.

SnapManager ripristina prima i file di controllo e poi i file di dati.

- Se SnapManager trova file temporanei nello stesso volume dei file tablespace standard, non è necessario eseguire un override per eseguire un ripristino a livello di volume.

Dopo il ripristino di un volume, lo spazio tabella TEMP viene riportato in linea.

Informazioni correlate

[Layout generali del database e configurazioni di storage consigliati](#)

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

Vantaggi e svantaggi dell'utilizzo del ripristino rapido

I DBA devono essere consapevoli dei vantaggi e degli svantaggi dell'utilizzo di ripristini rapidi basati su volumi.

Il ripristino dei backup del database con ripristini rapidi offre i seguenti vantaggi:

- I ripristini basati su volume riducono il tempo necessario per il ripristino dei backup.

- SnapManager offre controlli rapidi di idoneità per il ripristino. SnapManager analizza il backup del database e visualizza informazioni sulla possibilità di eseguire il ripristino basato su volume.
- È possibile visualizzare in anteprima l'operazione di ripristino e decidere se continuare con il percorso consigliato o ignorare il suggerimento con il processo selezionato.

Il ripristino dei backup del database con ripristini rapidi presenta i seguenti svantaggi:

- L'intero file system viene invertito, inclusi i file che non sono stati considerati parte del backup. Verranno ripristinati anche altri file, file system o LUN sul volume.
- SnapManager rimuove tutte le copie Snapshot eseguite dopo l'istantanea a cui si sta ripristinando. In effetti, si perde la cronologia dopo la data di copia Snapshot. Ad esempio, non è possibile ripristinare il backup di martedì se è già stato ripristinato il backup di lunedì.

È possibile evitare gli svantaggi seguendo questi consigli:

- Ottimizza il layout del database in base alle Best practice.
- Proteggere i backup sullo storage secondario. Tuttavia, se si eliminano le copie Snapshot dallo storage primario, non è possibile utilizzare ripristini rapidi per ripristinarle dallo storage secondario.

Controlli di idoneità per il ripristino rapido

Quando si sceglie di eseguire un ripristino rapido di un backup, SnapManager esegue prima un controllo di idoneità per determinare se è possibile utilizzare il processo di ripristino rapido.

SnapManager offre i seguenti tipi di controlli:

- Controlli obbligatori: SnapManager è in grado di eseguire il processo di ripristino rapido solo se tutte le condizioni di questo controllo vengono superate.
- Controlli sovrascrivibili: Se le condizioni di questo controllo non riescono, gli amministratori possono eseguire l'override del controllo per forzare un processo di ripristino rapido. Tuttavia, è necessario ignorare questi controlli con cautela.

La tabella seguente elenca i problemi che potrebbero verificarsi e indica se è possibile eseguire l'override del controllo di idoneità per il ripristino rapido:

Problema	Pass richiesto	Dettagli
ACFS, disco di voto o OCR sono presenti nel gruppo di dischi ASM in 11gR2	Sì	Impossibile eseguire il ripristino rapido. Risoluzione: Nessuna Impossibile eseguire l'override.
Solo i backup creati con SnapManager 3.0 o versioni successive possono essere ripristinati rapidamente	Sì	Impossibile eseguire l'override.

Problema	Pass richiesto	Dettagli
È possibile ripristinare rapidamente solo le copie Snapshot create con SnapDrive per UNIX 4.0 o versioni successive	Sì	Impossibile eseguire l'override.
Volume è un volume root	Sì	Il volume che viene ripristinato è un volume root nel sistema di storage. Soluzione: Non utilizzare il volume root sul sistema di storage. Impossibile eseguire l'override.
Il ripristino del volume non è disponibile in Windows	Sì	Il volume che viene ripristinato è un volume root nel sistema di storage. Risoluzione: Nessuna Impossibile eseguire l'override.
Il ripristino del volume è disattivato	Sì	Il ripristino del volume è stato disattivato. Risoluzione: Abilitare il ripristino del volume selezionando diverse opzioni all'avvio del ripristino. Nell'interfaccia della riga di comando, non utilizzare -fast -off. Impossibile eseguire l'override.

Problema	Pass richiesto	Dettagli
File di controllo e file di dati sullo stesso volume	Sì	<p>Per i backup online, i file di controllo e i file di dati non possono trovarsi sullo stesso volume perché SnapManager esegue due copie Snapshot del volume (una in cui i file di dati sono coerenti in modalità hot backup, e uno in cui i file di controllo del backup sono coerenti dopo il completamento della modalità di backup a caldo). Il ripristino del volume viene ripristinato alla prima copia Snapshot, che elimina la seconda copia Snapshot contenente i file di controllo del backup. Quando si verifica un ripristino solo del file di dati, i file di controllo vengono ripristinati in uno stato incoerente e SnapManager ripristina il file di controllo del backup, quindi apre il database con l'opzione resetlog, che non è il comportamento desiderato.</p> <p>Soluzione: Migrare i file di controllo e i file di dati su file system separati che non condividono lo stesso volume sottostante. Questo non aiuta il ripristino in cui il controllo non è riuscito, ma aiuterà le future operazioni di ripristino del backup.</p> <p>Impossibile eseguire l'override.</p>

Problema	Pass richiesto	Dettagli
I log di archiviazione e i file di dati non devono esistere sullo stesso volume	Sì	<p>I file di dati e i log di archiviazione del database risiedono in file system supportati dallo stesso volume del sistema di storage. Se è stato eseguito un ripristino di un volume, SnapManager non può aprire il database dopo un ripristino di un backup online perché il file di registro archiviato che viene scritto dopo che il database viene portato fuori dalla modalità di backup a caldo non è disponibile. Inoltre, non sarebbe possibile eseguire il rollforward delle transazioni successive che potrebbero essere state nei file di log dell'archivio.</p> <p>Soluzione: Migrare i log di archiviazione e i file di dati su file system separati che non condividono lo stesso volume del sistema di storage sottostante. Questo non aiuta il ripristino in cui il controllo non è riuscito, ma aiuterà le future operazioni di ripristino del backup.</p> <p>Impossibile eseguire l'override.</p>
I log online e i file di dati non devono esistere sullo stesso volume	Sì	<p>I file di dati e i log di ripristino online del database risiedono in file system supportati dallo stesso volume del sistema di storage. Se è stato eseguito un ripristino del volume, il ripristino non può utilizzare i log di ripristino online perché sarebbero stati ripristinati.</p> <p>Soluzione: Migrare i log di ripristino online e i file di dati su file system separati che non condividono lo stesso volume del sistema di storage sottostante. Questo non aiuta il ripristino in cui il controllo non è riuscito, ma aiuterà le future operazioni di ripristino del backup.</p> <p>Impossibile eseguire l'override.</p>

Problema	Pass richiesto	Dettagli
I file nel file system che non fanno parte dell'ambito di ripristino vengono ripristinati	Sì	<p>I file visibili sull'host, diversi dai file da ripristinare, esistono in un file system sul volume. Se è stato eseguito un ripristino rapido o un ripristino del file system lato storage, i file visibili sull'host vengono ripristinati al contenuto originale al momento della creazione della copia Snapshot. Se SnapManager rileva 20 o meno file, questi vengono elencati nella verifica di idoneità. In caso contrario, SnapManager visualizza un messaggio che indica di esaminare il file system.</p> <p>Soluzione: Migrare i file non utilizzati dal database su un file system diverso che utilizza un volume diverso. In alternativa, eliminare i file.</p> <p>Se SnapManager non è in grado di determinare lo scopo del file, è possibile eseguire l'override dell'errore di controllo. Se si esegue l'override del controllo, i file non inclusi nell'ambito di ripristino vengono ripristinati. Eseguire l'override di questo controllo solo se si è certi che il ripristino dei file non avrà alcun effetto negativo.</p>

Problema	Pass richiesto	Dettagli
I file system nel gruppo di volumi specificato che non fanno parte dell'ambito di ripristino vengono ripristinati	No	<p>Più file system si trovano nello stesso gruppo di volumi, ma non tutti i file system devono essere ripristinati. Il ripristino rapido e il ripristino del file system lato storage non possono essere utilizzati per ripristinare singoli file system all'interno di un gruppo di volumi, in quanto le LUN utilizzate dal gruppo di volumi contengono dati provenienti da tutti i file system. Tutti i file system all'interno di un gruppo di volumi devono essere ripristinati contemporaneamente per utilizzare il ripristino rapido o il ripristino del file system lato storage. Se SnapManager rileva 20 o meno file, SnapManager li elenca nel controllo di idoneità. In caso contrario, SnapManager visualizza un messaggio che indica di esaminare il file system.</p> <p>Soluzione: Migrare i file non utilizzati dal database in un gruppo di volumi diverso. In alternativa, eliminare i file system nel gruppo di volumi.</p> <p>Può eseguire l'override.</p>

Problema	Pass richiesto	Dettagli
I volumi host nel gruppo di volumi specificato che non fanno parte dell'ambito di ripristino vengono ripristinati	No	<p>Più volumi host (volumi logici) si trovano nello stesso gruppo di volumi, ma non tutti i volumi host devono essere ripristinati. Questo controllo è simile a quello eseguito dai file system nel gruppo di volumi che non fanno parte dell'ambito di ripristino, ad eccezione del fatto che gli altri volumi host nel gruppo di volumi non sono montati come file system sull'host. Soluzione: Migrare i volumi host utilizzati dal database in un gruppo di volumi diverso. In alternativa, eliminare gli altri volumi host nel gruppo di volumi.</p> <p>Se si ignora il segno di spunta, vengono ripristinati tutti i volumi host del gruppo di volumi. Eseguire l'override di questo controllo solo se si è certi che il ripristino degli altri volumi host non influisca negativamente su nulla.</p>
Le estensioni dei file sono cambiate dall'ultimo backup	Sì	Impossibile eseguire l'override.

Problema	Pass richiesto	Dettagli
I LUN mappati nel volume non inclusi nell'ambito di ripristino vengono ripristinati	Sì	<p>I LUN diversi da quelli richiesti per il ripristino nel volume sono attualmente mappati a un host. Non è possibile eseguire un ripristino del volume perché altri host o applicazioni che utilizzano queste LUN diventeranno instabili. Se i nomi LUN terminano con un trattino di sottolineatura e un indice intero (ad esempio _0 o _1), questi LUN sono in genere cloni di altre LUN all'interno dello stesso volume. È possibile che venga montato un altro backup del database o che esista un clone di un altro backup.</p> <p>Soluzione: Migrare i LUN non utilizzati dal database su un volume diverso. Se le LUN mappate sono cloni, cercare i backup montati dello stesso database o dei cloni del database e smontare il backup o rimuovere il clone.</p> <p>Impossibile eseguire l'override.</p>
I LUN non mappati nel volume non inclusi nell'ambito di ripristino vengono ripristinati	No	<p>Nel volume esistono LUN diversi da quelli richiesti per il ripristino. Questi LUN non sono attualmente mappati a nessun host, pertanto il ripristino non interrompe alcun processo attivo. Tuttavia, i LUN potrebbero essere temporaneamente non mappati.</p> <p>Soluzione: Migrare i LUN non utilizzati dal database su un volume diverso o eliminare i LUN.</p> <p>Se si esegue l'override di questo controllo, il ripristino del volume ripristinerà questi LUN nello stato in cui è stata eseguita la copia Snapshot. Se il LUN non esisteva al momento della copia Snapshot, il LUN non esisterà dopo il ripristino del volume. Eseguire l'override di questo controllo solo se si è certi che il ripristino delle LUN non influisca negativamente su nulla.</p>

Problema	Pass richiesto	Dettagli
I LUN presenti nella copia Snapshot del volume potrebbero non essere coerenti quando vengono ripristinati	No	<p>Durante la creazione della copia Snapshot, nel volume esistevano LUN diversi da quelli per cui era stata richiesta la copia Snapshot. Queste altre LUN potrebbero non trovarsi in uno stato coerente.</p> <p>Soluzione: Migrare i LUN non utilizzati dal database su un volume diverso o eliminare i LUN. Ciò non aiuta il processo di ripristino in cui il controllo non è riuscito, ma aiuta a ripristinare i backup futuri eseguiti dopo lo spostamento o l'eliminazione dei LUN.</p> <p>Se si esegue l'override di questo controllo, i LUN tornano allo stato incoerente in cui è stata eseguita la copia Snapshot. Eseguire l'override di questo controllo solo se si è certi che il ripristino delle LUN non influisca negativamente su nulla.</p>
Le nuove copie Snapshot hanno un clone del volume	Sì	<p>Sono stati creati cloni di copie Snapshot create dopo la richiesta di ripristino della copia Snapshot. Poiché un ripristino di un volume elimina le copie Snapshot successive e una copia Snapshot non può essere eliminata se dispone di un clone, non è possibile eseguire un ripristino di volume. Soluzione: Eliminare i cloni delle copie Snapshot successive.</p> <p>Impossibile eseguire l'override.</p>

Problema	Pass richiesto	Dettagli
Vengono montati backup più recenti	Sì	<p>Vengono montati i backup eseguiti dopo il ripristino del backup. Poiché un ripristino del volume elimina le copie Snapshot successive, una copia Snapshot non può essere eliminata se è dotata di un clone, un'operazione di montaggio del backup crea uno storage clonato e non può essere eseguito un ripristino del volume. Soluzione: Smontare il backup successivo o eseguire il ripristino da un backup eseguito dopo il backup montato.</p> <p>Impossibile eseguire l'override.</p>
Esistono cloni di backup più recenti	Sì	<p>I backup eseguiti dopo il ripristino sono stati clonati. Poiché un ripristino di un volume elimina le copie Snapshot successive e una copia Snapshot non può essere eliminata se dispone di un clone, non è possibile eseguire un ripristino di volume. Soluzione: Eliminare il clone del backup più recente o eseguire il ripristino da un backup eseguito dopo i backup che hanno dei cloni.</p> <p>Impossibile eseguire l'override.</p>

Problema	Pass richiesto	Dettagli
Le nuove copie Snapshot del volume vengono perse	No	<p>L'esecuzione di un ripristino del volume elimina tutte le copie Snapshot create dopo la copia Snapshot in cui viene ripristinato il volume. Se SnapManager è in grado di mappare una copia Snapshot successiva su un backup SnapManager nello stesso profilo, viene visualizzato il messaggio "i backup più recenti verranno liberati o cancellati". Se SnapManager non riesce a mappare una copia Snapshot successiva su un backup SnapManager nello stesso profilo, questo messaggio non viene visualizzato. Soluzione: Eseguire il ripristino da un backup successivo o eliminare le copie Snapshot successive.</p> <p>Può eseguire l'override.</p>

Problema	Pass richiesto	Dettagli
I backup più recenti verranno liberati o cancellati	No	<p>L'esecuzione di un ripristino del volume elimina tutte le copie Snapshot create dopo la copia Snapshot in cui viene ripristinato il volume. Pertanto, tutti i backup creati dopo il ripristino vengono cancellati o liberati. I backup successivi vengono eliminati nei seguenti scenari:</p> <ul style="list-style-type: none"> • Lo stato di backup non È PROTETTO • Retain.alwaysFreeExpiredBackups è falso in smo.config <p>I backup successivi vengono liberati nei seguenti scenari:</p> <ul style="list-style-type: none"> • Lo stato di backup è PROTETTO • Retain.alwaysFreeExpiredBackups è vero falso in smo.config <p>Soluzione: Eseguire il ripristino da un backup successivo oppure liberare o eliminare i backup successivi.</p> <p>Se si esegue l'override di questo controllo, i backup creati dopo il ripristino vengono cancellati o liberati.</p>

Problema	Pass richiesto	Dettagli
La relazione di SnapMirror per il volume viene persa	Sì (se RBAC è disattivato o non si dispone dell'autorizzazione RBAC)	<p>Il ripristino di un volume in una copia Snapshot precedente alla copia Snapshot di riferimento in una relazione SnapMirror distrugge la relazione. Risoluzione: Ripristino da un backup creato dopo la copia Snapshot di riferimento della relazione. In alternativa, interrompere manualmente la relazione di storage (quindi ricreare e basare nuovamente la relazione dopo il completamento del ripristino).</p> <p>Può eseguire l'override, se RBAC è attivato e si dispone dell'autorizzazione RBAC.</p>
La relazione SnapVault per il volume viene persa se si verifica il processo di ripristino rapido	Sì (se RBAC è disattivato o non si dispone dell'autorizzazione RBAC)	<p>Il ripristino di un volume in una copia Snapshot precedente alla copia Snapshot di riferimento in una relazione SnapVault distrugge la relazione. Risoluzione: Ripristino da un backup creato dopo la copia Snapshot di riferimento della relazione. In alternativa, interrompere manualmente la relazione di storage (quindi ricreare e basare nuovamente la relazione dopo il completamento del ripristino).</p> <p>Impossibile eseguire l'override se RBAC è attivato e si dispone dell'autorizzazione RBAC.</p>
I file NFS nel volume che non fanno parte dell'ambito di ripristino vengono ripristinati	No	<p>I file presenti nel volume del sistema di storage, che non sono visibili sull'host, vengono ripristinati se viene eseguito un ripristino del volume. Soluzione: Migrare i file non utilizzati dal database su un volume diverso o eliminare i file.</p> <p>Può eseguire l'override. Se si esegue l'override di questo errore di controllo, i LUN vengono cancellati.</p>

Problema	Pass richiesto	Dettagli
Esistono condivisioni CIFS per il volume	No	Il volume da ripristinare dispone di condivisioni CIFS. Altri host potrebbero accedere ai file nel volume durante il ripristino del volume. Soluzione: Rimuovere le condivisioni CIFS non necessarie. Può eseguire l'override.
Ripristino da una posizione alternativa	Sì	È stata fornita una specifica di ripristino per l'operazione di ripristino che specifica che i file devono essere ripristinati da una posizione alternativa. Solo le utility di copia lato host possono essere utilizzate per il ripristino da una posizione alternativa. Risoluzione: Nessuna. Impossibile eseguire l'override.
Il ripristino del file system lato storage non è supportato in un database RAC ASM	Sì	Impossibile eseguire l'override.

Recovery del backup

In SnapManager, è necessario eseguire contemporaneamente le operazioni di ripristino e ripristino. Non è possibile eseguire un'operazione di ripristino, quindi eseguire un'operazione di ripristino di SnapManager in un secondo momento.

In SnapManager 3.2 o versioni precedenti, è possibile utilizzare SnapManager per ripristinare e ripristinare il backup o SnapManager per ripristinare il backup e utilizzare un altro strumento, ad esempio Oracle Recovery Manager (RMAN), per ripristinare i dati. Poiché SnapManager è in grado di registrare i propri backup con RMAN, è possibile utilizzare RMAN per ripristinare e ripristinare il database con granularità più fini, come i blocchi. Questa integrazione combina i vantaggi della velocità e dell'efficienza dello spazio delle copie Snapshot con il livello di controllo ottimale per il ripristino mediante RMAN.



È necessario ripristinare un database prima di poterlo utilizzare. È possibile utilizzare qualsiasi strumento o script per ripristinare un database.

A partire da SnapManager 3.2 per Oracle, SnapManager consente il ripristino automatico dei backup del database utilizzando i backup del registro di archiviazione. Anche quando i backup del registro di archiviazione sono disponibili nella posizione esterna, SnapManager utilizza i backup del registro di archiviazione dalla posizione esterna per ripristinare i backup del database.

Se vengono aggiunti nuovi file di dati al database, Oracle consiglia di eseguire immediatamente un nuovo backup. Inoltre, se si ripristina un backup eseguito prima dell'aggiunta dei nuovi file di dati e si tenta di eseguire il ripristino a un punto successivo all'aggiunta dei nuovi file di dati, il processo di ripristino automatico

di Oracle potrebbe non riuscire, in quanto non è in grado di creare file di dati. Consultare la documentazione Oracle per il processo di ripristino dei file di dati aggiunti dopo un backup.

Stato del database necessario per il processo di ripristino

Lo stato del database da ripristinare dipende dal tipo di processo di ripristino che si desidera eseguire e dal tipo di file da includere.

La tabella seguente elenca lo stato in cui il database deve essere in base all'opzione di ripristino selezionata e al tipo di file che si desidera includere nel ripristino:

Tipo di ripristino	File inclusi	Stato del database per questa istanza	Stato del database per un'altra istanza (solo RAC)
Solo ripristino	File di controllo	Spegnere	Spegnere
File di sistema	Montare o spegnere	Montare o spegnere	Nessun file di sistema
Qualsiasi stato	Qualsiasi stato	Ripristino e ripristino	File di controllo
Spegnere	Spegnere	File di sistema	Montare
Montare o spegnere	Nessun file di sistema	Montare o aprire	Qualsiasi

Lo stato del database richiesto da SnapManager per un'operazione di ripristino dipende dal tipo di ripristino eseguito (file completi, parziali o di controllo). SnapManager non sposta il database in uno stato inferiore (ad esempio, da aperto a montaggio) a meno che non sia specificata l'opzione force.

Quali sono i piani di anteprima del ripristino

SnapManager fornisce piani di ripristino prima e dopo il completamento di un'operazione di ripristino. I piani di ripristino vengono utilizzati per visualizzare in anteprima, rivedere e analizzare i diversi metodi di ripristino.

Struttura del piano di ripristino

Il piano di ripristino è costituito dalle seguenti due sezioni:

- **Anteprima/Rivedi:** Questa sezione descrive come SnapManager ripristinerà (o ha ripristinato) ogni file.
- **Analisi:** Questa sezione descrive il motivo per cui alcuni meccanismi di ripristino non sono stati utilizzati durante l'operazione di ripristino.

La sezione Anteprima/Rivedi

Questa sezione mostra come ogni file sarà o è stato ripristinato. Quando si visualizza il piano di ripristino prima di un'operazione di ripristino, viene chiamato anteprima. Quando viene visualizzata dopo il completamento di un'operazione di ripristino, viene chiamata revisione.

L'esempio di anteprima seguente mostra che i file vengono ripristinati utilizzando il ripristino rapido basato su volume, il ripristino del file system lato storage e i metodi di ripristino del sistema lato storage. Per determinare

il motivo per cui tutti i file non vengono ripristinati utilizzando lo stesso metodo di ripristino, vedere la sezione analisi.

Preview:

The following files will be restored completely via: fast restore
+DG1/rac6/users.dbf

The following files will be restored completely via: storage side file system restore

+DG2/rac6/sysaux.dbf

+DG2/rac6/system.dbf

The following files will be restored completely via: storage side system restore

+DG2/rac6/undotbs1.dbf

+DG2/rac6/undotbs2.dbf

Ogni metodo di ripristino dispone di una sottosezione contenente informazioni sui file che possono essere ripristinati utilizzando tale metodo. Le sottosezioni vengono ordinate in base ai livelli di efficienza dei metodi di storage in diminuzione. Nell'esempio precedente, il metodo di ripristino rapido è più efficiente del metodo di ripristino del file system di storage e viene visualizzato per primo.

È possibile ripristinare un file con più metodi di ripristino. I metodi di ripristino multipli vengono utilizzati quando i LUN (Logical Unit Number) sottostanti utilizzati per un file system sono distribuiti tra diversi volumi del sistema di storage e alcuni volumi sono idonei per il ripristino del volume, mentre altri no. Se si utilizzano più metodi di ripristino per ripristinare lo stesso file, la sezione di anteprima sarà simile a quanto segue:

The following files will be restored via a combination of:
[fast restore, storage side file system restore. storage side system restore]

La sezione analisi

La sezione analisi illustra i motivi per cui alcuni meccanismi di ripristino non vengono utilizzati o non sono stati utilizzati. È possibile utilizzare queste informazioni per determinare i requisiti necessari per attivare meccanismi di ripristino più efficienti.

L'esempio seguente mostra una sezione di analisi:

Analysis:

The following reasons prevent certain files from being restored completely via: fast restore

- * LUNs present in snapshot of volume fas960:
 /vol/rac_6_asm_disks may not be consistent when reverted:
 [fas960:/vol/rac6_asm_disks/DG4D1.lun]
Mapped LUNs in volume fas960:/vol/rac_6_asm_disks
 not part of the restore scope will be reverted: [DG4D1.lun]

Files to restore:

- +DG2/rac6/sysaux.dbf
- +DG2/rac6/system.dbf
- +DG2/rac6/undotbs1.dbf
- +DG2/rac6/undotbs2.dbf

* Reasons denoted with an asterisk (*) are overridable.

Nell'esempio, il primo errore può essere sovrascritto utilizzando -FAST -override dall'interfaccia della riga di comando (CLI) o selezionando **Override** nell'interfaccia grafica utente (GUI). Il secondo errore relativo alle LUN mappate nel volume è obbligatorio e non sovrascrivibile.

Per risolvere i controlli, procedere come segue:

- Per risolvere un errore di controllo obbligatorio, modificare l'ambiente in modo che il controllo venga superato.
- Per risolvere un errore di controllo sovrascrivibile, è possibile modificare l'ambiente o eseguire l'override del controllo.

Tuttavia, è necessario prestare attenzione perché l'override del controllo può causare conseguenze indesiderate.

Visualizzazione in anteprima delle informazioni di ripristino del backup

È possibile visualizzare in anteprima le informazioni relative a un processo di ripristino del backup prima che si verifichi, per visualizzare le informazioni sull'idoneità al ripristino rilevate da SnapManager per Oracle nel backup. SnapManager analizza i dati del backup per determinare se il processo di ripristino può essere completato correttamente.

L'anteprima di ripristino fornisce le seguenti informazioni:

- Quale meccanismo di ripristino (ripristino rapido, ripristino del file system lato storage, ripristino del file lato storage o ripristino della copia del file lato host) può essere utilizzato per ripristinare ciascun file.
- Perché non sono stati utilizzati meccanismi più efficienti per ripristinare ciascun file, quando si specifica l'opzione -verbose.

Se si specifica l'opzione di anteprima nel comando di ripristino del backup, SnapManager non ripristina nulla, ma elenca i file da ripristinare e indica come verranno ripristinati.



È possibile visualizzare in anteprima tutti i tipi di meccanismi di ripristino. L'anteprima mostra informazioni su un massimo di 20 file.

1. Immettere il seguente comando: `smo backup restore -profile profile_name-label-label-complete -preview -verbose`

Ad esempio, immettere:

```
smo backup restore -profile targetdbl_prof1  
-label full_bkup_sales_nov_08 -complete -preview -verbose
```

L'esempio seguente mostra alcuni file ripristinati mediante il processo di ripristino della copia del file sul lato host e spiega anche perché alcuni file non possono essere ripristinati utilizzando l'opzione di ripristino rapido. Se si specifica l'opzione `-verbose`, SnapManager visualizza una sezione di anteprima e una sezione di analisi che spiegano il motivo per cui ciascun file non può essere ripristinato attraverso il processo di ripristino rapido.

PREVIEW:

The following files will be restored via host side file copy restore:

+DG2/sid/datafile10.dbf

+DG2/sid/datafile11.dbf

ANALYSIS:

The following reasons prevent certain files from being restored via fast restore:

Reasons:

Newer snapshots of /vol/volume2 have volume clones: SNAP_1

*Newer backups will be freed: nightly2, nightly3

Files to Restore:

/mnt/systemB/volume2/system.dbf

/mnt/systemB/volume2/users.dbf

/mnt/systemB/volume2/sysaux.dbf

/mnt/systemB/volume2/datafile04.dbf

/mnt/systemB/volume2/datafile05.dbf

The following reasons prevent certain files from being restored via fast restore:

Reasons:

* Newer snapshots of /vol/adm_disks will be lost: ADM_SNAP_5

* Luns present which were created after snapshot SNAP_0 was created:

/vol/adm_disks/disk5.lun

* Files not part of the restore scope will be reverted in file system:

+DG2

Files Not in Restore Scope: +DG2/someothersid/data01.dbf

+DG2/someothersid/data02.dbf

Files to Restore:

+DG2/sid/datafile08.dbf +DG2/sid/datafile09.dbf

+DG2/sid/datafile10.dbf +DG2/sid/datafile11.dbf

* Reasons denoted with an asterisk (*) are overridable.

2. Esaminare i motivi per cui non è possibile utilizzare altri processi di ripristino.
3. Avviare l'operazione di ripristino senza l'opzione -preview, se vengono visualizzati solo i motivi che possono essere sovrascrivibili.

È comunque possibile eseguire l'override dei controlli non obbligatori.

Ripristino dei backup mediante il ripristino rapido

È possibile forzare SnapManager per Oracle a utilizzare il processo SnapRestore basato su volume anziché altri processi di ripristino, se vengono soddisfatte tutte le condizioni di

idoneità obbligatorie per il ripristino rapido.

È possibile utilizzare il comando di backup restore con `-FAST`: `backup restore -fast [require | override | fallback | off]`

È possibile utilizzare l'opzione `-fast` solo se si desidera eseguire un ripristino completo di un backup completo. L'opzione `-FAST` include i seguenti parametri:

- **Richiedi:** Consente di eseguire un ripristino del volume se vengono soddisfatte tutte le condizioni di idoneità per il ripristino obbligatorio e non vengono rilevati controlli sovrascrivibili.

Se si specifica l'opzione `-fast`, ma non si specifica alcun parametro per `-FAST`, SnapManager utilizza il parametro-prescrivere come impostazione predefinita.

- **Override (Ignora):** Consente di ignorare i controlli di idoneità non obbligatori ed eseguire il ripristino rapido basato sul volume.
- **Fallback:** Consente di ripristinare il database utilizzando qualsiasi metodo determinato da SnapManager.

Se non si specifica `-FAST`, SnapManager utilizza il parametro `-fallback` come impostazione predefinita.

- **OFF:** Consente di evitare il tempo necessario per eseguire tutti i controlli di idoneità, per eseguire un processo di ripristino basato su file piuttosto che un processo di ripristino rapido.

Se il backup non supera i controlli di idoneità obbligatori, il ripristino rapido non può essere completato correttamente.

SnapManager esegue ripristini rapidi basati su volumi solo in ambienti basati su UNIX; SnapManager non esegue ripristini rapidi nell'ambiente Windows.

Durante l'esecuzione di VBSR sul backup del file di dati, se i file di dati e i file di log dell'archivio sono presenti nello stesso volume e se i file di log dell'archivio non sono presenti nel file system attivo, il ripristino e il ripristino del database hanno esito positivo. Tuttavia, le future istantanee del log di archiviazione vengono eliminate come parte del VBSR, con conseguente inserimento obsoleto del backup del log di archiviazione nel repository.

1. Immettere il seguente comando: `smo backup restore -profile profile_name-label label-complete-fast request-verbose`

```
smo backup restore -profile targetdb1_prof1
-label full_bkup_sales_nov_08 -complete -fast require -verbose
```

2. Esaminare i controlli di idoneità per il ripristino rapido.
3. Se il controllo di idoneità determina che nessun controllo obbligatorio ha avuto esito negativo, se è possibile ignorare determinate condizioni e se si desidera continuare il processo di ripristino, immettere il seguente comando: `Backup restore -fast override`

Informazioni correlate

[Creazione di script di pre-task, post-task e policy](#)

[Variabili disponibili negli script delle operazioni per l'operazione di ripristino](#)

Ripristino dei backup mediante Single file SnapRestore

È possibile ripristinare i backup utilizzando il metodo SFSR (Single file SnapRestore).

1. Creare un profilo dall'interfaccia grafica utente (GUI) di SnapManager.
2. Eseguire il backup del database utilizzando la GUI.
3. Scollegare i gruppi di servizi Oracle e NFS (Network file System) dai gruppi di servizi cluster e bloccarli.
4. Assicurarsi che la shell sicura (SSH) sia configurata tra gli host e SnapDrive per UNIX impostando l'opzione Secure-communication-between-nodes su on nel file snapdrive.conf.
5. Dalla GUI di SnapManager, eseguire il ripristino e il ripristino completi del backup utilizzando --alllogs.
6. Sbloccare i gruppi di servizi e collegarli nuovamente al gruppo di servizi del cluster.



Questa configurazione è applicabile solo quando si utilizza SnapDrive 4.1.1 D2 per UNIX e SnapDrive 4.2 per UNIX.

Se un'operazione di ripristino è seguita da un'altra operazione di ripristino, è possibile che la creazione della copia Snapshot di backup non riesca. Se si eseguono operazioni di ripristino successive entro il tempo specificato per il completamento di SFSR, SnapManager per Oracle risconterà errori di creazione delle copie Snapshot.

Per evitare errori di creazione delle copie Snapshot, assicurarsi che le operazioni di ripristino vengano eseguite dopo il periodo di tempo durante il quale SFSR è in corso.

A tale scopo, controllare lo stato del processo di split del clone del LUN immettendo il seguente comando dall'interfaccia della riga di comando del sistema di storage: `Rshfilernnamelun clone split statuslun-name`

Sample Output:

```
/vol/delaware_760gb/lun700gb (64% complete) ..
```



VBSR (Volume-Based SnapRestore) non è supportato sugli host Solaris che eseguono lo stack Veritas con ambienti SFRAC e VCS.

Ripristino dei backup sullo storage primario

È possibile utilizzare il comando di ripristino del backup per ripristinare un backup del database sullo storage primario.

SnapManager tenta di eseguire un ripristino rapido basato su volume per impostazione predefinita e fornisce informazioni sul controllo di idoneità. Se necessario, puoi ignorare alcuni controlli di idoneità. Se si è certi che un backup non può essere eseguito utilizzando un ripristino rapido, è possibile disattivare il controllo di idoneità del ripristino rapido ed eseguire un ripristino basato su file.

È possibile utilizzare le opzioni del comando di ripristino del backup per specificare se SnapManager deve ripristinare tutto o parte del backup. SnapManager consente inoltre di ripristinare i file di controllo insieme ai file di dati o agli spazi delle tabelle dai backup in un'operazione con un singolo utente. È possibile includere -controlfile with -complete per ripristinare i file di controllo insieme a tablespaces e file di dati.

È possibile selezionare una delle seguenti opzioni per ripristinare il backup:

Se si desidera ripristinare...	Utilizzare...
L'intero backup con tutti i tablespaces e i file di dati	-completo
L'elenco di tablespaces specifici	-tablespaces
File di dati specifici	-file
Solo i file di controllo	-controlfiles
Tablespace, file di dati e file di controllo	-complete -controlfiles

È anche possibile ripristinare il backup da una posizione alternativa specificando -restorespec.

Se si include -recover, è possibile ripristinare il database per:

- L'ultima transazione che si è verificata nel database (tutti i registri)
- Data e ora specifiche
- Un numero SCN (System Change Number) Oracle specifico
- L'ora del backup (nessun registro)
- Solo ripristino



Sia il ripristino di data e ora che il ripristino SCN sono ripristini point-in-time.

SnapManager (3.2 o versione successiva) consente di ripristinare automaticamente i backup del database ripristinati utilizzando i file di registro dell'archivio. Anche se i file di log dell'archivio sono disponibili nella posizione esterna, se si specifica l'opzione -recover-from-location, SnapManager utilizza i file di log dell'archivio dalla posizione esterna per ripristinare i backup del database ripristinati.

SnapManager fornisce la posizione esterna a Oracle. Tuttavia, Oracle non identifica i file dalla destinazione esterna. Questo comportamento si verifica nella destinazione dell'area di ripristino flash e nella destinazione di Automatic Storage Management (ASM). Si tratta di problemi con Oracle e la soluzione è avere sempre il backup dei file di log dell'archivio in tali layout di database.

Se viene fornita una data o un numero SCN incoerente, il ripristino si interrompe all'ultimo punto coerente recuperato con il messaggio di errore Recovery succeeded (Ripristino riuscito), ma insufficiente. È necessario eseguire manualmente il ripristino in uno stato coerente.

Per il ripristino quando non vengono applicati registri, SnapManager esegue il ripristino fino all'ultimo numero di configurazione del file di registro dell'archivio creato durante il backup. Se il database è coerente fino a quando non viene visualizzato questo SCN, il database viene aperto correttamente. Se a questo punto il database non è coerente, SnapManager tenta comunque di aprire il database, che verrà aperto correttamente, se il database è già coerente.



SnapManager non supporta il ripristino dei backup solo log dell'archivio.

Se la destinazione del log di archivio su un punto di montaggio NFS non è uno storage con funzionalità

Snapshot, SnapManager consente di ripristinare i backup del database ripristinati utilizzando il profilo. Prima di eseguire operazioni SnapManager su storage non Snapshot, aggiungere le destinazioni per `archiviLogs.exclude` in `smo.config`.

Prima di creare un profilo, è necessario impostare il parametro `exclude`. Solo dopo aver impostato il parametro `exclude` nel file di configurazione SnapManager, la creazione del profilo ha esito positivo.



Se il database è uno storage non compatibile con Snapshot su un gruppo di dischi ASM e quando il database è selezionato come destinazione del log di archiviazione, SnapManager non supporta il ripristino dei backup mediante il profilo.

Se il backup è già stato montato, SnapManager non lo installa di nuovo e utilizza il backup già montato. Se il backup viene montato da un altro utente e l'utente corrente non ha accesso al backup precedentemente montato, gli altri utenti devono fornire le autorizzazioni. Tutti i file di log dell'archivio dispongono dei permessi di lettura per i proprietari dei gruppi; l'utente corrente potrebbe non ottenere i permessi, se il backup viene montato da un gruppo di utenti diverso. Gli utenti possono assegnare manualmente i permessi ai file di registro dell'archivio montati e riprovare il ripristino o il ripristino.

Ripristino dei backup del database in un ambiente RAC (Real Application Clusters)

Durante il ripristino dei backup del database in un ambiente RAC, quando il file di log dell'archivio richiesto non viene trovato, Oracle richiede i file di log dell'archivio e passa da un thread diverso al numero di cambiamento nel database RAC. SnapManager per Oracle cerca di ripristinare il database come uno sforzo ottimale. Il ripristino corretto dei backup del database nell'ambiente RAC dipende dalla disponibilità dei file di log dell'archivio nei backup.

Il meccanismo di ripristino consigliato per il database RAC è il seguente:

- Assicurarsi che tutti i file di log dell'archivio siano disponibili nei backup o che tutti i file di log dell'archivio siano disponibili in una destinazione di log dell'archivio esterno.
- Se vengono fornite più destinazioni di log di archiviazione esterne, è possibile sovrapporre i file di log di archiviazione specificando le destinazioni di log di archiviazione esterne per tutti i thread.

Ad esempio, la posizione del log di archiviazione esterno - posso avere da 1 a 100 file di log di archiviazione, la posizione del log di archiviazione esterno - II può avere da 98 a 200 file di log di archiviazione e la posizione del log di archiviazione esterno - III può avere da 198 a 300 file di log di archiviazione.

- Mentre si eliminano i file di log dell'archivio, invece di eliminare tutti i file di log dell'archivio, è possibile eliminare i file di log dell'archivio fino a SCN o data, in modo che i backup possano avere gli stessi file di log dell'archivio.

È possibile specificare l'opzione `-dump` come parametro facoltativo per raccogliere i file dump dopo l'operazione di ripristino riuscita o non riuscita.

1. Immettere il seguente comando: `smo backup restore -profile profile_name-label label-complete-recover -alllogs [-recover-from-locationpath [,path2]]-dump-verbose`

```
backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 - complete -recover -alllogs -verbose
```

2. Per ripristinare i dati per diversi scenari, completare una delle seguenti operazioni:

Se si desidera ripristinare...	Esempio di comando
<p>Database completo senza file di controllo e ripristino a un numero SCN specifico (3794392). In questo caso, i file di controllo correnti esistono, ma tutti i file di dati vengono danneggiati o persi. Ripristinare e ripristinare il database da un backup online completo esistente a un punto immediatamente precedente a quello SCN.</p>	<pre>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -until 3794392 -verbose</pre>
<p>Completa il database senza file di controllo e ripristina fino a data e ora.</p>	<pre>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -until 2008-09-15:15:29:23 -verbose</pre>
<p>Completa il database senza file di controllo e ripristina fino a data e tempo. In questo caso, i file di controllo correnti esistono, ma tutti i file di dati vengono danneggiati o persi oppure si è verificato un errore logico dopo un determinato periodo di tempo. Ripristinare e ripristinare il database da un backup online completo esistente a una data e un'ora immediatamente prima del punto di errore.</p>	<pre>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -until "2008-09-15:15:29:23" -verbose</pre>
<p>Database parziale (uno o più file di dati) senza file di controllo e ripristino utilizzando tutti i registri disponibili. In questo caso, esistono i file di controllo correnti, ma uno o più file di dati vengono danneggiati o persi. Ripristinare questi file di dati e ripristinare il database da un backup online completo esistente utilizzando tutti i registri disponibili.</p>	<pre>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -files /u02/oradata/sales02.dbf /u02/oradata/sales03.dbf /u02/oradata/sales04.dbf -recover -alllogs -verbose</pre>
<p>Database parziale (uno o più tablespaces) senza file di controllo e ripristino utilizzando tutti i log disponibili. In questo caso, esistono i file di controllo correnti, ma uno o più tablespaces vengono eliminati o uno o più file di dati appartenenti allo spazio di tabella vengono danneggiati o persi. Ripristinare questi spazi delle tabelle e ripristinare il database da un backup online completo esistente utilizzando tutti i registri disponibili.</p>	<pre>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -tablespaces users -recover -alllogs -verbose</pre>

Se si desidera ripristinare...	Esempio di comando
Controllare solo i file e ripristinare utilizzando tutti i log disponibili. In questo caso, i file di dati esistono, ma tutti i file di controllo vengono danneggiati o persi. Ripristinare solo i file di controllo e ripristinare il database da un backup online completo esistente utilizzando tutti i registri disponibili.	<code>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -controlfiles -recover -alllogs -verbose</code>
Completa il database senza file di controllo e ripristina utilizzando i file di controllo di backup e tutti i log disponibili. In questo caso, tutti i file di dati vengono danneggiati o persi. Ripristinare solo i file di controllo e ripristinare il database da un backup online completo esistente utilizzando tutti i registri disponibili.	<code>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -using-backup -controlfile -recover -alllogs -verbose</code>
Ripristinare il database ripristinato utilizzando i file di log dell'archivio dalla posizione del log dell'archivio esterno.	<code>backup restore smo -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -using-backup -controlfile -recover -alllogs -recover-from-location /user1/archive -verbose</code>

3. Esaminare i controlli di idoneità per il ripristino rapido.

Immettere il seguente comando: `smo backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -alllogs -recover-from-location /user1/archive -verbose`

- Se il controllo di idoneità indica che non sono stati eseguiti controlli obbligatori e se è possibile ignorare determinate condizioni e se si desidera continuare il processo di ripristino, immettere quanto segue:
`Backup restore -fast override`
- Specificare le posizioni esterne del log di archiviazione utilizzando l'opzione `-recover-from-location`.

Informazioni correlate

[Ripristino dei backup mediante il ripristino rapido](#)

[Ripristino dei backup da una posizione alternativa](#)

[Il comando di ripristino del backup smo](#)

Esecuzione del recovery a livello di blocco con Oracle Recovery Manager (RMAN)

È possibile configurare SnapManager per catalogare i propri backup in Recovery Manager (RMAN), uno strumento Oracle, in modo da poter eseguire un ripristino a livello di blocco utilizzando RMAN. RMAN può utilizzare i file di controllo del database o un database del catalogo di ripristino separato come repository.

- Per eseguire un backup offline completo utilizzando SnapManager, immettere il seguente comando:

`backup smo create -offline-full-profileprofile_name-labelbackup_label_name-verbose`

Dove:

- profile_name è il nome del profilo associato al backup
- nome_etichetta_backup è il nome dell'etichetta di backup

```
smo backup create -offline -full -profile profile_monthly
-label full_backup -verbose

+
SMO-07109 [INFO ]: Cataloguing all files in backup set with RMAN
TAG=SMC_full_backup_1158773581857, RMAN=ES0/controlfile.
...
SMO-13037 [INFO ]: Successfully completed operation: Backup
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:02:20.506
Operation Id [ff8080810dcc47e3010dcc47eb7a0001] succeeded.
+
```

1. Per verificare che il backup sia catalogato con RMAN, dall'host del database immettere il seguente comando al prompt di RMAN:

```
list datafilecopy tag tag tag_name;
```

```

RMAN> list datafilecopy tag SMO_full_backup_1158773581857;

Recovery Manager: Release 10.2.0.1.0 - Production on Wed Sep 20 10:33:41
2008
Copyright (c) 1982, 2008, Oracle. All rights reserved.
using target database control file instead of recovery catalog
List of Datafile Copies
Key File S Completion Time Ckp SCN Ckp Time Name
-----
335 1 A 20-SEP-08 1347825 20-SEP-08
/opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
/system01.dbf
336 2 A 20-SEP-08 1347825 20-SEP-08
/opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
/undotbs01.dbf
334 3 A 20-SEP-08 1347825 20-SEP-08
/opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
/sysaux01.dbf
333 4 A 20-SEP-08 1347825 20-SEP-08
/opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
/user01.dbf
337 5 A 20-SEP-08 1347825 20-SEP-08
RMAN>

```

2. Per verificare il database e determinare se i blocchi sono corrotti, immettere il seguente comando:

```
dbv FILE=user01.dbf
```

Il seguente output mostra che due pagine sono corrotte:

```

DBVERIFY: Release 10.2.0.1.0 - Production on Wed Sep 20 13:35:44 2006
Copyright (c) 1982, 2005, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = user01.dbf
Page 625 is marked corrupt
Corrupt block relative dba: 0x01400271 (file 5, block 625)
Bad header found during dbv:
Data in bad block:
type: 240 format: 6 rdba: 0xed323b81
last change scn: 0x6f07.faa74628 seq: 0x87 flg: 0x02
spare1: 0x60 spare2: 0x5 spare3: 0xef7d
consistency value in tail: 0xa210fe71
check value in block header: 0x13c7
block checksum disabled...
Page 627 is marked corrupt
Corrupt block relative dba: 0x01400273 (file 5, block 627)
Bad header found during dbv:
Data in bad block:
type: 158 format: 7 rdba: 0x2101e16d
last change scn: 0xe828.42414628 seq: 0xb4 flg: 0xff
spare1: 0xcc spare2: 0x81 spare3: 0x8665
consistency value in tail: 0x46d20601
check value in block header: 0x1a84
computed block checksum: 0x6c30
DBVERIFY - Verification complete
Total Pages Examined : 1280
Total Pages Processed (Data) : 1123
Total Pages Failing (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing (Index): 0
Total Pages Processed (Other): 34
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
Total Pages Empty : 120
Total Pages Marked Corrupt: 2
Total Pages Influx : 0
Highest block SCN : 1337349 (0.1337349)

```

3. Per rendere accessibili i file del backup sull'host e su RMAN, montare il backup utilizzando il seguente comando:

```
smo backup mount -profileprofile_name-labellabel-verbose
```

```

smo backup mount -profile SALES1 -label full_backup -verbose

SMO-13046 [INFO ]: Operation GUID 8abc013111b9088e0111b908a7560001
starting on Profile SALES1
SMO-08052 [INFO ]: Beginning to connect mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/logs from
snapshot SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_logs.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/logs from
snapshot SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_logs.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/data from
snapshot SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_data.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/data from
snapshot SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_data.
SMO-08053 [INFO ]: Finished connecting mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001.
SMO-13037 [INFO ]: Successfully completed operation: Backup Mount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:01:00.981
Operation Id [8abc013111b9088e0111b908a7560001] succeeded.

```

4. Per ripristinare i blocchi, in RMAN, immettere il seguente comando:

```
blockrecover datafile '/mountpoint/path/file.dbf' block_id, dal tag backup_rman_tag
```

```

RMAN> blockrecover datafile
'/mnt/ssys1/Host4_ES0/file01.dbf' block 625, 626, 627
from tag SMO_full_backup_1158773581857;

Starting blockrecover at 20-SEP-08 using target database control file
instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=153 devtype=DISK
channel ORA_DISK_1: restoring block(s) from datafile copy
/opt/NetApp/smo/mnt/_mnt_ssys1_Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47
e3010dcc47eb7a0001/user01.dbf
starting media recovery
media recovery complete, elapsed time: 00:00:01
Finished blockrecover at 20-SEP-08

```

5. Per verificare se i blocchi sono stati riparati, utilizzare il seguente comando:

```
dbv FILE=nomefile.dbf
```

Il seguente output mostra che nessuna pagina è corrotta:

```

dbv FILE=user01.dbf

DBVERIFY: Release 10.2.0.1.0 - Production on Wed Sep 20 13:40:01 2008
Copyright (c) 1982, 2008, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = user01.dbf
DBVERIFY - Verification complete
Total Pages Examined : 1280
Total Pages Processed (Data) : 1126
Total Pages Failing (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing (Index): 0
Total Pages Processed (Other): 34
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
Total Pages Empty : 120
Total Pages Marked Corrupt : 0
Total Pages Influx : 0
Highest block SCN : 1337349 (0.1337349)

```

Tutti i blocchi corrotti sono stati riparati e ripristinati.

Ripristinare i file da una posizione alternativa

SnapManager consente di ripristinare i file di dati e i file di controllo da una posizione

diversa da quella delle copie Snapshot nel volume originale.

La posizione originale corrisponde alla posizione del file sul file system attivo al momento del backup. La posizione alternativa è la posizione da cui verrà ripristinato un file.

È possibile ripristinare i seguenti dati da una posizione alternativa:

- I file di dati da un file system intermedio a un file system attivo
- I blocchi di dati da un dispositivo raw intermedio a un dispositivo raw attivo

Il recovery è automatizzato da SnapManager. Quando si ripristinano i file da posizioni esterne, SnapManager utilizza il comando `recovery automatic from location`.

SnapManager utilizza anche Oracle Recovery Manager (RMAN) per ripristinare i file. I file da ripristinare devono essere riconoscibili da Oracle. I nomi dei file devono essere nel formato predefinito. Durante il ripristino dall'area di ripristino flash, SnapManager fornisce il percorso tradotto a Oracle. Oracle, tuttavia, non esegue il ripristino dall'area di ripristino flash perché non è in grado di generare il nome file corretto. Idealmente, l'area di ripristino flash è una destinazione destinata a funzionare con RMAN.

Informazioni correlate

[Creazione di specifiche di ripristino](#)

Ripristinare i backup da una panoramica di posizione alternativa

Per ripristinare un backup del database da una posizione alternativa, attenersi alla seguente procedura, ciascuna delle quali è descritta più avanti in questa sezione.

- Eseguire una delle seguenti operazioni, a seconda del layout del database e dei fattori da ripristinare:
 - Ripristinare i file di dati richiesti da nastro, SnapVault, SnapMirror o qualsiasi altro supporto su qualsiasi file system montato sull'host del database.
 - Ripristinare il file system richiesto e montarlo sull'host del database.
 - Connettersi ai dispositivi raw richiesti presenti nell'host locale.
- Creare un file XML (Extensible Markup Language) con specifica di ripristino che includa le mappature richieste da SnapManager per il ripristino dalla posizione alternativa alla posizione originale. Salvare il file in una posizione a cui SnapManager può accedere.
- Utilizzare SnapManager per ripristinare e ripristinare i dati utilizzando il file XML delle specifiche di ripristino.

Ripristino dei dati dai file

Prima di eseguire il ripristino da una posizione alternativa, è necessario ripristinare i file necessari da qualsiasi supporto di storage e ripristinare i file da applicazioni come SnapVault o SnapMirror su un file system montato sull'host locale.

È possibile utilizzare l'operazione di ripristino da una posizione alternativa per copiare i file da un file system alternativo a un file system attivo.

È necessario specificare le posizioni alternative da cui ripristinare i file originali creando una specifica di ripristino.

Ripristino dei dati dal file system

Prima di ripristinare i dati da una posizione alternativa, è necessario ripristinare il file system necessario e montarlo sull'host locale.

È possibile richiamare l'operazione di ripristino da una posizione alternativa per copiare i file da file system alternativi a file system attivi.

Per eseguire questa operazione, è necessario specificare i punti di montaggio alternativi da cui ripristinare i punti di montaggio originali e i nomi delle copie Snapshot originali creando un file di specifica di ripristino.



Il nome della copia Snapshot è un componente necessario perché lo stesso file system potrebbe essere bloccato più volte in una singola operazione di backup (ad esempio, una volta per i file di dati e una volta per il file di registro).

Per la gestione automatica dello storage (ASM), il nome del gruppo di dischi deve essere lo stesso del gruppo di dischi clonato da SnapManager per registrare il backup con Oracle Recovery Manager (RMAN). Questo nome può essere ottenuto visualizzando le proprietà di backup.

Informazioni correlate

[Creazione di specifiche di ripristino](#)

Ripristino dei dati dai dispositivi raw

Prima di eseguire il ripristino da una posizione alternativa, è necessario connettersi ai dispositivi raw necessari presenti sull'host locale.

È possibile richiamare il ripristino da un'operazione di posizione alternativa per copiare i blocchi di dati da dispositivi raw alternativi a dispositivi raw attivi. Per eseguire questa operazione, è necessario specificare il dispositivo raw alternativo da cui ripristinare il dispositivo raw originale creando una specifica di ripristino.

Informazioni correlate

[Creazione di specifiche di ripristino](#)

Creazione di specifiche di ripristino

Il file delle specifiche di ripristino è un file XML che contiene le posizioni originale e alternativa da cui è possibile ripristinare il file. SnapManager utilizza questo file di specifica per ripristinare i file dalla posizione specificata.

È possibile creare il file delle specifiche di ripristino utilizzando qualsiasi editor di testo. È necessario utilizzare un'estensione .xml per il file.

1. Aprire un file di testo.
2. Inserire il seguente indirizzo: `<restore-specification xmlns="http://www.netapp.com" class="bare">http://www.netapp.com`
3. Inserire le informazioni di mappatura dei file utilizzando il formato mostrato nell'esempio seguente:

```
<file-mapping>
  <original-location>/path/dbfilename.dbf</original-location>
  <alternate-location>/path/dbfilename1.dbf</alternate-location>
</file-mapping>
```

La mappatura file specifica da dove viene ripristinato un file. La posizione originale è la posizione del file sul file system attivo al momento del backup. La posizione alternativa è la posizione da cui viene ripristinato il file.

4. Inserire le informazioni di mappatura del file system montato utilizzando il formato mostrato nell'esempio:

```
<mountpoint-mapping>
  <original-location>/path/db_name</original-location>
  <snapname>snapname</snapname>
  <alternate-location>/path/vaultlocation</alternate-location>
</mountpoint-mapping>
<mountpoint-mapping>
  <original-location>+DiskGroup_1</original-location>
  <snapname>snapname</snapname>
  <alternate-location>+DiskGroup_2</alternate-location>
</mountpoint-mapping>
```

Mountpoint si riferisce al percorso di directory (/mnt/myfs/) o a un punto di montaggio del gruppo di dischi ASM (Automatic Storage Management) (ad esempio +MY_DG). La mappatura del punto di montaggio specifica il punto di montaggio da cui vengono ripristinati i file. La posizione originale è la posizione del punto di montaggio nel file system attivo al momento del backup. La posizione alternativa è il punto di montaggio da cui vengono ripristinati i file nella posizione originale. Snapname è il nome della copia Snapshot in cui è stato eseguito il backup dei file originali.

Per ASM, il nome del gruppo di dischi deve essere lo stesso del gruppo di dischi clonato da SnapManager per registrare il backup con RMAN. Questo nome può essere ottenuto visualizzando le proprietà di backup.



Il nome della copia Snapshot è un componente necessario perché lo stesso file system può essere utilizzato più volte in una singola operazione di backup (ad esempio, una volta per i file di dati e una volta per i registri).

5. Inserire tag e posizioni di mappatura raw dei dispositivi utilizzando il formato mostrato nell'esempio:

```
<raw-device-mapping>
  <original-location>/path/raw_device_name</original-location>
  <alternate-location>/path/raw_device_name</alternate-location>
</raw-device-mapping>
```

Il mapping raw dei dispositivi specifica la posizione da cui viene ripristinato un dispositivo raw.

6. Inserire il seguente indirizzo: </restore-specification>

7. Salvare il file come file .xml e chiudere la specifica.

Esempio di ripristino delle specifiche

L'esempio seguente mostra la struttura delle specifiche di ripristino:

```
<?xml version="1.0" encoding="UTF-8"?>
<restore-specification xmlns="http://www.netapp.com">
<!-- "Restore from file(s)" -->
    <file-mapping>
        <original-location>/mnt/pathname/dbname/users01.dbf</original-
location>
        <alternate-location>/mnt/vault/users01.dbf</alternate-location>
    </file-mapping>
<!-- "Restore from host mounted file system(s)" -->
    <mountpoint-mapping>
        <original-location>/mnt/pathname/dbname/fs</original-location>
        <snapname>Snapshotname</snapname>
        <alternate-location>/mnt/vaultlocation</alternate-location>
    </mountpoint-mapping>
<!-- "Restore from ASM mounted file system(s)" -->
    <mountpoint-mapping>
        <original-location>+DISKGROUP_1</original-location>
        <snapname>snapshotname</snapname>
        <alternate-location>+DISKGROUP_2</alternate-location>
    </mountpoint-mapping>
<!-- "Restore from raw device" -->
    <raw-device-mapping>
        <original-location>/pathname/devicename</original-location>
        <alternate-location>/pathname/devicename</alternate-location>
    </raw-device-mapping>
</restore-specification>
```

Ripristino dei backup da una posizione alternativa

È possibile ripristinare i backup da una posizione alternativa per ripristinare i file di dati da un file system intermedio a un file system attivo o per ripristinare i blocchi di dati da un dispositivo raw intermedio a un dispositivo raw attivo.

- Creare un file XML con specifica di ripristino e specificare il tipo di metodo di ripristino che si desidera utilizzare.

È possibile utilizzare il comando `smo backup restore` e specificare il file XML delle specifiche di ripristino creato per ripristinare il backup da una posizione alternativa.

1. Immettere il seguente comando: `smo backup restore -profileprofile-label-label-complete-alllogs -restorespecrestorespec`

Backup del database di cloning

Se si clona un database, è possibile eseguire attività come il test di un aggiornamento a un database senza influire sul database in produzione, duplicare un'installazione master su diversi sistemi di formazione o duplicare un'installazione master come installazione di base su altri server con requisiti simili.

È possibile eseguire le seguenti attività relative alla clonazione:

- Clonare un database da un backup esistente.
- Clonare un database nello stato corrente, che consente di creare il backup e il clone in un'unica procedura.
- Clonare un backup protetto sullo storage secondario o anche terzo.
- Clonare un database e utilizzare script plug-in personalizzati, che vengono eseguiti prima o dopo l'operazione di clonazione.
- Clonare un database sullo stesso host su cui risiede il database.
- Clonare un database utilizzando i file di log dell'archivio dalla posizione del log dell'archivio esterno.
- Clonare un database in un host alternativo.
- Clonare un database RAC.
- Visualizza un elenco di cloni.
- Visualizza informazioni dettagliate sui cloni.
- Eliminare i cloni.

Cos'è Cloning

È possibile clonare un database per creare una replica esatta del database originale. È possibile creare il clone da un backup completo o dallo stato corrente del database.

Di seguito sono riportati alcuni dei vantaggi della creazione di un clone mediante SnapManager:

Vantaggi	Dettagli
Velocità	L'operazione di clonazione SnapManager utilizza la funzione FlexClone disponibile con Data ONTAP. Ciò consente di clonare rapidamente grandi volumi di dati.
Efficienza dello spazio	Quando si crea un clone utilizzando SnapManager, lo spazio è necessario solo per le modifiche tra il backup e il clone. Un clone di SnapManager è una copia Snapshot scrivibile del database originale e può crescere in base alle esigenze. Al contrario, un clone fisico del database richiede uno spazio sufficiente per copiare l'intero database.

Vantaggi	Dettagli
Copia virtuale	È possibile utilizzare il database clonato come se fosse il database originale. Ad esempio, è possibile utilizzare un clone per test, verifiche di piattaforme e aggiornamenti, simulazioni multiple su un set di dati di grandi dimensioni e test e staging della sede remota. Le modifiche apportate al clone non influiscono sul database originale. Una volta clonato il database, il database clonato è completamente operativo.
Semplicità	È possibile clonare un database su qualsiasi host utilizzando i comandi SnapManager.

È possibile clonare un backup sullo storage primario (locale) o su un backup protetto sullo storage secondario (remoto). Tuttavia, non è possibile clonare un backup se l'operazione di backup è in corso o se il backup è stato trasferito allo storage secondario.

Prima di clonare un database, è necessario assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Assicurarsi che la directory [/etc]/var/opt/oracle/oratab non contenga una voce che punta all'identificatore del sistema di destinazione.
- Eliminare il file <SID>.ora spfilserie da €ORACLE_HOME/dbs.
- Eliminare il file init <SID>.ora da €ORACLE_HOME/dbs.
- Eliminare le destinazioni di dump Oracle specificate nel file di specifica del clone.
- Eliminare i file di controllo Oracle specificati nel file di specifica del clone.
- Eliminare i file di log di ripristino Oracle specificati nel file di specifica del clone.

È necessario assegnare al clone un nuovo identificatore di sistema. Non è possibile eseguire contemporaneamente due database con lo stesso identificatore di sistema sullo stesso host. È possibile avere un clone su un host diverso utilizzando lo stesso identificatore di sistema. È possibile assegnare un'etichetta al clone o lasciare che SnapManager crei un'etichetta utilizzando l'identificatore di sistema, la data e l'ora di creazione del clone.

Quando si inserisce un'etichetta, non includere spazi o caratteri speciali.

Nell'ambito del processo di cloning, SnapManager crea i file e i parametri Oracle necessari per il database clonato. Un esempio di un file Oracle necessario è inatit <SID>.ora.

Quando si clona un database, SnapManager crea un nuovo file init <SID>.ora per il database nella directory €ORACLE_HOME/dbs.

Quando SnapManager clona lo storage per un database, crea anche un nuovo punto di montaggio del file system, ma non modifica la struttura della directory sotto il punto di montaggio dall'interfaccia CLI di SnapManager. Tuttavia, dalla GUI di SnapManager, è possibile modificare la struttura della directory e i metadati del file system.

Oracle 11g in un ambiente Direct NFS (DNFS) consente una configurazione aggiuntiva dei punti di montaggio, ad esempio percorsi multipli per il bilanciamento del carico nel file oranfstab. SnapManager non modifica questo file, pertanto tutte le proprietà aggiuntive che si desidera utilizzare per un clone devono essere aggiunte manualmente al file oranfstab dopo la clonazione con SnapManager.

È possibile clonare un database RAC (Real Application Cluster) e un database non in cluster. Un clone RAC viene avviato come singolo database.

È possibile clonare un backup del database sull'host in cui risiede il database o su un host alternativo.

È inoltre possibile clonare un database ASM su un host remoto. Durante questa operazione, è necessario assicurarsi che l'istanza di ASM sia in esecuzione sull'host remoto.

Se il database clonato utilizzava una spfile, SnapManager crea una spfile per il clone. Il file viene inserito nella directory Oracle_HOME/dbs e viene creata la struttura di directory per i file di diagnostica. Il nome del file è spfile <SID>.ora.

Metodi di cloning

È possibile clonare un database utilizzando uno dei due metodi. Il metodo scelto influisce sull'operazione di creazione del clone.

La tabella seguente descrive i metodi di cloning e il loro effetto sull'operazione di creazione del clone e la relativa opzione -Reserve. È possibile clonare un LUN utilizzando uno dei due metodi.

Metodo di cloning
Descrizione
clonare create -reserve
Cloning del LUN
Viene creato un nuovo LUN clone all'interno dello stesso volume.
Quando l'opzione -Reserve for a LUN (riserva per LUN) è impostata su yes (sì), lo spazio viene riservato alle dimensioni del LUN completo all'interno del volume.
Cloning di volumi
Viene creato un nuovo FlexClone e il LUN clone esiste all'interno del nuovo volume clone. Utilizza la tecnologia FlexClone.
Quando l'opzione -Reserve per un volume è impostata su yes, lo spazio viene riservato per l'intera dimensione del volume all'interno dell'aggregato.

Creazione di specifiche di cloni

SnapManager per Oracle utilizza un file XML di specifica del clone, che include mappature, opzioni e parametri da utilizzare nell'operazione del clone. SnapManager utilizza queste informazioni per determinare dove posizionare i file cloni e come gestire le informazioni diagnostiche, i file di controllo, i parametri e così via.

È possibile creare il file di specifica del clone utilizzando l'interfaccia grafica utente (GUI), l'interfaccia della riga di comando (CLI) o un editor di testo di SnapManager.

Quando si crea il file di specifica del clone utilizzando un editor di testo, è necessario salvarlo come file .xml. È possibile utilizzare questo file XML per altre operazioni di clonazione.

È inoltre possibile creare un modello di specifica clone e personalizzarlo. È possibile utilizzare il comando modello clone smo oppure, nella GUI, utilizzare la procedura guidata Clone.

SnapManager per Oracle aggiunge una stringa di versione a qualsiasi modello di specifica clone generato. SnapManager per Oracle presuppone la versione più recente per qualsiasi file di specifica clone privo di stringa di versione.

Se si desidera eseguire la clonazione remota, non modificare le posizioni predefinite dei file di dati, ripristinare i file di log e i file di controllo nel file di specifica del clone. Se si modifica la posizione predefinita, SnapManager non crea il clone o il clone su un database che non supporta la funzionalità Snapshot. Pertanto, la creazione automatica del profilo non riesce.



Sebbene le informazioni relative al punto di montaggio e al gruppo di dischi ASM siano modificabili dalla GUI, è possibile modificare solo il nome del file e non le posizioni dei file.

È possibile eseguire un'attività più volte, con combinazioni di parametri e valori uguali o diverse.

1. Aprire un file di testo e inserire il testo come illustrato nell'esempio seguente:

```
<clone-specification xmlns="http://www.example.com">
  <storage-specification/>
  <database-specification/>
</clone-specification>
```

2. Nel componente delle specifiche dello storage, inserire i punti di montaggio per i file di dati.

La specifica dello storage elenca le posizioni per il nuovo storage creato per il clone, come ad esempio i punti di montaggio dei file di dati e i dispositivi raw. Questi elementi devono essere mappati dall'origine alla destinazione.

Nell'esempio seguente viene visualizzata la sintassi del punto di montaggio del file di dati utilizzata nella specifica del clone:

```
<mountpoint>
  <source>/mnt/path/source_data file_mountpoint</source>
  <destination>/mnt/path/target_data file_mountpoint</destination>
</mountpoint>
```

3. Facoltativo: Se si dispone di un dispositivo raw sull'origine, è necessario specificare il percorso del dispositivo raw sull'origine, quindi specificare la destinazione `auto-generation="true"` per la destinazione.

A differenza del file di mappatura dei cloni delle versioni precedenti di SnapManager per Oracle, non è possibile specificare una posizione per il dispositivo raw sulla destinazione. SnapManager per Oracle sceglierà il nome del dispositivo successivo disponibile per il dispositivo raw clonato.

Nell'esempio seguente viene visualizzata la sintassi raw del dispositivo utilizzata nella specifica del clone:

```
<raw-device>
  <source>/dev/raw/raw1</source>
  <destination auto-generate="true"/>
</raw-device>
```

4. Nel componente delle specifiche del database, identificare le informazioni del file di controllo come elenco dei file di controllo che si desidera creare per il clone.

La specifica del database specifica le opzioni del database per il clone, ad esempio file di controllo, log di ripristino, log di archiviazione e parametri Oracle.

Nell'esempio seguente viene visualizzata la sintassi del file di controllo utilizzata nella specifica del clone:

```
<controlfiles>
  <file>/mnt/path/clonename/control/control01.ctl</file>
  <file>/mnt/path/clonename/control/control02.ctl</file>
</controlfiles>
```

5. Specificare la struttura del log di ripristino per il clone.

Nell'esempio seguente viene visualizzata la struttura di directory del log di ripristino per la clonazione:

```
<redologs>
  <redogroup>
    <file>/mnt/path/clonename/redo/redo01.log</file>
    <number>1</number>
    <size unit="M">100</size>
  </redogroup>
  <redogroup>
    <file>/mnt/path/clonename/redo/redo02.log</file>
    <number>2</number>
    <size unit="M">100</size>
  </redogroup>
</redologs>
```

6. Specificare i parametri Oracle che devono essere impostati su valori diversi nel database clonato. Se si utilizza Oracle 10, è necessario specificare i seguenti parametri:

- Dump in background
- Core dump
- Dump dell'utente
- (Facoltativo) registri di archiviazione



Se i valori dei parametri non sono impostati correttamente, l'operazione di clonazione viene interrotta e viene visualizzato un messaggio di errore.

Se non si specifica la posizione in cui sono memorizzati i registri di archiviazione, SnapManager crea il clone in modalità noarchivelog. SnapManager copia le informazioni di questo parametro nel file init.ora del clone.

L'esempio seguente mostra la sintassi dei parametri utilizzata nella specifica dei cloni:

```
<parameters>
  <parameter>
    <name>log_archive_dest_1</name>
    <value>LOCATION=/mnt/path/clonename/archive</value>
  </parameter>
</parameters>
```

+ + è possibile utilizzare un valore predefinito utilizzando un elemento predefinito all'interno dell'elemento del parametro. Nell'esempio seguente, il parametro os_Authentication_PREFIX prenderà il valore predefinito perché viene specificato l'elemento predefinito:

+

+

+

```
<parameters>
  <parameter>
    <name>os_authent_prefix</name>
    <default></default>
  </parameter>
</parameters>
```

+ + è possibile specificare una stringa vuota come valore per un parametro utilizzando un elemento vuoto. Nell'esempio seguente, os_Authentication_PREFIX viene impostato su una stringa vuota:

+

+

+

```
<parameters>
  <parameter>
    <name>os_authent_prefix</name>
    <value></value>
  </parameter>
</parameters>
```

+ + NOTA: È possibile utilizzare il valore del file init.ora del database di origine per il parametro senza specificare alcun elemento.

+ + se un parametro ha valori multipli, è possibile fornire i valori dei parametri separati da virgole. Ad esempio, se si desidera spostare i file di dati da una posizione all'altra, è possibile utilizzare il parametro `db_file_name_convert` e specificare i percorsi dei file di dati separati da virgole, come illustrato nell'esempio seguente:

+

+

+

```
<parameters>
  <parameter>
    <name>db_file_name_convert</name>
    <value>>/mnt/path/clonename/data file1,/mnt/path/clonename/data
file2</value>
  </parameter>
</parameters>
```

+ + se si desidera spostare i file di log da una posizione all'altra, è possibile utilizzare il parametro `log_file_name_convert` e specificare i percorsi dei file di log separati da virgole, come illustrato nell'esempio:

+

+

+

```
<parameters>
  <parameter>
    <name>log_file_name_convert</name>

    <value>>/mnt/path/clonename/archivle1,/mnt/path/clonename/archivle2</value
>
  </parameter>
</parameters>
```

1. Facoltativo: Specificare istruzioni SQL arbitrarie da eseguire sul clone quando è online.

È possibile utilizzare le istruzioni SQL per eseguire attività come la ricreazione dei file temporanei nel database clonato.



È necessario assicurarsi che un punto e virgola non sia incluso alla fine dell'istruzione SQL.

Di seguito viene riportata un'istruzione SQL di esempio eseguita come parte dell'operazione di clonazione:


```

<sql-statements>
  <sql-statement>
    ALTER TABLESPACE TEMP ADD
    TEMPFILE '/mnt/path/clonename/temp_user01.dbf'
    SIZE 41943040 REUSE AUTOEXTEND ON NEXT 655360
    MAXSIZE 32767M
  </sql-statement>
</sql-statements>

```

Esempio di specifica di clonazione

Nell'esempio seguente viene illustrata la struttura delle specifiche dei cloni, inclusi i componenti delle specifiche di storage e database:

```

<clone-specification xmlns="http://www.example.com">

  <storage-specification>
    <storage-mapping>
      <mountpoint>
        <source>/mnt/path/source_mountpoint</source>
        <destination>/mnt/path/target_mountpoint</destination>
      </mountpoint>
      <raw-device>
        <source>/dev/raw/raw1</source>
        <destination auto-generate="true"/>
      </raw-device>
      <raw-device>
        <source>/dev/raw/raw2</source>
        <destination auto-generate="true"/>
      </raw-device>
    </storage-mapping>
  </storage-specification>

  <database-specification>
    <controlfiles>
      <file>/mnt/path/clonename/control/control01.ctl</file>
      <file>/mnt/path/clonename/control/control02.ctl</file>
    </controlfiles>
    <redologs>
      <redogroup>
        <file>/mnt/path/clonename/redo/redo01.log</file>
        <number>1</number>
        <size unit="M">100</size>
      </redogroup>
    </redologs>
  </database-specification>
</clone-specification>

```

```

        <file>/mnt/path/clonename/redo/redo02.log</file>
        <number>2</number>
        <size unit="M">100</size>
    </redogroup>
</redologs>
<parameters>
    <parameter>
        <name>log_archive_dest_1</name>
        <value>LOCATION=/mnt/path/clonename/archive</value>
    </parameter>
    <parameter>
        <name>background_dump_dest</name>
        <value>/mnt/path/clonename/admin/bdump</value>
    </parameter>
    <parameter>
        <name>core_dump_dest</name>
        <value>/mnt/path/clonename/admin/cdump</value>
    </parameter>
    <parameter>
        <name>user_dump_dest</name>
        <value>/mnt/path/clonename/admin/udump</value>
    </parameter>
</parameters>
</database-specification>
</clone-specification>

```

Informazioni correlate

[Clonazione di database e utilizzo di script plug-in personalizzati](#)

[Clonare i database dai backup](#)

[Clonazione dei database nello stato corrente](#)

[Considerazioni per clonare un database su un host alternativo](#)

Clonazione di database e utilizzo di script plug-in personalizzati

SnapManager fornisce un metodo per utilizzare gli script personalizzati prima e dopo un'operazione di clonazione. Ad esempio, potrebbe essere stato creato uno script personalizzato che convalida un SID del database clone e garantisce che il SID sia consentito dalla policy di naming. Utilizzando il plug-in del clone di SnapManager, è possibile includere gli script personalizzati e farli eseguire automaticamente prima o dopo un'operazione di clone di SnapManager.

1. Visualizza script plug-in di esempio.
2. Creare uno script da zero o modificare uno degli script dei plug-in di esempio.

Creare lo script personalizzato in base alle linee guida dello script del plug-in SnapManager.

3. Inserire lo script personalizzato in una directory specificata.
4. Aggiornare il file XML delle specifiche dei cloni e includere informazioni sullo script personalizzato da utilizzare durante il processo di cloning.
5. Utilizzando un comando SnapManager, verificare che gli script personalizzati siano operativi.
6. Quando si avvia l'operazione di clonazione, includere il nome dello script e i parametri facoltativi.

Clonare i database dai backup

È possibile clonare un database da un backup utilizzando il comando `clone create`.

Creare prima un file di specifica clone per il database. SnapManager crea il clone in base alle informazioni contenute in questo file di specifica.

È necessario assegnare al clone un nuovo SID (System Identifier) Oracle. Non è possibile eseguire contemporaneamente due database con lo stesso SID sullo stesso host. È possibile disporre di un clone su un host diverso che utilizza lo stesso SID. Per specificare un nome univoco per il clone, utilizzare `-label`. Se non si utilizza questa opzione, SnapManager crea un nome univoco per il clone che include il SID, la data e l'ora.

Dopo aver clonato un database, è possibile aggiornare i file `tnsname.ora` sui computer client con le nuove informazioni di connessione al database clonato. I file `tnsnames.ora` vengono utilizzati per connettersi a un'istanza Oracle senza dover specificare le informazioni complete del database. SnapManager non aggiorna i file `tnsnames.ora`.

Se si utilizza il profilo creato con `-include-with-online-backups`, SnapManager crea sempre un backup che include i file di log dell'archivio. SnapManager consente di clonare solo i backup completi del database.

SnapManager (3.2 o versione successiva) consente di clonare i backup contenenti i file di dati e i file di log dell'archivio.

Se il log di archiviazione è disponibile da una posizione esterna, è possibile specificare la posizione esterna durante la clonazione per il ripristino del database clonato in uno stato coerente. L'utente deve assicurarsi che la posizione esterna sia accessibile da Oracle. La clonazione dei backup solo log dell'archivio non è supportata.

Sebbene il backup del registro di archiviazione venga creato insieme al backup parziale online, non è possibile creare un clone del database utilizzando questo backup.

È possibile clonare il backup del database dalla posizione del file di log dell'archivio esterno solo per un database standalone.

La clonazione del backup online del database Real Application Clusters (RAC) utilizzando la posizione esterna del file di log dell'archivio non riesce a causa di un errore di ripristino. Questo perché il database Oracle non riesce a trovare e applicare i file di log dell'archivio per il ripristino dalla posizione del log dell'archivio esterno durante la clonazione del backup del database.

È possibile specificare l'opzione `-dump` come parametro facoltativo per raccogliere i file dump dopo l'operazione di creazione del clone riuscita o non riuscita.

Clonazione del backup dei file di dati senza backup del log di archiviazione

Quando il backup dei file di dati non include il backup del registro di archiviazione, SnapManager per Oracle clona il database in base al numero di modifica del sistema registrato durante il backup. Se non è possibile

ripristinare il database clonato, viene visualizzato il messaggio di errore file di log archiviato per thread <number> e change <SCN> required to complete recovery error (Modifica richiesta per il ripristino completo), anche se SnapManager per Oracle continua a clonare il database e infine riesce a creare il clone.

Quando si esegue il cloning utilizzando il backup dei file di dati senza includere il backup del registro di archiviazione, SnapManager ripristina il database clonato fino all'ultimo SCN del registro di archiviazione, registrato durante il backup.

1. Creare un file di specifica clone.
2. Per creare un clone, immettere il seguente comando: `Clone smo create -backup-labelbackup_name -newsidnew_sid-labelclone_label-profileprofile_name-clonespecfull_path_to_clonespecfile [-taskspekspec] [-recover-from-location] path 1 [,<path2>...][-dump]`

Informazioni correlate

[Clonazione dei database nello stato corrente](#)

[Considerazioni per clonare un database su un host alternativo](#)

[Creazione di specifiche di cloni](#)

[Comando di creazione del clone smo](#)

[Creazione di script di pre-task, post-task e policy](#)

[Variabili disponibili negli script di attività per l'operazione di cloni](#)

[Creazione di script di attività](#)

[Memorizzazione degli script delle operazioni](#)

Clonazione dei database nello stato corrente

È possibile creare un backup e un clone del database dallo stato corrente del database utilizzando un singolo comando.

Quando si specifica il profilo con l'opzione `-current`, SnapManager crea prima un backup e poi un clone dallo stato corrente del database.

Nell'impostazione del profilo, se è stato attivato il backup dei file di dati e dei registri di archiviazione per la clonazione, ogni volta che si esegue il backup dei file di dati online, viene eseguito anche il backup dei registri di archiviazione. Durante la clonazione del database, SnapManager crea il backup dei file di dati insieme al backup del log di archiviazione e crea il clone del database. Se il backup del registro di archiviazione non è incluso, SnapManager non crea il backup del registro di archiviazione e quindi non può creare il clone del database.

1. Per clonare il database nello stato corrente, immettere il seguente comando: `smo clone create -profileprofile_name-current -labelclone_name-clonespec./clonespec_filename.xml`

Questo comando esegue un backup automatico completo (generando l'etichetta di backup) e crea immediatamente un clone da tale backup, utilizzando una specifica di clone esistente che si desidera utilizzare.



È possibile specificare l'opzione `-dump` come parametro facoltativo per raccogliere i file dump dopo le operazioni riuscite o non riuscite. Il dump viene raccolto sia per le operazioni di backup che per quelle di cloni.

Clonare i backup del database senza resetlog

SnapManager consente di eseguire la clonazione flessibile in modo da ripristinare manualmente il database clonato al punto desiderato senza aprire il database utilizzando i resetlog. È inoltre possibile configurare manualmente il database clonato come database di standby Data Guard.

Quando è possibile selezionare l'opzione `-no-resetlogs` durante la creazione del clone, SnapManager esegue le seguenti attività per creare il database clonato:

1. Esegue l'attività di pre-elaborazione, se specificata, prima di avviare l'operazione di cloni
2. Crea il database clonato con il SID specificato dall'utente
3. Esegue le istruzioni SQL emesse nel database clonato.

Vengono eseguite correttamente solo le istruzioni SQL che possono essere eseguite in stato di montaggio.

4. Esegue l'attività di post-elaborazione, se specificata.

Quali operazioni è necessario eseguire per ripristinare manualmente il database clonato

1. Montare i backup del log di archiviazione e ripristinare manualmente il database clonato utilizzando i file di log di archiviazione dal percorso montato.
2. Dopo aver eseguito il ripristino manuale, aprire il database clonato recuperato con l'opzione `-resetlogs`.
3. Creare spazi tabella temporanei, se necessario.
4. Eseguire l'utility DBNEWID.
5. Concedere il privilegio sysdba alle credenziali del database clonato.

Mentre si clonano i backup del database utilizzando l'opzione `-no-resetlog`, SnapManager lascia il database clonato nello stato montato per il ripristino manuale.



Il database clonato creato con l'opzione `-no-resetlogs` non è un database completo. Pertanto, non è necessario eseguire operazioni SnapManager su questo database, sebbene SnapManager non limiti l'esecuzione di alcuna operazione.

Se non si specifica l'opzione `-no-resetlog`, SnapManager applica i file di log dell'archivio e apre il database con i resetlog.

1. Immettere il seguente comando: `smo clone create -profileprofile_name [-backup-labelbackup_name | -backup-idbackup_id | current] -newsidnew_sid-clonespecfull_path_to_clonespecfile-no-resetlogs`

Se si tenta di specificare entrambe le opzioni `-no-resetlog` e `recovery-from-location`, SnapManager non consente di specificare entrambe le opzioni e visualizza il messaggio di errore SMO-04084: Specificare una delle opzioni: `-No-resetlog` o `-recover-from-location`.

Esempio

```
smo clone create -profile product -backup-label full_offline -newsid  
PROD_CLONE -clonespec prod_clonespec.xml -label prod_clone-reserve -no  
-reset-logs
```

Considerazioni per clonare un database su un host alternativo

Prima di poter clonare su un host diverso da quello su cui risiede il database, è necessario soddisfare alcuni requisiti.

La seguente tabella mostra i requisiti di configurazione degli host di origine e destinazione:

Configurazione dei prerequisiti	Requisito
Architettura	Deve essere lo stesso sia per gli host di origine che per quelli di destinazione
Sistema operativo e versione	Deve essere lo stesso sia per gli host di origine che per quelli di destinazione
SnapManager per Oracle	Deve essere installato e in esecuzione sia sull'host di origine che su quello di destinazione
Credenziali	Deve essere impostato per consentire all'utente di accedere all'host di destinazione
Oracle	La stessa versione software deve essere installata sia sull'host di origine che su quello di destinazione. Il listener Oracle deve essere in esecuzione sull'host di destinazione.
Stack di storage compatibile	Deve essere lo stesso sia per gli host di origine che per quelli di destinazione
Protocollo utilizzato per accedere ai file di dati	Deve essere lo stesso sia per gli host di origine che per quelli di destinazione
Gestori di volumi	Deve essere configurato sia sull'host di origine che su quello di destinazione e deve essere di versioni compatibili

È inoltre possibile clonare un database ASM (Automatic Storage Management) su un host remoto. Durante questa operazione, è necessario assicurarsi che l'istanza di ASM sia in esecuzione sull'host remoto.

Clonazione di un database in un host alternativo

È possibile utilizzare il comando `clone create` per clonare un backup del database su un host alternativo.

- Creare un profilo o disporre di un profilo esistente.
- Creare un backup completo o disporre di un backup del database esistente.
- Creare una specifica di cloni o disporre di una specifica di cloni esistente.
 - a. Per clonare un database in un host alternativo, immettere il seguente comando: `smo clone create -backup-label backup_label_name-newsid new_sid-host target_host-label clone_label-comment comment_text-profile profile_name-clonespec full_path_to_clonespecfile`

Oracle non consente di eseguire contemporaneamente due database con lo stesso SID sullo stesso host. Per questo motivo, è necessario fornire un nuovo SID per ciascun clone. Tuttavia, è possibile avere un database su un altro host con lo stesso SID.

Informazioni correlate

[Creazione di profili](#)

[Clonare i database dai backup](#)

[Creazione di specifiche di cloni](#)

[Comando di creazione del clone `smo`](#)

Visualizzazione di un elenco di cloni

È possibile visualizzare un elenco di cloni associati a un particolare profilo.

L'elenco include le seguenti informazioni sui cloni in un profilo:

- L'ID del clone
- Stato dell'operazione clone
- SID Oracle per il clone
- Host su cui risiede il clone
- Etichetta per il clone

Se si specifica l'opzione `-verbose`, l'output mostra anche i commenti immessi per il clone.

1. Per visualizzare un elenco di tutti i cloni di un profilo, immettere il seguente comando `smo clone list -profile profile_name [-quiet | -verbose]`

Informazioni correlate

[Il comando `smo clone list`](#)

Visualizzazione di informazioni dettagliate sui cloni

È possibile visualizzare informazioni dettagliate su un clone specifico utilizzando il

comando clone show.

Il comando clone show visualizza le seguenti informazioni:

- Clonare l'identificatore di sistema e l'ID clone
- Clonare lo stato dell'operazione
- Clonare la data o l'ora di inizio e di fine della creazione
- Clona etichetta
- Clonare il commento
- Etichetta e ID di backup
- Database di origine
- Ora di inizio e fine del backup
- Nome del database, tablespace e file di dati
- Nome host e file system contenenti file di dati
- Volumi del sistema di storage e copie Snapshot che eseguono il backup del clone
- Se il clone è stato creato utilizzando il backup sullo storage primario o secondario
 - a. Immettere il seguente comando: `smo clone show -profile profile_name [-label label | -id guid]`

Informazioni correlate

[Comando di visualizzazione del clone smo](#)

Eliminazione dei cloni

È possibile eliminare i cloni quando la dimensione della copia Snapshot raggiunge tra il 10% e il 20% del backup. Ciò garantisce inoltre che il clone disponga dei dati più aggiornati.

L'etichetta è l'identificatore univoco di ciascun clone di un profilo. È possibile utilizzare l'etichetta o l'ID del clone, ma non l'identificatore di sistema (SID) per eliminare il clone.



La SID del clone e l'etichetta del clone non sono uguali.

Quando si elimina un clone, il database deve essere in esecuzione. In caso contrario, molti file e directory per il clone esistente non verranno cancellati, con conseguente maggiore lavoro prima della creazione di un altro clone.

Le directory specificate per alcuni parametri Oracle nel clone vengono distrutte quando il clone viene cancellato e devono contenere solo dati per il database clonato: Destinazioni registro archivio, background, core e destinazioni di dump utente. I file di audit non vengono cancellati.



Non è possibile eliminare un clone quando viene utilizzato in altre operazioni.

È possibile raccogliere i file dump dopo un'operazione di eliminazione dei cloni riuscita o non riuscita.

1. Immettere il seguente comando: `smo clone delete -profile_name [-label label | -id guid] [-`


```
syspasswordsyspassword]] [login-username]db_username-password] db_password-portdb_port] [-  
asminstance-asmusernameasm_username-asmpasswordasm_password][[-force][[-dump][[-verbose]][-  
verbose]]][[-verbose]
```

Esempio

```
smo clone delete -profile targetdb1_prof1 -label sales0908_clone1
```

Informazioni correlate

[Il comando di eliminazione del clone smo](#)

Dividere un clone

SnapManager consente di suddividere e gestire un clone esistente creato utilizzando la tecnologia FlexClone. Nella tecnologia FlexClone, il clone e il database originale condividono gli stessi blocchi di dati fisici.

Prima di eseguire l'operazione di suddivisione dei cloni, è possibile sapere che la dimensione stimata del clone da suddividere e lo spazio necessario disponibile sull'aggregato.

Un nuovo profilo viene generato da SnapManager se l'operazione di suddivisione del clone ha esito positivo. Se SnapManager non riesce a creare il nuovo profilo, è possibile crearne uno nuovo manualmente. È possibile utilizzare il nuovo profilo per creare backup del database, ripristinare i dati e creare cloni. Se l'operazione di suddivisione dei cloni ha esito positivo, indipendentemente dal fatto che il nuovo profilo sia stato creato o meno, i metadati correlati ai cloni vengono rimossi dal database del repository.

È possibile eseguire le seguenti attività relative alla suddivisione dei cloni:

- Visualizzare la stima del clone split.
- Dividere un clone su uno storage primario.
- Dividere un clone su uno storage secondario.
- Visualizzare lo stato delle operazioni di divisione dei cloni.
- Interrompere l'operazione di suddivisione del clone.
- Distruggere il profilo insieme allo storage sottostante.
- Eliminare il profilo creato per un clone separato.

Quando si divide un clone dal volume principale, le copie Snapshot associate al volume clonato vengono eliminate. I backup creati per il database clonato prima del processo di suddivisione del clone non possono essere utilizzati perché le copie Snapshot di questi backup vengono eliminate e i backup rimangono come voci obsolete nel repository.

Visualizzazione di una stima di divisione clone

La stima della suddivisione del clone consente di conoscere lo spazio libero totale disponibile sull'aggregato, la quantità di spazio condiviso tra il clone e il database originale e lo spazio utilizzato esclusivamente dal clone. Inoltre, è possibile visualizzare la data e l'ora in cui è stato creato il clone sottostante e l'età del clone. In base a questa

stima, decidi se dividere o meno un clone.

Per visualizzare la stima della suddivisione del clone, immettere il nome del profilo del clone originale e l'etichetta o GUID dell'operazione. Se il clone si trova in un host diverso, è possibile specificare il nome dell'host.

1. Per visualizzare la stima del clone split, immettere il seguente comando: `smo clone split-estimate -profileprofile [-hosthostname] [-labelclone-label | -idclone-id] [-quiet | -verbose]`

Nell'esempio seguente viene illustrato il comando per la stima dello storage suddiviso in cloni:

```
smo clone split-estimate  
  
-profile p1 -label clone_test_label
```

Suddivisione di un clone sullo storage primario o secondario

È possibile utilizzare il comando `clone split` per dividere il clone. Una volta completata la suddivisione del clone, i metadati del clone vengono rimossi dal database del repository e il backup associato al clone può essere cancellato o liberato.

Il nuovo profilo creato dopo l'operazione di split viene utilizzato per la gestione del clone split. Il nuovo profilo sarà simile a qualsiasi altro profilo esistente in SnapManager. È possibile utilizzare questo profilo per eseguire operazioni di backup, ripristino e clonazione.

Inoltre, è possibile configurare la notifica e-mail per il nuovo profilo. Ciò consente all'amministratore del database di essere informato sullo stato dell'operazione del database eseguita utilizzando il profilo.



SnapManager supporta l'operazione di splitting solo se eseguita su FlexClone.

Se l'operazione di divisione non riesce, viene visualizzato un messaggio di errore appropriato con il motivo del guasto. Lo stato di più operazioni viene visualizzato anche nel registro delle operazioni. Ad esempio:

```
--[ INFO] The following operations were completed:  
Clone Split : Success  
Profile Create : Failed  
Clone Detach : Success
```

È possibile raccogliere i file dump dopo un'operazione di suddivisione dei cloni non riuscita o riuscita.



Dopo aver immesso il comando `clone split`, non arrestare il server SnapManager fino all'avvio dell'operazione `clone split`.



SnapManager genera il profilo anche se non si fornisce alcun valore per l'account Oracle (osaccount e osgroup).

1. Immettere il seguente comando: `smo clone split -profileclone-profile-hostname [-labelclone-label | -idclone`

```
-id]-split-labelsplit-operation-label-commentcommentnew-profilenew-profile-name [-profile-profile-  
nomerepo_service_name-db] [-nomernomerdb_{nomerdb}] [-nomernomerdb  
{nomernomernomesellabutoutente}] [-nomesellabutoutente]}
```

Visualizzazione dello stato del processo di suddivisione dei cloni

È possibile visualizzare lo stato di avanzamento del processo di divisione avviato.

1. Per visualizzare l'avanzamento del processo di suddivisione dei cloni, immettere il seguente comando: `smo clone split-status -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-status -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Visualizzazione del risultato del processo di suddivisione dei cloni

È possibile visualizzare il risultato del processo di suddivisione dei cloni avviato.

1. Per visualizzare il risultato del processo di suddivisione dei cloni, immettere il seguente comando: `smo clone split-result -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-result -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Interruzione del processo di suddivisione dei cloni

È possibile interrompere il processo di suddivisione dei cloni in esecuzione.

Una volta interrotto il processo di divisione, non è possibile ripristinarlo.

1. Per interrompere l'operazione di suddivisione dei cloni, immettere il seguente comando: `smo clone split-stop -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-stop -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Eliminazione di un profilo

È possibile eliminare un profilo purché non contenga backup riusciti attualmente utilizzati in altre operazioni. È possibile eliminare i profili che contengono backup liberati o cancellati.

1. Immettere il seguente comando: `smo profile delete -profileprofile [-quiet | -verbose]`

È possibile eliminare un nuovo profilo creato per la divisione clone. Durante l'eliminazione, nell'interfaccia

della riga di comando di SnapManager viene visualizzato il messaggio di avviso Impossibile distruggere il profilo in un secondo momento.

```
smo profile delete -profile AUTO-REVEN
```

Distruggere un profilo

SnapManager consente di distruggere il profilo associato al clone split (database) insieme allo storage sottostante. Prima di distruggere il profilo, assicurarsi di rimuovere i backup e i cloni associati.

1. Per distruggere un profilo creato utilizzando l'operazione di clonazione divisa e il database di cloni divisi, immettere il seguente comando: `smo profile destroy -profileprofile [-hosthostname] [-quiet | -verbose]`

```
smo profile destroy -profile AUTO-REVEN
```

Eliminazione di un ciclo operativo di suddivisione dei cloni da un database di repository

È possibile eliminare una voce del ciclo operativo diviso per cloni da un database di repository.

1. Per eliminare una voce del ciclo operativo di split clone da un database di repository, immettere il seguente comando: `smo clone split-delete -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-delete -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Introduzione alla protezione dei dati in SnapManager

SnapManager supporta la protezione dei dati per proteggere i backup sui sistemi storage secondari o terziari. È necessario impostare le relazioni di SnapMirror e SnapVault tra i volumi di origine e di destinazione.

Se si utilizza Data ONTAP in 7-Mode, SnapManager offre una protezione dei dati basata su policy grazie all'integrazione con Protection Manager (OnCommand Unified Manager). Ciò automatizza la replica dei backup SnapManager su un sistema di storage primario su un sistema di storage secondario o anche su un sistema di storage terzo utilizzando le policy di SnapVault o SnapMirror create dall'amministratore dello storage o del backup in Gestione protezione. La conservazione sullo storage primario è controllata da SnapManager in base alla conservazione definita durante la creazione del profilo e alla classe di conservazione contrassegnata durante la creazione del backup. La conservazione del backup dello storage secondario è controllata dalla policy definita in Protection Manager.

Se si utilizza Clustered Data ONTAP, SnapManager 3.4 fornisce le policy di protezione dei dati di *SnapManager_cDOT_Mirror* e *SnapManager_cDOT_Vault*. Durante la creazione di un profilo, è possibile selezionare questi criteri in base alla relazione di SnapMirror o SnapVault stabilita utilizzando l'interfaccia

utente di Clustered Data ONTAP o Gestione di sistema. Quando si crea un backup selezionando il profilo per cui è stata attivata la protezione, i backup vengono protetti in un sistema di storage secondario.

Se si utilizzava SnapManager 3.3.1 con Clustered Data ONTAP, i backup venivano protetti utilizzando post-script selezionati durante la creazione dei profili. Se si desidera utilizzare tali profili, dopo l'aggiornamento a SnapManager 3.4 è necessario eseguire le seguenti operazioni.

- È necessario aggiornare i profili per selezionare la policy *SnapManager_cDOT_Mirror* o *SnapManager_cDOT_Vault* ed eliminare il post-script utilizzato per la protezione dei dati.
- Dopo aver aggiornato il profilo per utilizzare la policy *SnapManager_cDOT_Vault*, è necessario eliminare le pianificazioni di backup esistenti e creare nuove pianificazioni per specificare l'etichetta SnapVault per i backup.
- Se i profili sono stati creati in SnapManager 3.3.1 senza selezionare gli script successivi, è necessario aggiornarli per selezionare il criterio *SnapManager_cDOT_Mirror* o *SnapManager_cDOT_Vault* per abilitare la protezione dei dati.



Se nel sistema di storage secondario sono presenti backup mirrorati o vault utilizzando gli script successivi di SnapManager 3.3.1, non è possibile utilizzarli per il ripristino o la clonazione utilizzando SnapManager 3.4.

Se si utilizza Clustered Data ONTAP, SnapManager 3.4.2 supporta più relazioni di protezione (SnapMirror e SnapVault) sui volumi di origine. Sono supportate solo una relazione SnapMirror e una relazione SnapVault per volume. È necessario creare profili separati, ciascuno con i criteri SnapManager_cDOT_Mirror e SnapManager_cDOT_Vault selezionati.



SnapDrive per Unix 5.3.2 e versioni successive è necessario per utilizzare più policy di protezione.

Quali sono le policy di protezione

I criteri di protezione sono regole che regolano la modalità di protezione dei backup del database. È possibile selezionare i criteri di protezione durante la creazione del profilo.

Un criterio di protezione definisce i seguenti parametri:

- Quando trasferire le copie sullo storage secondario
- La quantità massima di dati che devono essere trasferiti in orari pianificati
- Per quanto tempo conservare le copie per ciascuna posizione di backup
- Soglie di avviso e di errore per i tempi di ritardo

Quando la protezione è attivata, SnapManager crea un dataset per il database. Un set di dati è costituito da un insieme di set di storage insieme alle informazioni di configurazione associate ai dati. I set di storage associati a un set di dati includono un set di storage primario utilizzato per esportare i dati nei client e l'insieme di repliche e archivi presenti in altri set di storage. I set di dati rappresentano dati esportabili dell'utente. Se l'amministratore disattiva la protezione per un database, SnapManager elimina il dataset.

Quali sono gli stati di protezione

SnapManager mostra lo stato di ciascun backup. Gli amministratori devono conoscere i diversi stati e monitorare lo stato dei backup.

Un backup del database può avere i seguenti stati di protezione:

Stato	Definizione	Spiegazione
Protetto	La protezione è stata richiesta ed è stata attivata.	La protezione è attivata per il backup in SnapManager e Gestione protezione ha copiato correttamente il backup in un altro set di dischi fisici (anche noto come storage secondario). Se Protection Manager rimuove un backup dallo storage secondario a causa di un criterio di conservazione, il backup può tornare allo stato non protetto.
Non protetto	La protezione è stata richiesta, ma non è stata completata.	La protezione è attivata per il backup, ma il backup non viene copiato in un altro set di dischi fisici. Il backup non è ancora protetto o la protezione non è riuscita oppure è stato protetto in precedenza ma non è più protetto. Quando si crea un backup, lo stato di protezione iniziale del backup non viene richiesto o non viene protetto. Se il backup non è protetto, diventa protetto quando viene trasferito allo storage secondario.
Non richiesto	Protezione non richiesta.	La protezione non è abilitata per il backup. Una copia logica dei dati esiste sugli stessi dischi fisici (anche noto come backup locale). Se la protezione non viene richiesta al momento della creazione del backup, la protezione sul backup viene sempre visualizzata come non richiesta.

Quali sono i pool di risorse

Un pool di risorse è un insieme di storage fisico inutilizzato (ad esempio, sistemi di storage o aggregati) da cui è possibile eseguire il provisioning di nuovi volumi o LUN per contenere i dati. Se si assegna un sistema storage a un pool di risorse, tutti gli aggregati su tale sistema storage diventano disponibili per il provisioning.

Gli amministratori dello storage utilizzano la console di Protection Manager per assegnare un pool di risorse alle copie di backup e mirror. L'applicazione di provisioning può quindi eseguire automaticamente il provisioning dei volumi dalle risorse fisiche del pool di risorse per contenere backup e copie mirror.

Per i profili protetti, SnapManager visualizza le informazioni relative a un profilo e indica se a tale profilo è stato

assegnato un pool di risorse di storage. In caso contrario, il profilo viene considerato "non conforme". Una volta assegnato un pool di risorse di storage al dataset del profilo corrispondente, il profilo viene considerato "conforme".

Sulle diverse policy di protezione

È possibile selezionare criteri diversi per proteggere i backup sui sistemi di storage secondari o terziari.

Se si utilizza Data ONTAP in modalità 7 e SnapManager è integrato con Gestione protezione, è necessario selezionare una delle seguenti policy di protezione durante la creazione del profilo. La console di gestione di Protection Manager fornisce modelli per configurare le policy di protezione per i set di dati. Anche se i criteri di protezione del disaster recovery sono elencati nell'interfaccia utente di SnapManager, questi criteri non sono supportati.

Policy	Descrizione
Backup	Il backup di un set di dati viene eseguito localmente e anche dallo storage primario a quello secondario utilizzando SnapVault o SnapMirror.
Eseguire il backup, quindi eseguire il mirroring	Viene eseguito il backup di un set di dati dallo storage primario a quello secondario utilizzando SnapVault o SnapMirror e quindi il mirroring su un partner SnapMirror.
Solo copie Snapshot locali	Un dataset utilizza solo copie Snapshot locali nello storage primario.
Mirrorare	Il mirroring di un dataset dallo storage primario a quello secondario viene eseguito mediante SnapMirror.
Eseguire il mirroring e il backup	Viene eseguito il mirroring di un set di dati dallo storage primario a quello secondario utilizzando SnapMirror e quindi il backup sullo storage secondario mediante SnapVault o SnapMirror.
Mirrorare e mirrorare	Un set di dati viene mirrorato dallo storage primario a quello secondario su due partner SnapMirror diversi.
Mirrorare, quindi eseguire il backup	Viene eseguito il mirroring di un set di dati dallo storage primario a quello secondario utilizzando SnapMirror e quindi il backup sullo storage terzo utilizzando SnapVault o SnapMirror.
Mirrorare, quindi mirrorare	Un set di dati viene mirrorato dallo storage primario a quello secondario utilizzando SnapMirror e quindi eseguito il mirroring su un partner SnapMirror aggiuntivo.

Policy	Descrizione
Nessuna protezione	Un set di dati non dispone di copie Snapshot, backup o protezione con copia speculare di alcun tipo.
Solo backup remoto	Il backup dei dati su un sistema storage viene eseguito in remoto sullo storage secondario utilizzando SnapVault o SnapMirror. L'applicazione concessa in licenza non esegue alcun backup locale sullo storage primario. Questo criterio di protezione può essere applicato a sistemi di terze parti con Open Systems SnapVault installato.

Se si utilizza Clustered Data ONTAP, è necessario selezionare una delle seguenti policy di protezione durante la creazione del profilo.

Policy	Descrizione
SnapManager_cDOT_Mirror	Esegue il mirroring del backup.
SnapManager_cDOT_Vault	Effettua il vault del backup.

Configurazione e abilitazione della protezione dei dati basata su policy

È necessario configurare SnapDrive e il server DataFabric Manager per abilitare la protezione dei dati sul profilo per proteggere i backup sui sistemi di storage secondari. È possibile selezionare i criteri di protezione nella console di Protection Manager per specificare la modalità di protezione dei backup del database.



Per abilitare la protezione dei dati, è necessario assicurarsi che OnCommand sia installato su un server separato.

Configurazione del server DataFabric Manager e di SnapDrive quando RBAC è attivato

Quando RBAC (role-based access control) è attivato, è necessario configurare il server DataFabric Manager in modo che includa le funzionalità RBAC. È inoltre necessario registrare l'utente SnapDrive creato nel server DataFabric Manager e l'utente root del sistema di storage in SnapDrive.

1. Configurare il server DataFabric Manager.
 - a. Per aggiornare il server DataFabric Manager e aggiornare le modifiche apportate direttamente sul sistema di storage dal database di destinazione, immettere il seguente comando: `host dfm Discover storage_system`
 - b. Creare un nuovo utente nel server DataFabric Manager e impostare la password.
 - c. Per aggiungere l'utente del sistema operativo all'elenco di amministrazione del server di DataFabric Manager, immettere il seguente comando: `dfm user add sd-admin`
 - d. Per creare un nuovo ruolo nel server DataFabric Manager, immettere il seguente comando: `ruolo dfm`

create ruolo sd-admin-role

- e. Per aggiungere la funzionalità globale DFM.Core.AccessCheck al ruolo, immettere il seguente comando: `ruolo dfm add sd-admin-role DFM.Core.AccessCheck Global`
- f. Per aggiungere il ruolo di amministratore sd all'utente del sistema operativo, immettere il seguente comando: `dfm user role set sd-adminsd-admin-role`
- g. Per creare un altro ruolo nel server DataFabric Manager per l'utente root di SnapDrive, immettere il seguente comando: `ruolo dfm create sd-Protect`
- h. Per aggiungere funzionalità RBAC al ruolo creato per l'utente root di SnapDrive o l'amministratore, immettere i seguenti comandi: `ruolo dfm add sd-Protect SD.Config.Read ruolo Globaldfm add sd-Protect SD.Config.Write ruolo Globaldfm add sd-Protect SD.Config.Delete ruolo Globaldfm add sd-Protect`
- i. Per aggiungere l'utente oracle del database di destinazione all'elenco degli amministratori nel server DataFabric Manager e assegnare il ruolo sd-Protect, immettere il seguente comando: `dfm user add -r sd-protectaradb_host1/oracle`
- j. Per aggiungere il sistema storage utilizzato dal database di destinazione nel server DataFabric Manager, immettere il seguente comando: `dfm host set storage_system hostLogin=oracle hostPassword=password`
- k. Per creare un nuovo ruolo nel sistema di storage utilizzato dal database di destinazione nel server DataFabric Manager, immettere il seguente comando: `ruolo host dfm create -h storage_system-c "api-,login-" storage-rbac-role`
- l. Per creare un nuovo gruppo nel sistema di storage e assegnare il nuovo ruolo creato nel server DataFabric Manager, immettere il seguente comando: `dfm host usergroup create -h storage_system-r storage-rbac-rolestorage-rbac-group`
- m. Per creare un nuovo utente nel sistema di storage e assegnare il nuovo ruolo e il gruppo creato nel server DataFabric Manager, immettere il seguente comando: `dfm host user create -h storage_system-r storage-rbac-role -p password -g storage-rbac-grouptaradb_host1`

2. Configurare SnapDrive.

- a. Per registrare le credenziali dell'utente sd-admin con SnapDrive, immettere il seguente comando: `snapdrive config set -dfm sd-admin dfm_host`
- b. Per registrare l'utente root o l'amministratore del sistema storage con SnapDrive, immettere il seguente comando: `snapdrive config set taradb_host 1 host_system`

Configurazione di SnapDrive quando RBAC non è attivato

Per abilitare la protezione dei dati, è necessario registrare l'utente root o l'amministratore del server DataFabric Manager e l'utente root del sistema storage con SnapDrive.

1. Per aggiornare il server DataFabric Manager e le modifiche apportate direttamente sul sistema di storage dal database di destinazione, immettere il seguente comando:

`host dfm discover storage_system`
2. Per registrare l'utente root o l'amministratore del server DataFabric Manager con SnapDrive, immettere il seguente comando:

`Set di configurazione SnapDrive -dfm Administrator dfm_host`
3. Per registrare l'utente root o l'amministratore del sistema storage con SnapDrive, immettere il seguente comando:


config. SnapDrive imposta root storage_system

Informazioni sull'attivazione o la disattivazione della protezione dei dati nel profilo

È possibile attivare o disattivare la protezione dei dati durante la creazione o l'aggiornamento di un profilo di database.

Per creare un backup protetto di un database sulle risorse di storage secondarie, gli amministratori del database e gli amministratori dello storage eseguono le seguenti operazioni.

Se si desidera...	Quindi...
Creare o modificare un profilo	<p>Per creare o modificare un profilo, attenersi alla seguente procedura:</p> <ul style="list-style-type: none">• Abilitare la protezione del backup sullo storage secondario.• Se si utilizza Data ONTAP in 7-Mode e si è installato Protection Manager, è possibile selezionare i criteri creati dall'amministratore dello storage o del backup in Protection Manager. <p>Se si utilizza Data ONTAP in 7-Mode e la protezione è attivata, SnapManager crea un dataset per il database. Un set di dati è costituito da un insieme di set di storage insieme alle informazioni di configurazione associate ai dati. I set di storage associati a un set di dati includono un set di storage primario utilizzato per esportare i dati nei client e l'insieme di repliche e archivi presenti in altri set di storage. I set di dati rappresentano dati esportabili dell'utente. Se l'amministratore disattiva la protezione per un database, SnapManager elimina il dataset.</p> <ul style="list-style-type: none">• Se si utilizza ONTAP, selezionare il criterio <i>SnapManager_cDOT_Mirror</i> o <i>SnapManager_cDOT_Vault</i> a seconda della relazione SnapMirror o SnapVault creata. <p>Quando si disattiva la protezione di backup, viene visualizzato un messaggio di avviso che indica che il set di dati verrà eliminato e che non sarà possibile ripristinare o clonare i backup per questo profilo.</p>
Visualizzare il profilo	<p>Poiché l'amministratore dello storage non ha ancora assegnato risorse di storage per implementare il criterio di protezione, il profilo viene visualizzato come non conforme sia nell'interfaccia grafica utente di SnapManager che nell'output del comando di visualizzazione del profilo.</p>

Se si desidera...	Quindi...
Assegnare le risorse di storage nella console di gestione di Protection Manager	Nella console di gestione di Protection Manager, l'amministratore dello storage visualizza il dataset non protetto e assegna un pool di risorse per ogni nodo del dataset associato al profilo. L'amministratore dello storage verifica quindi che i volumi secondari siano sottoposti a provisioning e che le relazioni di protezione siano inizializzate.
Visualizza il profilo conforme in SnapManager	In SnapManager, l'amministratore del database rileva che il profilo è stato modificato in stato conforme sia nell'interfaccia utente grafica che nell'output del comando di visualizzazione del profilo, indicando che le risorse sono state assegnate.
Creare il backup	<ul style="list-style-type: none"> • Selezionare backup completo. • Inoltre, selezionare se il backup deve essere protetto e selezionare la classe di conservazione primaria (ad esempio, oraria o giornaliera). • Se si utilizza Data ONTAP in 7-Mode e si desidera proteggere immediatamente il backup sullo storage secondario sovrascrivendo il programma di protezione di Protection Manager, specificare l'opzione -protectnow. • Se si utilizza ONTAP e si desidera proteggere immediatamente il backup sullo storage secondario, specificare l'opzione Protect (protezione). <div>  <p>L'opzione protectnow non è applicabile in Clustered Data ONTAP.</p> </div>
Visualizzare il backup	Il nuovo backup viene visualizzato come pianificato per la protezione, ma non ancora protetto (nell'interfaccia SnapManager e nell'output del comando show di backup). Lo stato di protezione viene visualizzato come "Not Protected" (non protetto).
Visualizzare l'elenco di backup	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 "non protetto" a "protetto".

In che modo SnapManager conserva i backup sullo storage locale

SnapManager consente di creare backup conformi alle policy di conservazione, che

specificano il numero di backup riusciti nello storage locale da conservare. È possibile specificare il numero di backup riusciti da conservare nel profilo per un determinato database.

È possibile creare backup per:

- 10 giorni di backup giornalieri sullo storage primario
- 2 mesi di backup mensili sullo storage primario
- 7 giorni di backup giornalieri sullo storage secondario
- 4 settimane di backup settimanali sullo storage secondario
- 6 mesi di backup mensili sullo storage secondario

Per ogni profilo in SnapManager, è possibile modificare i valori per le seguenti classi di conservazione non limitate:

- Ogni ora
- Ogni giorno
- Settimanale
- Mensile

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 sua classe di conservazione o il numero di backup supera il numero di conservazione. Ad esempio, se il numero di backup è 15 (SnapManager ha eseguito 15 backup riusciti) e il requisito di durata è impostato per 10 giorni di backup giornalieri, i cinque backup idonei meno recenti scadono.

Dopo la scadenza di un backup, SnapManager libera o elimina il backup scaduto. SnapManager conserva sempre l'ultimo backup eseguito.

SnapManager conta solo il numero di backup riusciti per il conteggio della conservazione e non prende in considerazione quanto segue:

Backup non inclusi nel numero di conservazione	Ulteriori dettagli
Backup non riusciti	SnapManager conserva le informazioni relative ai backup riusciti e non riusciti. Sebbene i backup non riusciti richiedano solo uno spazio minimo nel repository, è possibile eliminarli. I backup non riusciti rimangono nel repository fino a quando non vengono cancellati.
Backup progettati per essere conservati su base illimitata o backup per una classe di conservazione diversa	SnapManager non elimina i backup da conservare senza limiti. Inoltre, SnapManager considera solo i backup nella stessa classe di conservazione (ad esempio, SnapManager considera solo i backup orari per il conteggio orario di conservazione).

Backup non inclusi nel numero di conservazione	Ulteriori dettagli
Backup montati dallo storage locale	Quando vengono montate, le copie Snapshot vengono clonate e quindi non sono considerate idonee per la conservazione. SnapManager non è in grado di eliminare le copie Snapshot se clonate.
Backup utilizzati per creare un clone sullo storage locale	SnapManager conserva tutti i backup utilizzati per creare cloni, ma non li prende in considerazione per il conteggio della conservazione dei backup.
Backup clonati o montati sullo storage secondario che utilizzano il criterio di protezione mirror	Se SnapManager elimina le copie Snapshot per il backup sulla risorsa di storage primaria e le copie Snapshot vengono mirrorate, il backup successivo sullo storage secondario non avrà esito positivo.

Quando si libera un backup dalle risorse di storage primarie, le risorse primarie (copie Snapshot) utilizzate dal backup vengono distrutte, ma i metadati del backup sono ancora disponibili. SnapManager non prende in considerazione i backup liberati nel numero di conservazione dei backup.

SnapManager fornisce un conteggio e una durata di conservazione predefiniti per ciascuna classe di conservazione. Ad esempio, per il conteggio delle classi di conservazione orarie, SnapManager, per impostazione predefinita, conserva quattro backup orarie. È possibile eseguire l'override di queste impostazioni predefinite e impostare i valori durante la creazione o l'aggiornamento del profilo o modificare i valori predefiniti per il conteggio e la durata di conservazione nel file `smo.config`.

È possibile proteggere i backup sullo storage primario eseguendo il backup sullo storage secondario. Mentre SnapManager gestisce la conservazione e la pianificazione dei backup sullo storage primario, Protection Manager gestisce la conservazione e la pianificazione dei backup sullo storage secondario.

Quando i backup locali scadono in base alla loro policy di conservazione, vengono cancellati o liberati, a seconda che siano protetti o meno.

- Se sono protetti, i backup locali vengono liberati. Le risorse di storage o le copie Snapshot vengono eliminate, ma i backup rimangono nel repository SnapManager e sono disponibili per il ripristino dallo storage secondario. Non è necessario liberare i backup (ad esempio, con il comando `backup free`). I backup vengono liberati fino a quando il backup non esiste più nello storage secondario e, a quel punto, il backup viene cancellato.
- Se non sono protetti, i backup locali vengono cancellati.

In un'operazione di backup solo archiviando, SnapManager non archivia i file di log di ripristino, a differenza del processo di backup del database online. È necessario aggiungere uno script di pretask per archiviare i file di log di ripristino prima di eseguire l'operazione di backup di solo archivio. Lo script di pretask deve eseguire il comando `alter system switch logfile`.

L'esempio seguente mostra le azioni che SnapManager esegue su diversi tipi di backup, in base a una policy di conservazione dei backup tre giorni (con il conteggio impostato su 3):

Data di backup	Stato	Azione della politica di conservazione intrapresa	Spiegazione
----------------	-------	---	-------------

5/10	Riuscito	Mantenere	Si tratta del backup più recente, quindi verrà mantenuto.
5/9	Riuscito, clonato	Saltare	SnapManager non prende in considerazione i backup utilizzati per la clonazione nel conteggio dei criteri di conservazione. Questo backup viene omissso dal numero di backup riusciti.
5/8	Montato con successo	Saltare	SnapManager non considera i backup montati nel conteggio dei criteri di conservazione. Questo backup viene omissso dal numero di backup riusciti.
5/7	Non riuscito	Saltare	I backup non riusciti non vengono conteggiati.
5/5	Riuscito	Mantenere	SnapManager mantiene questo secondo backup giornaliero di successo.
5/3	Riuscito	Mantenere	SnapManager mantiene questo terzo backup giornaliero di successo.
5/2	Riuscito	Eliminare	SnapManager conta questo backup riuscito, ma dopo che SnapManager ha raggiunto tre backup giornalieri, questo backup viene eliminato.

Informazioni correlate

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

Considerazioni per l'esecuzione della protezione dei dati

È necessario conoscere alcune considerazioni per l'esecuzione della protezione dei dati.

- Per eseguire operazioni di cloning o ripristino da sistemi secondari, è necessario montare il volume di destinazione nello spazio dei nomi ed esportarlo correttamente.

- È necessario disattivare il parametro di configurazione SnapDrive check-export-permission-nfs-clone impostando il valore su Off.

La documentazione di SnapDrive per UNIX sul sito di supporto NetApp contiene informazioni aggiuntive sul parametro check-export-permission-nfs-clone.

- È necessario configurare la relazione di SnapMirror per i volumi di storage secondari richiesti nel sistema di storage secondario.
- È necessario configurare la relazione SnapVault per i qtree dello storage secondario richiesti nel sistema di storage secondario per Data ONTAP che opera in 7-Mode.
- È necessario definire un criterio e regole per l'etichetta SnapMirror definita dall'utente se si utilizza SnapVault post-script per Clustered Data ONTAP.

SnapVault post-script supporta i volumi Data ONTAP in cluster e i tipi di relazione SnapMirror DP e XDP. La documentazione di ONTAP sul sito del supporto NetApp contiene informazioni sulla configurazione di SnapMirror e SnapVault.

- Negli ambienti NAS, è necessario configurare il percorso dei dati NAS primario e secondario utilizzando il comando SnapDrive config set-mgmtpathmanagement_pathmanagement_pathmanagement_pathmanagement_pathmanagement_pathda tapath_path.

Ad esempio, SnapDrive config set -mgmtpath f3050-197-91 f3050-197-91 f3050-197-91 f3050-220-91, dove f3050-197-91 è il percorso di gestione e f3050-220-91 è il percorso dei dati.

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

Licenze richieste per la protezione dei dati in SnapManager

È necessario assicurarsi che le licenze richieste per la protezione dei dati siano installate e attivate sui sistemi di storage primario e secondario.

I sistemi storage primari ricevono gli ultimi aggiornamenti delle transazioni per il database Oracle, memorizzano i dati e forniscono la protezione di backup locale del database. Il sistema di storage primario gestisce anche i file di dati del database, i file di log e i file di controllo. I sistemi storage secondari fungono da storage remoto per i backup protetti.

Per la protezione dei dati, è necessario installare e abilitare le seguenti licenze sui sistemi di storage primari:



Se si desidera attivare la protezione dei dati sui sistemi di storage secondari, è necessario installare e abilitare queste licenze sui sistemi di storage secondari.

- Data ONTAP in 7-Mode (7.3.1 o versione successiva) o Clustered Data ONTAP (8.2 o versione successiva)
- SnapVault (a seconda della policy di protezione)
- SnapRestore
- SnapMirror (a seconda della policy di protezione)
- FlexClone è richiesto per NFS (Network file System) e cloning.

FlexClone è inoltre necessario per la SAN (Storage Area Network) solo se SnapDrive è configurato per l'utilizzo di FlexClone negli ambienti SAN.

- Il protocollo appropriato, ad esempio NFS, Internet Small computer System Interface (iSCSI) o Fibre Channel (FC)


SnapVault o SnapMirror devono essere installati sui sistemi di storage primario e secondario in base alle policy di protezione utilizzate. I criteri di protezione di base del backup richiedono solo l'installazione di SnapVault sui sistemi di supporto. I criteri che includono la protezione mirror richiedono l'installazione di SnapMirror nei sistemi di supporto. I criteri di backup e disaster recovery mirror richiedono l'installation di SnapMirror nei sistemi di supporto.

Protezione dei backup dei database su storage secondario o terzo

È possibile utilizzare SnapManager per proteggere le copie di backup su sistemi di storage secondari o terziari.

1. Immettere il seguente comando: `smo backup create -profile profile_name {[-full {-online | -offline | -auto} [-retain {-hourly | -daily | -weekly | -monthly | -unlimited}] [-verify] | [-data [[-filesfiles [files]] | [-tablespaces-tablespaces [-tablespaces]] [-datalabellabel] {-online | -offline | -auto} [-retain {-hourly | [-daily | -weekly | -monthly | -unlimited}] [-verify] | [-archivelogs [-labellabel] [-commentcomment] [-snapvaultlabelSnapVault_label] [-protect | -noprotect | -protectnow] [-backup-destpath1 [, [path2]]] [-exclude-destpath1 [, path2]]] [-prunelogs {-all | -untilSCNuntilSCN | -until-date yyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}} -prune -destprune_dest1, [prune_dest2]] [-taskspectaskspec]} [-dump] [-force] [-quiet | -verbose]`

Se si desidera...	Quindi...
Creare un backup di un database online o offline, invece di consentire a SnapManager di gestire se è online o offline	Specificare l'opzione -offline o -online per creare un backup del database offline o online. Se si utilizza l'opzione -offline o -online, non è possibile utilizzare l'opzione -auto.
Lasciare che SnapManager gestisca il backup di un database, indipendentemente dal fatto che sia online o offline	Specificare l'opzione -auto. Se si utilizza l'opzione -auto, non è possibile utilizzare l'opzione -offline o -online.
Aggiungere un commento sul backup	Specificare l'opzione -comment, seguita dalla stringa di descrizione.
Forzare il database nello stato in cui è stato specificato il backup, indipendentemente dallo stato in cui si trova attualmente	Specificare l'opzione -force.
Verificare il backup al momento della creazione	Specificare l'opzione -verify.

Se si desidera...	Quindi...
Creare un backup sullo storage secondario	<p>Specificare l'opzione -Protect.</p> <ul style="list-style-type: none"> Se si utilizza ONTAP e si desidera proteggere immediatamente il backup sullo storage secondario, specificare l'opzione -Protect. <div style="display: flex; align-items: center;">  <div> <p>L'opzione -protectnow non è applicabile in Clustered Data ONTAP.</p> </div> </div> <ul style="list-style-type: none"> Se si utilizza Data ONTAP in 7-Mode e si desidera proteggere immediatamente il backup sullo storage secondario sovrascrivendo il programma di protezione di Protection Manager, specificare l'opzione -protectnow. Per impedire il backup sullo storage secondario, specificare l'opzione -noprotect. Se si utilizza ONTAP e si seleziona il criterio di protezione <i>SnapManager_cDOT_Vault</i> durante la creazione del profilo, è necessario specificare l'opzione -snapvaultlabel. È necessario fornire l'etichetta SnapMirror specificata nelle regole del criterio SnapMirror durante l'impostazione della relazione SnapVault come valore.
Specificare i valori della classe di conservazione	<p>Specificare l'opzione -retain e indicare se il backup deve essere conservato a seconda di una delle seguenti classi di conservazione:</p> <ul style="list-style-type: none"> orario giornaliero settimanale mensile -Unlimited se non si specifica la classe di conservazione, SnapManager utilizza -hourly per impostazione predefinita.

Esempi

Il seguente comando protegge un backup del database:

```
smo backup create -profile PAYDB -protect -retain -daily -full auto -label full_bkup_sales
```

Il seguente comando protegge immediatamente un backup del database:

```
smo backup create -profile PAYDB -protectnow -retain -daily -full auto  
-label full_bkup_sales
```

Ripristino dei backup protetti dallo storage secondario

È possibile ripristinare backup protetti dallo storage secondario. Tuttavia, non è possibile ripristinare i backup dallo storage secondario se il backup esiste anche sullo storage primario.

Informazioni correlate

[Il comando di ripristino del backup smo](#)

[Ripristino dei backup da una posizione alternativa](#)

[Creazione di specifiche di ripristino](#)

Panoramica sui ripristini dei backup protetti

È possibile scegliere il metodo di ripristino da utilizzare per ripristinare i dati di backup dallo storage secondario allo storage primario.

Nella tabella seguente sono illustrati i diversi scenari e metodi che è possibile utilizzare per ripristinare un backup dallo storage secondario:

Ripristinare la destinazione	Spiegazione
Direttamente allo storage primario	<p>Restituisce i dati dal sistema di storage secondario direttamente alla posizione originale sul sistema di storage primario sulla stessa rete utilizzata per proteggere i dati.</p> <p>SnapManager utilizza il metodo di storage diretto quando possibile. Questo metodo non è possibile se i dati si trovano in un file system su una SAN (Storage Area Network) e se si verifica una delle seguenti condizioni:</p> <ul style="list-style-type: none">• Altri file non di database non vengono ripristinati nello stesso file system.• Le copie Snapshot dei file di controllo e dei file di dati in un file system in fase di ripristino sono state eseguite in momenti diversi.• Il numero di unità logica (LUN) si trova in un gruppo di volumi, ma le altre LUN dello stesso gruppo di volumi non vengono ripristinate.

Ripristinare la destinazione	Spiegazione
Direttamente all'host	Clona i dati sul sistema di storage secondario e monta i dati clonati sull'host. Una volta clonati e montati i dati, SnapManager li copia nella posizione originale.
Indirettamente allo storage o all'host	<p>Restituisce i dati dal sistema di storage secondario a una nuova posizione sul sistema primario sulla stessa rete utilizzata per proteggere i dati e per montare il nuovo storage sull'host. Una volta restituiti e montati i dati, SnapManager li copia nella posizione originale. Il metodo di storage indiretto potrebbe richiedere molto tempo per restituire i dati.</p> <p>SnapManager copia prima i dati su un volume scratch sull'host primario prima che SnapManager li utilizzi per ripristinare e ripristinare il database. L'eliminazione automatica dei dati di scratch dipende dal protocollo utilizzato.</p> <ul style="list-style-type: none"> • Per LA SAN, SnapManager elimina i dati restituiti. • Per il NAS (Network-Attached Storage), SnapManager elimina il contenuto dei qtree restituiti, ma non elimina i qtree stessi. Per eliminare i qtree, gli amministratori devono montare il volume scratch e rimuovere i qtree utilizzando il comando UNIX rmdir.

Se non è possibile restituire direttamente i dati allo storage, SnapManager può restituire i dati direttamente all'host o indirettamente allo storage o all'host. Il metodo dipende dalla policy che stabilisce se l'organizzazione consente la connessione diretta allo storage secondario o richiede la copia dei dati sulla rete di storage. È possibile gestire questo criterio impostando le informazioni di configurazione nel file `smo.config`.

Informazioni correlate

[Parametri di configurazione di SnapManager](#)

Ripristino dei backup dallo storage secondario

È possibile ripristinare i backup protetti dallo storage secondario e scegliere la modalità di copia dei dati nello storage primario.

È possibile utilizzare il comando di backup restore con l'opzione `-from-secondary` per ripristinare i dati dallo storage secondario. Se non si specifica l'opzione `-from-secondary`, SnapManager ripristina i dati dalle copie Snapshot sullo storage primario.

Non è possibile utilizzare l'opzione `-from-secondary` se il backup esiste sullo storage primario; il backup primario deve essere liberato prima di poter ripristinare un backup dallo storage secondario. Se si utilizza un volume temporaneo, è necessario specificare il volume utilizzando l'opzione `-temp-volume`.

Specificare l'opzione `-copy-id` ogni volta che si specifica l'opzione `-from-secondary`. Se nel sistema di storage secondario sono presenti più backup, viene utilizzata l'opzione `-copy-id` per specificare quale copia di backup

nello storage secondario deve essere utilizzata per l'operazione di ripristino.



Se si utilizza Data ONTAP in modalità 7, è necessario specificare un valore valido per l'opzione -copy-id. Tuttavia, se si utilizza Clustered Data ONTAP, l'opzione -copy-id non è richiesta.

Durante il ripristino dei dati dallo storage secondario, SnapManager tenta innanzitutto di ripristinare i dati direttamente dal sistema di storage secondario al sistema di storage primario (senza coinvolgere l'host). Se SnapManager non è in grado di eseguire questo tipo di ripristino (ad esempio, se i file non fanno parte del file system), SnapManager eseguirà un ripristino della copia del file sul lato host. SnapManager offre due metodi per eseguire un ripristino della copia del file sul lato host dallo storage secondario. Il metodo selezionato da SnapManager viene configurato nel file smo.config.

- Se restore.secondaryAccessPolicy = diretto, SnapManager clona i dati sullo storage secondario, monta i dati clonati dal sistema di storage secondario sull'host, quindi copia i dati dal clone nell'ambiente attivo.

Questo è il criterio di accesso secondario predefinito.

- Se restore.secondaryAccessPolicy = indiretto, SnapManager copia prima i dati in un volume temporaneo sullo storage primario, monta i dati dal volume temporaneo all'host, quindi copia i dati dal volume temporaneo nell'ambiente attivo.

Questo criterio deve essere utilizzato solo se l'host non dispone di accesso diretto al sistema di storage secondario. I ripristini con il metodo indiretto richiedono il doppio del tempo rispetto al metodo diretto, poiché vengono create due copie dei dati.

a. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Ripristinare un database completo se il backup selezionato esiste sullo storage primario	Immettere il seguente comando: smo backup restore -profileprofile_name-labellabel-complete -recover -alllogs[-copy-idid]
Ripristinare un database completo se il backup selezionato non esiste sullo storage primario	Immettere il seguente comando: smo backup restore -profileprofile_name-labellabel-complete -recover -alllogs-from-secondary [-temp-volume <temp_volume>] [-copy-idid]

Esempio

Il seguente comando ripristina un backup protetto dal sistema di storage secondario:

```
smo backup restore -profile PAYDB -label daily_monday -complete  
-recover alllogs -from-secondary -copy-id 3042 -temp-volume  
smo_scratch_restore_volume  
Operation Id [8abc011215d385920115d38599470001] succeeded.
```

Clonazione di backup protetti

È possibile utilizzare SnapManager per clonare una copia di un backup protetto.

L'host (selezionato per il clone) deve avere accesso allo storage secondario utilizzando lo stesso protocollo di storage (ad esempio, SAN o NAS).

È possibile utilizzare l'opzione `-from-secondary` per specificare che si desidera clonare dallo storage secondario.

Specificare l'opzione `-copy-id` ogni volta che si specifica l'opzione `-from-secondary`. Se nel sistema di storage secondario sono presenti più backup, viene utilizzata l'opzione `-copy-id` per specificare quale copia di backup nello storage secondario deve essere utilizzata per la clonazione.



Se si utilizza Data ONTAP in modalità 7, è necessario specificare un valore valido per l'opzione `-copy-id`. Tuttavia, se si utilizza Clustered Data ONTAP, l'opzione `-copy-idoption` non è richiesta.

L'eliminazione dei cloni dei backup protetti sui sistemi di storage secondari potrebbe non riuscire. Questo problema si verifica quando l'ora di sistema dei sistemi di storage primario e secondario non è sincronizzata.

1. Creare un clone di una copia di backup protetta: `Clone smo create -backup-label backup_name -newsid new_sid-label clone_label-profile profile_name-clonespec full_path_to_clonespec file-from-secondary -copy-id id`

Esempio

```
smo clone create -label testdb_clone_clstest
-profile sys_db_finance -from-secondary -copy-id 3042
sys_db_finance_sept_08
```

SnapManager per Oracle utilizza Protection Manager per proteggere un backup del database

SnapManager per Oracle e Protection Manager, se installato rispettivamente su un host UNIX e sul server, consente all'amministratore del database SnapManager di configurare ed eseguire backup del database Oracle basati su policy nello storage secondario, e ripristinare, se necessario, i dati di cui è stato eseguito il backup dallo storage secondario a quello primario.

Nell'esempio seguente, un amministratore di database, che utilizza SnapManager, crea un profilo per un backup locale sullo storage primario e un altro profilo per un backup protetto sullo storage secondario. Quindi, questo DBA collabora con l'amministratore dello storage di rete, che utilizza la console di Protection Manager, per configurare un backup basato su policy del database dallo storage primario a quello secondario.

Dettagli del database di destinazione

Questo esempio di protezione integrata del database descrive la protezione di un database delle retribuzioni. Nell'esempio vengono utilizzati i seguenti dati.

L'amministratore del database (DBA) di TechCo, un'azienda con 3000 persone con sede ad Atlanta, deve creare un backup coerente del database delle retribuzioni di produzione, PAYDB. La strategia di protezione per il backup su storage primario e secondario richiede che DBA e l'amministratore dello storage collaborino per eseguire il backup del database Oracle sia localmente sullo storage primario che in remoto, su storage

secondario in una posizione remota.

- **Informazioni sul profilo**

Quando si crea un profilo in SnapManager, sono necessari i seguenti dati:

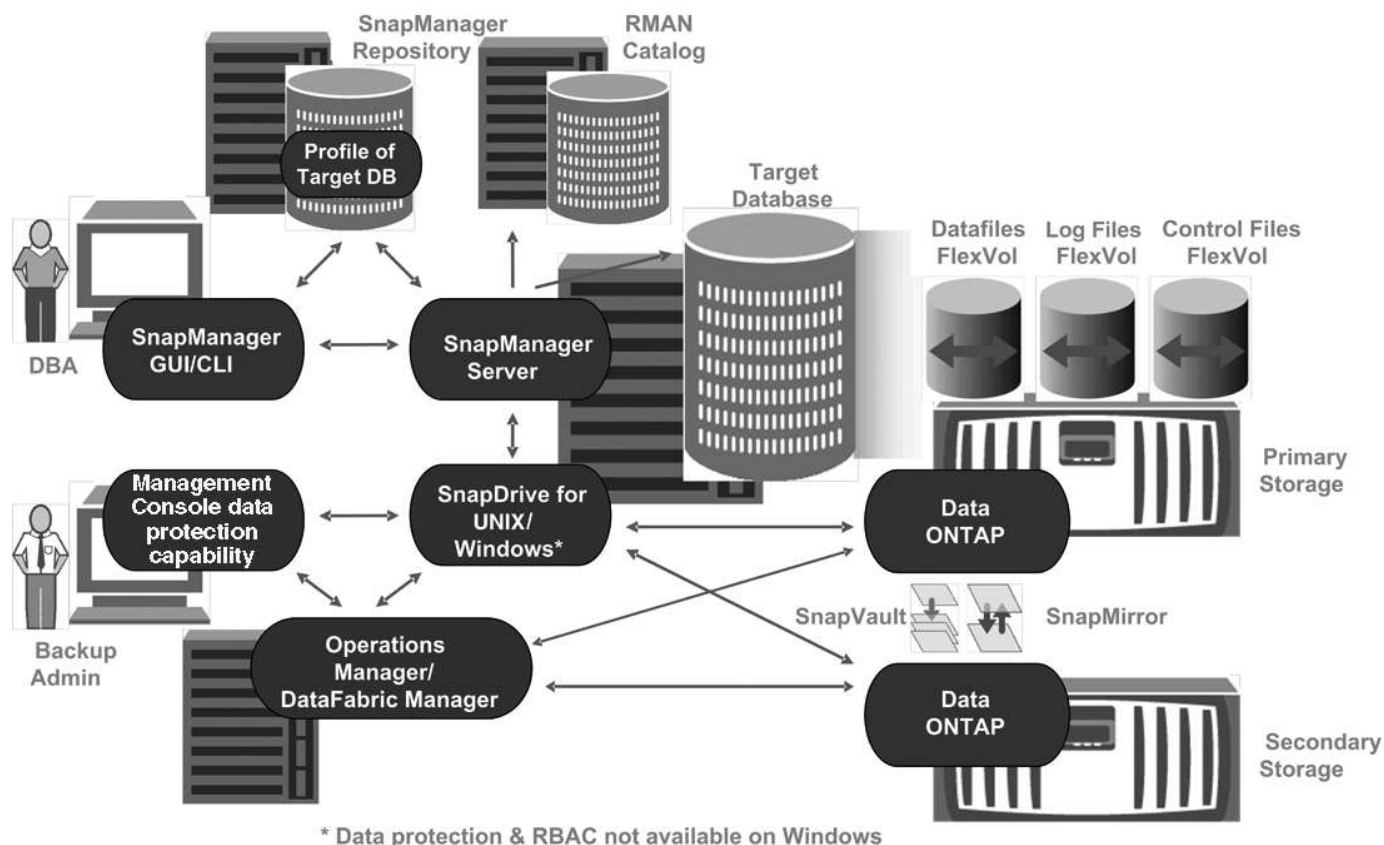
- Nome database: PAYDB
- Nome host: payroll.techco.com
- ID database: Payrolldb
- Nome profilo: Payroll_prod
- Connection mode (modalità di connessione): Autenticazione del database
- Schema di denominazione Snapshot: smo_hostname_dbsid_smopprofile_scope_mode_smid (che si traduce in "smo_payroll.xyz.com_payrolldb_payroll_prod_f_h_x")

Configurazione e topologia dello storage primario e secondario

In questo esempio, la società TechCo esegue il proprio database delle retribuzioni su un server di database che è anche un host SnapManager per Oracle e memorizza i dati del database delle retribuzioni e i file di configurazione sui sistemi di storage primari presso la sede centrale dell'azienda. Il requisito aziendale è quello di proteggere il database con backup giornalieri e settimanali sullo storage locale e backup su sistemi storage in un sito di storage secondario a cinquanta miglia di distanza.

L'illustrazione seguente mostra i componenti della funzionalità di protezione dei dati di SnapManager per Oracle e della console di gestione NetApp necessari per supportare la protezione di backup locale e secondario.

Architecture



Per gestire il database delle retribuzioni e supportarne la protezione di backup locale e secondario, come illustrato nella figura precedente, viene utilizzata la seguente implementazione.

• Host SnapManager

L'host SnapManager, payroll.techco.com, si trova presso la sede centrale dell'azienda e viene eseguito su un server UNIX, che esegue anche il programma di database che genera e gestisce il database delle retribuzioni.

◦ Connessioni

Per supportare il backup locale e la protezione del backup secondario, l'host SnapManager dispone di connessioni di rete ai seguenti componenti:

- SnapManager per client Oracle
- Repository SnapManager, che esegue il programma di database, SnapDrive per UNIX e SnapManager
- Sistemi storage primari
- Sistemi storage secondari
- Server DataFabric Manager

◦ Prodotti installati

L'host SnapManager viene installato con i seguenti prodotti per questo esempio:

- Server SnapManager
- SnapDrive per UNIX
- Utility host

• **Sistemi di storage primario TechCo**

Il database delle retribuzioni, inclusi i file di dati, i file di log e i file di controllo associati, si trova sui sistemi di storage primari. Questi dispositivi si trovano nella sede centrale della società TechCo insieme all'host SnapManager e alla rete che collega lo storage primario e l'host SnapManager. Gli ultimi aggiornamenti e transazioni del database delle retribuzioni vengono scritti nei sistemi di storage primari. Le copie Snapshot, che forniscono protezione di backup locale del database delle retribuzioni, risiedono anche nei sistemi di storage primario.

◦ **Connessioni**

Per supportare la protezione di backup secondario, i sistemi di storage primario dispongono di connessioni di rete ai seguenti componenti:

- Host SnapManager che esegue il programma di database, SnapDrive per UNIX e SnapManager
- Sistemi storage secondari
- Server DataFabric Manager

◦ **Prodotti installati**

Per questo esempio, è necessario abilitare le seguenti licenze su questi sistemi:

- Data ONTAP 7.3.1 o versione successiva
- SnapVaultData ONTAP primario
- FlexVol (richiesto per NFS)
- SnapRestore
- Protocollo NFS

• **Sistemi storage secondari TechCo**

I sistemi di storage secondari, situati in un sito di storage secondario connesso alla rete a cinquanta miglia di distanza, vengono utilizzati per memorizzare i backup secondari del database delle retribuzioni.

◦ **Connessioni**

Per supportare la protezione di backup secondario, i sistemi di storage secondari dispongono di connessioni di rete ai seguenti componenti:

- Sistemi storage primari
- Server DataFabric Manager

◦ **Prodotti installati**

Per questo esempio, è necessario abilitare le seguenti licenze sui sistemi di storage secondari:

- Data ONTAP
- SnapVaultData ONTAP secondario
- SnapRestore

- FlexVol (richiesto per NFS)
- Protocollo NFS

• **Server DataFabric Manager**

Il server DataFabric Manager, techco_dfm, si trova nella sede centrale dell'azienda in una posizione accessibile dall'amministratore dello storage. Il server DataFabric Manager, tra le altre funzioni, coordina le attività di backup tra lo storage primario e secondario.

◦ **Connessioni**

Per supportare la protezione di backup secondario, il server DataFabric Manager mantiene le connessioni di rete ai seguenti componenti:

- Console di gestione NetApp
- Sistemi storage primari
- Sistemi storage secondari

◦ **Prodotti installati**

Il server DataFabric Manager è concesso in licenza per i seguenti prodotti server per questo esempio:

- DataFabric Manager

• **Repository SnapManager**

Il repository SnapManager, situato su un server dedicato, memorizza i dati relativi alle operazioni eseguite da SnapManager, ad esempio il tempo di backup, tablespace e datafile di cui è stato eseguito il backup, i sistemi di storage utilizzati, i cloni creati e le copie Snapshot create. Quando un DBA tenta un ripristino completo o parziale, SnapManager esegue una query nel repository per identificare i backup creati da SnapManager per Oracle per il ripristino.

◦ **Connessioni**

Per supportare la protezione di backup secondario, i sistemi di storage secondari dispongono di connessioni di rete ai seguenti componenti:

- Host SnapManager
- SnapManager per client Oracle

• **NetApp Management Console**

NetApp Management Console è la console di interfaccia utente grafica utilizzata dall'amministratore dello storage per configurare pianificazioni, policy, set di dati e assegnazioni di pool di risorse per abilitare il backup su sistemi storage secondari, accessibili all'amministratore dello storage.

◦ **Connessioni**

Per supportare la protezione di backup secondario, NetApp Management Console dispone di connessioni di rete ai seguenti componenti:

- Sistemi storage primari
- Sistemi storage secondari
- Server DataFabric Manager

- **SnapManager per client Oracle**

Il client SnapManager per Oracle è l'interfaccia utente grafica e la console della riga di comando utilizzati dall'amministratore di database per le retribuzioni in questo esempio per configurare ed eseguire backup e backup locali sullo storage secondario.

- **Connessioni**

Per supportare il backup locale e la protezione del backup secondario, il client SnapManager per Oracle dispone di connessioni di rete ai seguenti componenti:

- Host SnapManager
- Repository SnapManager, che esegue il programma di database, SnapDrive per UNIX e SnapManager
- Host del database (se separato dall'host che esegue SnapManager)
- Server DataFabric Manager

- **Prodotti installati**

Per supportare il backup locale e la protezione del backup secondario, è necessario installare il software client SnapManager per Oracle su questo componente.

Pianificazione del backup e strategia di conservazione

Il DBA desidera garantire che i backup siano disponibili in caso di perdita di dati, in caso di disastro e per motivi normativi. Ciò richiede una policy di conservazione attentamente studiata per i vari database.

Per il database delle retribuzioni in produzione, il DBA aderisce alla seguente strategia di conservazione TechCo:

Frequenza di backup	Durata della conservazione	Tempi di backup	Tipo di storage
Una volta al giorno	10 giorni	19:00	Primario (locale)
Una volta al giorno	10 giorni	19:00	Secondario (archivio)
Una volta alla settimana	52 settimane	Sabato 1:00	Secondario (archivio)

- **Vantaggi del backup locale**

Il backup locale giornaliero offre una protezione del database istantanea, utilizza una larghezza di banda di rete pari a zero, utilizza un minimo di spazio di storage aggiuntivo, fornisce un ripristino istantaneo e offre funzionalità di backup e ripristino di precisione.

Poiché i backup settimanali finali del database delle retribuzioni vengono conservati per un minimo di 52 settimane in un sito di storage secondario, non è necessario conservare i backup giornalieri per più di 10 giorni.

- **Vantaggi del backup protetto**

I backup giornalieri e settimanali sullo storage secondario in una posizione remota garantiscono che, se i dati nel sito di storage primario vengono danneggiati, il database di destinazione rimane protetto e può essere ripristinato dallo storage secondario.

I backup giornalieri sullo storage secondario vengono eseguiti per proteggersi dai danni al sistema di storage primario. Poiché i backup settimanali finali del database delle retribuzioni vengono conservati per un minimo di 52 settimane, non è necessario conservare i backup giornalieri per più di 10 giorni.

Riepilogo del flusso di lavoro per il backup del database locale e secondario

In questo esempio, il DBA (utilizzando SnapManager) e l'amministratore dello storage (utilizzando la funzionalità di protezione dei dati della console di gestione NetApp) coordinano le azioni per configurare il backup locale e secondario (noto anche come backup protetto) del database di destinazione.

La sequenza di azioni eseguite è riassunta come segue:

- **Configurazione del pool di risorse secondario**

L'amministratore dello storage utilizza la funzionalità di protezione dei dati di NetApp Management Console per configurare un pool di risorse di sistemi storage nel sito secondario che può essere utilizzato per memorizzare il backup del database delle retribuzioni.

- **Pianificazione del backup secondario**

L'amministratore dello storage utilizza la funzionalità di protezione dei dati di NetApp Management Console per configurare le pianificazioni di backup secondarie.

- **Configurazione del criterio di protezione**

L'amministratore dello storage utilizza la funzionalità di protezione dei dati di NetApp Management Console per configurare una policy di protezione di backup secondaria per il database di destinazione. Il criterio di protezione include le pianificazioni e specifica il tipo di protezione di base per implementare la protezione di backup (backup, mirroring o una combinazione di entrambi) e definisce i criteri di conservazione dei nomi per i nodi di storage primari, secondari e talvolta terziari.

- **Configurazione del profilo del database e assegnazione dei criteri di protezione**

L'amministratore di database utilizza SnapManager per creare o modificare un profilo del database di destinazione che supporti il backup secondario. Durante la configurazione del profilo, l'amministratore di database:

- Abilita la protezione del backup sullo storage secondario.
- Assegna a questo profilo la nuova policy di protezione creata e recuperata dalla funzionalità di protezione dei dati di NetApp Management Console.

L'assegnazione della policy di protezione include automaticamente il database di destinazione in un set di dati con funzionalità di protezione dei dati di NetApp Management Console parzialmente sottoposto a provisioning, ma non conforme. Una volta eseguito il provisioning completo, la configurazione del set di dati consente il backup del database di destinazione sullo storage secondario.

Il nome del dataset utilizza la seguente sintassi: smo_hostname_databasename, che si traduce in "smo_payroll.techco.com_paydb".

- **Provisioning dello storage secondario e terzo**

L'amministratore dello storage utilizza la funzionalità di protezione dei dati di NetApp Management Console per assegnare pool di risorse per il provisioning dei nodi di storage secondari e talvolta terziari (se la policy di protezione assegnata specifica nodi di storage terziari).

- **Backup su storage locale**

L'amministratore di database apre il profilo con la protezione attivata in SnapManager e crea un backup completo sullo storage locale. Il nuovo backup viene visualizzato in SnapManager come pianificato per la protezione, ma non ancora protetto.

- **Conferma backup secondario**

Poiché il backup si basava su un profilo abilitato alla protezione, il backup viene trasferito al backup secondario in base alla pianificazione del criterio di protezione. L'amministratore di database utilizza SnapManager per confermare il trasferimento del backup allo storage secondario. Una volta copiato il backup nello storage secondario, SnapManager modifica lo stato di protezione del backup da "non protetto" a "protetto".

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:

- a. Nell'elenco Variable Token (token variabile), selezionare la variabile **{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. 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>_<profilename> 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".

Ripristino del database dal backup

Se il contenuto attivo del database delle retribuzioni viene accidentalmente perso o distrutto, SnapManager e la funzionalità di protezione dei dati della console di gestione NetApp supportano il ripristino di tali dati da un backup locale o da uno storage secondario.

Utilizzo di SnapManager per Oracle per ripristinare un backup locale sullo storage primario

È possibile ripristinare i backup locali presenti sullo storage primario. L'intero processo viene eseguito utilizzando SnapManager per Oracle.

È inoltre possibile visualizzare in anteprima le informazioni relative a un processo di ripristino del backup. Questa operazione consente di visualizzare informazioni sull'idoneità di ripristino di un backup. SnapManager analizza i dati di un backup per determinare se il processo di ripristino può essere completato utilizzando il ripristino basato su volume o il metodo di ripristino basato su file.

L'anteprima di ripristino mostra le seguenti informazioni:

- Quale meccanismo di ripristino (ripristino rapido, ripristino del file system lato storage, ripristino del file lato storage o ripristino della copia del file lato host) verrà utilizzato per ripristinare ciascun file.
- Perché non sono stati utilizzati meccanismi più efficienti per ripristinare ciascun file.

In anteprima del piano di ripristino, SnapManager non ripristina nulla. L'anteprima mostra informazioni fino a 20 file.

Se si desidera visualizzare in anteprima un ripristino dei file di dati ma il database non è montato, SnapManager monta il database. Se il database non può essere montato, l'operazione non riesce e SnapManager riporta il database al suo stato originale.

1. Nella struttura ad albero del repository, fare clic con il pulsante destro del mouse sul backup che si desidera ripristinare e selezionare **Restore** (Ripristina).
2. Nella pagina iniziale della procedura guidata di ripristino e ripristino, fare clic su **Avanti**.
3. Nella pagina Restore Configuration Information (Ripristina informazioni configurazione), selezionare **complete Datafile/tablespace Restore with Control Files** (completa ripristino file dati/tablespace con file di controllo).
4. Fare clic su **Allow shutdown of database if necessary**.

SnapManager modifica lo stato del database, se necessario. Ad esempio, se il database è offline e deve essere online, SnapManager lo impone online.

5. Nella pagina Recovery Configuration Information (informazioni configurazione ripristino), fare clic su **All Logs** (tutti i registri).

SnapManager ripristina e ripristina il database all'ultima transazione e applica tutti i log richiesti.

6. Nella pagina Restore Source Location Configuration (Configurazione percorso di origine ripristino), visualizzare le informazioni relative al backup su primario e fare clic su **Next** (Avanti).

Se il backup esiste solo sullo storage primario, SnapManager ripristina il backup dallo storage primario.

7. Nella pagina Volume Restore Configuration Information (informazioni di configurazione ripristino volume), selezionare **tentativo di ripristino volume** per tentare il metodo di ripristino volume.
8. Fare clic su **Fallback to file-based restore**.

Questo consente a SnapManager di utilizzare il metodo di ripristino basato su file se non è possibile utilizzare il metodo di ripristino del volume.

9. Fare clic su **Preview** per visualizzare i controlli di idoneità per il ripristino rapido e le informazioni sui controlli obbligatori e sovrascrivibili.

10. Nella pagina Perform operation (Esegui operazione), verificare le informazioni immesse e fare clic su **Restore** (Ripristina).
11. Per visualizzare i dettagli del processo, fare clic su **Dettagli operazione**.

Utilizzo di SnapManager per Oracle per ripristinare i backup dallo storage secondario

Gli amministratori possono ripristinare i backup protetti dallo storage secondario e scegliere come copiare di nuovo i dati nello storage primario.

Prima di tentare di ripristinare il backup, controllare le proprietà del backup e assicurarsi che il backup sia liberato nel sistema di storage primario e protetto sullo storage secondario.

1. Nella struttura ad albero di SnapManager per Oracle Repository, fare clic con il pulsante destro del mouse sul backup che si desidera ripristinare e selezionare **Ripristina**.
2. Nella pagina iniziale della procedura guidata di ripristino e ripristino, fare clic su **Avanti**.
3. Nella pagina Restore Configuration Information (Ripristina informazioni configurazione), fare clic su **complete Datafile/tablespace Restore with Control Files** (completa ripristino file dati/tablespace con file di controllo).
4. Fare clic su **Allow shutdown of database if necessary**, quindi fare clic su **Next**.

SnapManager modifica lo stato del database, se necessario. Ad esempio, se il database è offline e deve essere online, SnapManager lo impone online.

5. Nella pagina Recovery Configuration Information (informazioni configurazione ripristino), fare clic su **All Logs** (tutti i registri). Quindi, fare clic su **Avanti**.

SnapManager ripristina e ripristina il database all'ultima transazione e applica tutti i log richiesti.

6. Nella pagina Restore Source Location Configuration (Configurazione percorso di origine ripristino), selezionare l'ID dell'origine di backup protetta e fare clic su **Next** (Avanti).
7. Nella pagina Volume Restore Configuration Information (informazioni di configurazione ripristino volume), fare clic su **tentativo di ripristino del volume** per tentare il ripristino del volume.
8. Fare clic su **Fallback to file-based restore**.

Questo consente a SnapManager di utilizzare il metodo di ripristino basato su file se non è possibile completare il metodo di ripristino del volume.

9. Per visualizzare i controlli di idoneità per il ripristino rapido e le informazioni sui controlli obbligatori e sovrascrivibili, fare clic su **Anteprima**.
10. Nella pagina Perform operation (Esegui operazione), verificare le informazioni fornite e fare clic su **Restore** (Ripristina).
11. Per visualizzare i dettagli del processo, fare clic su **Dettagli operazione**.

Esecuzione delle operazioni di gestione

È possibile eseguire attività di gestione dopo aver configurato e configurato SnapManager. Queste attività consentono di gestire le normali operazioni oltre al backup, al ripristino e alla clonazione.

Gli amministratori possono eseguire le operazioni utilizzando l'interfaccia grafica utente o l'interfaccia della riga di comando.

Visualizzazione di un elenco di operazioni

È possibile visualizzare un elenco riepilogativo di tutte le operazioni eseguite rispetto a un profilo.

Quando si elencano le operazioni associate a un particolare profilo, è possibile visualizzare le seguenti informazioni:

- Data di inizio e fine dell'operazione
 - Stato del funzionamento
 - ID operazione
 - Tipo di operazione
 - Host su cui è stato eseguito
- a. Per elencare le informazioni riepilogative di tutte le operazioni, utilizzare il seguente comando: `smo operation list profile -profile profile_name-delimiter character [-quiet | -verbose]`

Quando viene specificata l'opzione `-delimitatore`, il comando elenca ogni riga su una riga separata e gli attributi in tale riga sono separati dal carattere specificato.

Informazioni correlate

[Il comando `smo Operation list`](#)

Visualizzazione dei dettagli delle operazioni

È possibile visualizzare informazioni dettagliate su un particolare profilo per verificare l'esito positivo o negativo di un'operazione. Inoltre, consente di determinare le risorse di storage in uso per una determinata operazione.

È possibile visualizzare i seguenti dettagli relativi a una determinata operazione:

- ID operazione
 - Tipo di operazione
 - Se l'operazione è stata forzata
 - Informazioni di runtime, tra cui stato, data di inizio e di fine dell'operazione
 - L'host su cui è stata eseguita l'operazione, inclusi l'ID del processo e la versione di SnapManager
 - Informazioni sul repository
 - Risorse di storage in uso
- a. Per visualizzare le informazioni dettagliate relative a un ID operazione specifico, immettere il seguente comando: `smo operation show -profile profile_name [-label label | -id id] [-quiet | -verbose]`

Informazioni correlate

Invio di comandi da un host alternativo

È possibile eseguire comandi CLI da un host diverso dall'host del database e SnapManager instraderà i comandi immessi all'host appropriato.

Affinché il sistema invii un'operazione all'host corretto, deve prima sapere dove trovare il profilo per l'operazione. In questa procedura, il sistema mantiene il profilo per il repository delle informazioni di mappatura di un file nella home directory dell'utente sull'host locale.

1. Per far sì che la home directory dell'utente locale sia consapevole delle mappature da profilo a repository in modo da poter instradare la richiesta di operazione, immettere il seguente comando: `smo profile sync -repository-dbname repo_dbname-host repo_host-port repo_port-login-username repo_username [-quiet | -verbose]`

Verifica della versione del software SnapManager

È possibile determinare la versione del prodotto in esecuzione sull'host locale eseguendo il comando `version`.

1. Per verificare la versione di SnapManager, immettere il seguente comando: `Versione smo`

Informazioni correlate

[Il comando smo version](#)

Arresto del server host SnapManager

Una volta terminato l'utilizzo di SnapManager, potrebbe essere necessario arrestare il server.

1. Per arrestare il server, immettere il seguente comando, come utente root: `smo_server stop`

Informazioni correlate

[Il comando smo_server stop](#)

Riavvio del server host UNIX di SnapManager

È possibile riavviare il server su un host UNIX utilizzando l'interfaccia CLI.

1. Per riavviare il server, immettere il seguente comando: `smo_server restart`

Disinstallazione del software da un host UNIX

Se il software SnapManager non è più necessario, è possibile disinstallarlo dal server host.

1. Accedere come root.
2. Per arrestare il server, immettere il seguente comando: `smo_server stop`

3. Per rimuovere il software SnapManager, immettere il seguente comando: `UninstallSmo`
4. Dopo il testo introduttivo, premere **Invio** per continuare.

La disinstallazione viene completata.

Informazioni correlate

[Il comando `smo_server stop`](#)

Configurazione di una notifica via email

SnapManager consente di ricevere una notifica via email sullo stato di completamento delle operazioni di database eseguite dal profilo. SnapManager genera il messaggio e-mail e aiuta a intraprendere le azioni appropriate in base allo stato di completamento delle operazioni del database. La configurazione della notifica via email è un parametro facoltativo.

È possibile configurare una notifica e-mail per un singolo profilo come notifica del profilo e per più profili in un database di repository come notifica di riepilogo.

Notifica del profilo

Per un singolo profilo, è possibile ricevere un'e-mail per le operazioni di database riuscite o non riuscite.



Per impostazione predefinita, la notifica e-mail è attivata per le operazioni di database non riuscite.

Notifica di riepilogo

La notifica di riepilogo consente di ricevere un'e-mail di riepilogo sulle operazioni del database eseguite utilizzando più profili. È possibile attivare notifiche orarie, giornaliere, settimanali o mensili.



Da SnapManager 3.3, le notifiche di riepilogo vengono inviate solo se si specifica il server host che deve inviare la notifica. Se si aggiorna SnapManager da una versione precedente alla 3.3, le notifiche di riepilogo potrebbero non essere inviate se non è stato specificato il server host nella configurazione delle notifiche di riepilogo.



Se si crea un repository in un nodo di un database che si trova in un ambiente RAC (Real Application Clusters) e si attiva la notifica di riepilogo, in seguito quando si aggiunge lo stesso repository a un altro nodo del database, l'email di notifica di riepilogo viene inviata due volte.

È possibile utilizzare la notifica a livello di profilo o la notifica di riepilogo alla volta.

SnapManager abilita la notifica via email per le seguenti operazioni di database eseguite dal profilo:

- Creazione di backup sullo storage primario
- Ripristinare i backup
- Creare cloni
- Separare i cloni

- Verificare i backup

Dopo aver creato o aggiornato i profili con la notifica e-mail attivata, è possibile disattivarla. Se si disattiva la notifica e-mail, non si ricevono più avvisi e-mail per le operazioni di database eseguite dal profilo.

L'e-mail ricevuta contiene i seguenti dettagli:

- Nome dell'operazione di database, ad esempio backup, ripristino o clonazione
- Nome del profilo utilizzato per l'operazione del database
- Nome del server host
- Identificatore di sistema del database
- Ora di inizio e fine dell'operazione del database
- Stato dell'operazione del database
- Messaggio di errore, se presente
- Eventuali messaggi di avviso

È possibile configurare quanto segue:

- Mail server per un repository
- Notifica via email per un nuovo profilo
- Notifica via email per un profilo esistente
- Notifica e-mail di riepilogo per più profili in un repository



È possibile configurare la notifica via email sia dall'interfaccia della riga di comando (CLI) che dall'interfaccia grafica utente (GUI).

Configurazione di un server di posta per un repository

SnapManager consente di specificare i dettagli del server di posta da cui inviare gli avvisi e-mail.

SnapManager consente di specificare il nome host o l'indirizzo IP del server di posta del mittente e il numero di porta del server di posta per un nome di database del repository che richiede la notifica via email. È possibile configurare il numero di porta del server di posta in un intervallo compreso tra 0 e 65535; il valore predefinito è 25. Se si richiede l'autenticazione per l'indirizzo e-mail, è possibile specificare il nome utente e la password.

È necessario specificare il nome o l'indirizzo IP del server host che gestisce la notifica e-mail.

1. Per configurare il server di posta per l'invio di avvisi e-mail, immettere il seguente comando: `smo notification set -sender-email email_address-mailhost mailhost-mailport mailport [-Authentication-username-password password] -repository-port repo_port-dbname repo_service_name-ostrepo_host-login -username_username`

Le altre opzioni per questo comando sono le seguenti:

`[-force]` (forza)

Per effettuare le seguenti operazioni...	Quindi...
Per specificare l'indirizzo e-mail del mittente.	Specificare l'opzione -sender-email. Da SnapManager 3.2 per Oracle, è possibile includere il trattino (-) specificando il nome di dominio dell'indirizzo e-mail. Ad esempio, è possibile specificare l'indirizzo e-mail del mittente come - sender-emailuser@org-corp.com .
Per specificare il nome host o l'indirizzo IP del server di posta del mittente.	Specificare l'opzione -mailhost.
Per specificare il numero di porta del server di posta elettronica per un nome di database del repository che richiede la notifica via email. È possibile configurare il numero di porta del server di posta in un intervallo compreso tra zero e 65535; il valore predefinito è 25.	Specificare l'opzione -mailport.
Specificare il nome utente e la password se si richiede l'autenticazione per l'indirizzo e-mail.	Specificare l'opzione -Authentication seguita dal nome utente e dalla password.

Nell'esempio seguente viene configurato il server di posta.

```
smo notification set -sender-email admin1@org.com -mailhost
hostname.org.com -mailport 25 authentication -username admin1 -password
admin1 -repository -port 1521 -dbname SMOREPO -host hotspur -login
-username grabal21 -verbose
```

Configurazione della notifica e-mail per un nuovo profilo

Quando si crea un nuovo profilo, è possibile configurare per ricevere una notifica via email al completamento dell'operazione del database.

- È necessario configurare l'indirizzo e-mail da cui vengono inviati gli avvisi.
- È necessario utilizzare un elenco separato da virgole per più indirizzi e-mail.

Assicurarsi che non vi sia spazio tra la virgola e l'indirizzo e-mail successivo.

- Immettere il seguente comando: `smo profile create -profileprofile [-profile-passwordprofile_password] -repository-dbnamerepo_service_name-hostrepo_host-portrepo_port-login-username -username_username_username_name_db_host [-siddsdpub][-nomespaint.names.com] {-[-names.com] [-]} -nomespaint.com [-names.com]-names.com [-names.com]-names.com--names.com] nome_nome_account [-] [-nomeself]_nome_account [-nomeself]_nome_account [-] [-nomeself]_nome_nome_account [-nomeself] [-nomeself]_nome_nome_nome_nome_nome [-nomeself]_nomeself] [-nomeself]_nome_nome`

Le altre opzioni per questo comando sono le seguenti:

[-force] (forza)



SnapManager supporta fino a 1000 caratteri per gli indirizzi e-mail.

Quando si crea un backup dei file di dati e dei file di log di archiviazione insieme utilizzando il profilo (per la creazione di backup del log di archiviazione separati) e la creazione del backup del file di dati non riesce, viene inviata una notifica e-mail con il backup dei dati come nome dell'operazione invece del backup dei dati e del backup dei log di archiviazione. Una volta eseguita correttamente l'operazione di backup del file di dati e del file di log dell'archivio, viene visualizzato il seguente output:

```
Profile Name      : PROF_31
Operation Name    : Data Backup and Archive Logs Backup
Database SID      : TENDB1
Database Host     : rep01.rtp.org.com
Start Date        : Fri Sep 23 13:37:21 EDT 2011
End Date          : Fri Sep 23 13:45:24 EDT 2011
Status            : SUCCESS
Error messages    :
```

Nell'esempio seguente viene visualizzata la notifica e-mail configurata durante la creazione di un nuovo profilo:

```
smo profile create -profile sales1 -profile-password sales1 -repository
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username oba5
-database -dbname DB1 -host 10.72.197.142 -sid DB1 -osaccount oracle
-osgroup dba -notification -success -email admin1@org.com -subject
{profile}_{operation-name}_{db-sid}_{db-host}_{start-date}_{end-
date}_{status}
```

Personalizzazione dell'oggetto dell'e-mail per un nuovo profilo

È possibile personalizzare l'oggetto dell'e-mail per il nuovo profilo al momento della creazione.

Puoi personalizzare l'oggetto dell'email usando il modello {profile}_{nome-operazione}_{db-sid}_{db-host}_{data-inizio}_{data-fine}_{stato} o inserisci il tuo testo.

Nome della variabile	Descrizione	Valore di esempio
profilo	Nome del profilo utilizzato per l'operazione del database	PROF1
nome-operazione	Nome operazione database	Backup, backup dei dati, backup dei dati e dei registri di archiviazione
db-sid	SID del database	DB1

Nome della variabile	Descrizione	Valore di esempio
db-host	Nome del server host	Host
data di inizio	Ora di inizio dell'operazione del database nel formato mmdd:hh:ss yyyy	Aprile 27 21:00:45 PST 2012
data di fine	Ora di fine dell'operazione del database nel formato mmdd:hh:ss yyyy	Aprile 27 21:10:45 PST 2012
stato	Stato operativo del database	Successo

Se non si fornisce alcun valore per le variabili, SnapManager visualizza il seguente messaggio di errore: Valori mancanti -subject.

1. Immettere il seguente comando: `smo profile create -profileprofile [-profile-passwordprofile_password] -repository-dbnamerepo_service_name-hostrepo_host-portrepo_port-login-username-username -username_username_name_db_host [-siddsdpub] [-nomespaint.com] {-name} [-nomespaint.com] [-} }}-nomes.com] [-nomes.com]--nomes.com]-nomes.com] [--nomes.com] [-nomes.com]-nomeself] nomeself] [-nomeself-] [-nomeself-nomeself]_nome_nome_nome] [-nomeself] [-nomeself] nome_nome_nome_nome] [-nomeself]] [-]_nome_nome_nome_nome_nomeself]_nome`

Di seguito viene riportato un esempio che mostra il modello dell'oggetto dell'e-mail:

```
smo profile create -profile sales1 -profile-password admin1 -repository
-database dbname repo2 -host 10.72.197.133 -port 1521 -login -username admin2
-database dbname DB1 -host 10.72.197.142 -sid DB1
-osaccount oracle -osgroup dba -profile-notification -success -email
admin@org.com -subject {profile}_{operation-name}_{db-sid}_{db-
host}_{start-date}_{end-date}_{status}
```

Configurazione della notifica e-mail per un profilo esistente

Quando si aggiorna un profilo, è possibile configurare per ricevere una notifica via email al completamento dell'operazione di database.

- È necessario configurare l'indirizzo e-mail da cui vengono inviati gli avvisi.
- È necessario inserire un singolo indirizzo e-mail o più indirizzi e-mail a cui verranno inviati gli avvisi.

È possibile utilizzare un elenco separato da virgole per più indirizzi. Assicurarsi che non vi sia spazio tra la virgola e l'indirizzo e-mail successivo. In alternativa, è possibile aggiungere un oggetto all'e-mail.

- a. Immettere il seguente comando: `smo profile update -profileprofile [-profile-passwordprofile_password][-database-dbnamedb_dbname-host db_host [-siddb_sid] [-login -username db_username -password_db_port db_port] [{-rman{-controlfile | {-login -nomeaccount [-nomeutente] nsutaprotect] [-nomeaccount [-nomeutente]-nomeaccount [-nomeutente]_email [-nomeutente]_nsnomeutente]_nsnomeaccount [-nomeutente]_nsnomeaccount [-`

```
nomeutente]_nsnomeutente]_email [-nomeutente]_nsnomeutente]_email [-  
nomeutente]_nsnomeutente]_nsnomeutente]_password] [-nomeutente] [-  
}}}]_nsnomeutente]_password_password_chiave_chiave_chiave] [
```

È possibile utilizzare l'opzione Success per ricevere una notifica solo per le operazioni di database riuscite e l'opzione failure per ricevere una notifica solo per le operazioni di database non riuscite.

Personalizzazione dell'oggetto e-mail per un profilo esistente

SnapManager consente di personalizzare il modello di oggetto dell'e-mail per un profilo esistente aggiornando tale profilo. Questo modello di soggetto personalizzato è applicabile solo al profilo aggiornato.

1. Immettere il seguente comando: `smo profile update -profileprofile [-profile-passwordprofile_password][[-database-dbnamedb_dbname-host db_host [-siddb_sid] [-login -username db_username -password_db_port db_port] [{-rman{-controlfile | {-login -nomeaccount [-nomeutente] [-nomeutente]_nsutaprotect] [-nomeaccount [-nomeutente]-nomeaccount [-nomeutente]_email [-nomeutente]_nsnomeutente]_nsnomeaccount [-nomeutente]_nsnomeaccount [-nomeutente]_nsnomeutente]_email [-nomeutente]_nsnomeutente]_email [-nomeutente]_nsnomeutente]_password] [-nomeutente] [-}}}]_nsnomeutente]_password [-]_nsnomeutente]_password`

Nell'esempio seguente viene mostrato un modello di oggetto dell'e-mail:

```
smo profile update -profile sales1 -profile-password sales1 -repository  
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username admin2  
-database -dbname DB1 -host 10.72.197.142 -sid DB1  
-osaccount oracle -osgroup dba -profile-notification -success -email  
admin@org.com -subject {profile}_{operation-name}_{db-sid}_{db-  
host}_{start-date}_{end-date}_{status}
```

Configurazione della notifica email di riepilogo per più profili

SnapManager consente di configurare una notifica e-mail di riepilogo per più profili in un database di repository.

È possibile impostare l'host del server SnapManager come host di notifica da cui l'email di notifica di riepilogo viene inviata ai destinatari. Se il nome host o l'indirizzo IP del server SnapManager viene modificato, è possibile aggiornare anche l'host di notifica.

È possibile selezionare uno degli orari di pianificazione in cui si desidera ricevere una notifica via email:

- Ogni ora: Per ricevere una notifica via email ogni ora
- Daily (giornaliero): Per ricevere una notifica via email ogni giorno
- Settimanale: Per ricevere una notifica via email ogni settimana
- Mensile: Per ricevere una notifica via email mensile

Per ricevere le notifiche relative alle operazioni eseguite con tali profili, è necessario inserire un singolo indirizzo e-mail o un elenco separato da virgole. Quando si immettono più indirizzi e-mail, assicurarsi che non

Aggiunta di un profilo esistente alle notifiche email di riepilogo

SnapManager consente di aggiungere un profilo esistente a una notifica email di riepilogo durante l'aggiornamento del profilo.

1. Immettere il seguente comando: `smo profile update -profileprofile_name [-profile-passwordprofile_password] -repository-dbnamerepo_service_name-hostrepo_host-portrepo_port-login-username-username-username-username][-{-contacourly}[-nomespaint.com]_nomespaint.com [-{_nomespaint.com} [-nomespaint.com]_nomespaint.com] [-} }}_nomespaint.com]_nomespaint.com] [-_nomes.com]_nome_nomespaint.com] [-_nomespaint.com] [-nomespaint.com]_nome_nomes.com] [-_nomes.com]_nomes.com]_nomes.com] [-nomes.com]_nomes.com] [-_nome_nomes.com]_nomes.com]_nomes.com] [-] [-nomes.com]_nomes.com]_nomes.com]_nom`

Disattivazione della notifica e-mail per più profili

Dopo aver attivato la notifica e-mail di riepilogo per più profili, è possibile disattivarli per non ricevere più avvisi e-mail.

SnapManager consente di disattivare la notifica e-mail di riepilogo per le operazioni di database eseguite dal profilo. Dalla CLI di SnapManager, immettere il comando di notifica `remove-summary-notification` per disattivare la notifica email di riepilogo per più profili e il nome del database del repository per cui non è richiesta la notifica email.

1. Per disattivare la notifica di riepilogo per più profili in un database di repository, immettere il seguente comando: `smo notification remove-summary-notification -repository-portrepo_port -dbnamerepo_service_name-ostrepo_host-login-username_username`

Nell'esempio seguente viene illustrata la disattivazione della notifica di riepilogo per più profili in un database di repository:

```
smo notification remove-summary-notification -repository -port 1521
-dbname repo2 -host 10.72.197.133 -login -username oba5
```

Creazione di script e file di specifica delle attività per le operazioni SnapManager

SnapManager per Oracle utilizza un file XML (Extensible Markup Language) con specifica di attività che indica le attività preliminari e successive per le operazioni di backup, ripristino e clonazione. È possibile aggiungere i nomi degli script di pre-task e post-task nel file XML per le attività da eseguire prima o dopo le operazioni di backup, ripristino e clonazione.

In SnapManager (3.1 o versioni precedenti), è possibile eseguire gli script di pre-task e post-task solo per l'operazione di clone. In SnapManager (3.2 o versioni successive) per Oracle, è possibile eseguire gli script di pre-task e post-task per le operazioni di backup, ripristino e clonazione.

In SnapManager (3.1 o versioni precedenti), la sezione delle specifiche delle attività fa parte del file XML delle specifiche dei cloni. A partire da SnapManager 3.2 per Oracle, la sezione relativa alle specifiche delle attività è un file XML separato.



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.

In SnapManager (3.2 o versioni successive) per Oracle, l'utente deve assicurarsi che vengano soddisfatte le seguenti condizioni per il successo delle operazioni SnapManager:

- Per le operazioni di backup e ripristino, utilizzare il file XML delle specifiche dell'attività.
- Per l'operazione di cloni, fornire due file di specifica: Un file XML di specifica di cloni e un file XML di specifica di attività.

Se si desidera attivare l'attività di pre-task o post-task, è possibile aggiungere il file XML delle specifiche dell'attività.

È possibile creare il file di specifica dell'attività utilizzando l'interfaccia grafica utente (GUI) di SnapManager, l'interfaccia della riga di comando (CLI) o un editor di testo. Per abilitare le funzionalità di modifica appropriate, è necessario utilizzare un'estensione .xml per il file. Si consiglia di salvare questo file in modo da poterlo utilizzare per operazioni di backup, ripristino e clonazione future.

Il file XML delle specifiche delle attività include due sezioni:

- La sezione delle attività preliminari include script che possono essere eseguiti prima delle operazioni di backup, ripristino e clonazione.
- La sezione post-task include script che possono essere eseguiti dopo le operazioni di backup, ripristino e clonazione.

I valori inclusi nelle sezioni pre-task e post-task devono rispettare le seguenti linee guida:

- Task name (Nome attività): Il nome dell'attività deve corrispondere al nome dello script, visualizzato quando si esegue il comando `plugin.sh -describe`.



In caso di mancata corrispondenza, potrebbe essere visualizzato il seguente messaggio di errore: Il file non è stato trovato.

- Parameter name (Nome parametro): Il nome del parametro deve essere una stringa che può essere utilizzata come impostazione di una variabile di ambiente.

La stringa deve corrispondere al nome del parametro nello script personalizzato, visualizzato quando si esegue il comando `plugin.sh -describe`.

È possibile creare il file di specifica in base alla struttura del seguente file di esempio:

```

<task-specification>
  <pre-tasks>
<task>
  <name>name</name>
  <parameter>
    <name>name</name>
    <value>value</value>
  </parameter>
</task>
</pre-tasks>
<post-tasks>
  <task>
    <name>name</name>
    <parameter>
      <name>name</name>
      <value>value</value>
    </parameter>
  </task>
</post-tasks>
</task-specification>

```



Il file XML delle specifiche delle attività non deve contenere alcun criterio.

Dalla GUI di SnapManager, è possibile impostare il valore del parametro e salvare il file XML. È possibile utilizzare la pagina Task abilitazione (abilitazione attività) della procedura guidata Backup Create (creazione backup), della procedura guidata Restore (Ripristino) o Recovery (Ripristino) e della procedura guidata Clone Create (creazione clone) per caricare il file XML delle specifiche attività esistenti e utilizzare il file selezionato per l'attività di pre-task o post-task.

Un'attività può essere eseguita più volte, con combinazioni di parametri e valori uguali o diverse. Ad esempio, è possibile utilizzare un'operazione di salvataggio per salvare più file.



SnapManager utilizza i tag XML forniti nel file di specifica dell'attività per l'attività di pre-elaborazione o post-elaborazione per le operazioni di backup, ripristino e clonazione indipendentemente dall'estensione del file di specifica dell'attività.

Creazione di script di pre-task, post-task e policy

SnapManager consente di creare gli script per l'attività di pre-elaborazione, l'attività di post-elaborazione e le attività di policy delle operazioni di backup, ripristino e clonazione. È necessario posizionare gli script nella directory di installazione corretta per eseguire l'attività di pre-elaborazione, l'attività di post-elaborazione e le attività di policy dell'operazione SnapManager.

Contenuto degli script Pretask e post-task

Tutti gli script devono includere quanto segue:

- Operazioni specifiche (controllo, descrizione ed esecuzione)
- (Facoltativo) variabili di ambiente predefinite
- Codice specifico per la gestione degli errori (codice di ritorno (rc))



Per validare lo script, è necessario includere il codice corretto per la gestione degli errori.

È possibile utilizzare gli script di pretask per molti scopi, ad esempio per ripulire uno spazio su disco prima dell'avvio dell'operazione SnapManager. È anche possibile utilizzare gli script post-task, ad esempio, per valutare se SnapManager dispone di spazio su disco sufficiente per completare l'operazione.

Contenuto dello script dell'attività Policy

È possibile eseguire lo script dei criteri senza utilizzare operazioni specifiche come controllo, descrizione ed esecuzione. Lo script include le variabili ambientali predefinite (opzionali) e il codice specifico per la gestione degli errori.

Lo script dei criteri viene eseguito prima delle operazioni di backup, ripristino e clonazione.

Formato supportato

Un file script shell con estensione .sh può essere utilizzato come prescritt e post-script.

Directory di installazione dello script

La directory in cui si installa lo script influisce sul modo in cui viene utilizzato. È possibile inserire gli script nella directory ed eseguire lo script prima o dopo l'esecuzione delle operazioni di backup, ripristino o clonazione. È necessario inserire lo script nella directory specificata nella tabella e utilizzarlo su base facoltativa quando si specifica l'operazione di backup, ripristino o clonazione.



Prima di utilizzare gli script per l'operazione SnapManager, assicurarsi che la directory dei plug-in disponga dell'autorizzazione eseguibile.

Attività	Backup	Ripristinare	Clonare
Pre-elaborazione	<default_installation_directory>/plugins/backup/create/pre	<default_installation_directory>/plugins/restore/create/pre	<default_installation_directory>/plugins/clone/create/pre
Post-elaborazione	<default_installation_directory>/plugins/backup/create/post	<default_installation_directory>/plugins/restore/create/post	<default_installation_directory>/plugins/clone/create/post
Basato su policy	<default_installation_directory>/plugins/backup/create/policy	<default_installation_directory>/plugins/restore/create/policy	<default_installation_directory>/plugins/clone/create/policy

Posizioni degli script di esempio

Di seguito sono riportati alcuni esempi degli script di pre-task e post-task per le operazioni di backup e clonazione disponibili nel percorso della directory di installazione:

- <default_installation_directory>/plugin/esempi/backup/create/pre
- <default_installation_directory>/plugin/esempi/backup/create/post
- <default_installation_directory>/plugin/esempi/clone/create/pre
- <default_installation_directory>/plugin/esempi/clone/create/post

Cosa è possibile modificare nello script

Se si crea un nuovo script, è possibile modificare solo le operazioni di descrizione ed esecuzione. Ogni script deve contenere le seguenti variabili: Contesto, timeout e parametro.

Le variabili descritte nella funzione descrivi dello script devono essere dichiarate all'inizio dello script. È possibile aggiungere nuovi valori di parametro in Parameter=() e quindi utilizzare i parametri nella funzione Execute.

Script di esempio

Di seguito viene riportato uno script di esempio con un codice di ritorno specificato dall'utente per la stima dello spazio nell'host SnapManager:

```
#!/bin/bash
# $Id:
//depot/prod/capstan/main/src/plugins/unix/examples/backup/create/pre/disk
_space_estimate.sh#5 $
name="disk space estimation ($(basename $0))"
description="pre tasks for estimating the space on the target system"
context=
timeout="0"
parameter=()
EXIT=0
PRESERVE_DIR="/tmp/preserve/$(date +%Y%m%d%H%M%S) "
function _exit {
    rc=$1
    echo "Command complete."
    exit $rc
}
function usage {
    echo "usage: $(basename $0) { -check | -describe | -execute }"
    _exit 99
}
function describe {
    echo "SM_PI_NAME:$name"
    echo "SM_PI_DESCRIPTION:$description"
    echo "SM_PI_CONTEXT:$context"
    echo "SM_PI_TIMEOUT:$timeout"
    IFS=^
    for entry in ${parameter[@]}; do
        echo "SM_PI_PARAMETER:$entry"
    done
}
```

```

done
_exit 0
}
function check {
    _exit 0
}
function execute {
    echo "estimating the space on the target system"
    # Shell script to monitor or watch the disk space
    # It will display alert message, if the (free available) percentage
    # of space is >= 90%
    #
-----
    # Linux shell script to watch disk space (should work on other UNIX
oses )
    # set alert level 90% is default
    ALERT=90
    df -H | grep -vE '^Filesystem|tmpfs|cdrom' | awk '{ print $5 " " $1
}' | while read output;
do
    #echo $output
    usep=$(echo $output | awk '{ print $1}' | cut -d'%' -f1 )
    partition=$(echo $output | awk '{ print $2 }' )
    if [ $usep -ge $ALERT ]; then
        echo "Running out of space \"$partition ($usep%)\", on
$(hostname) as on $(date)" |
        fi
    done
    _exit 0
}
function preserve {
    [ $# -ne 2 ] && return 1
    file=$1
    save=$(echo ${2:0:1} | tr [a-z] [A-Z])
    [ "$save" == "Y" ] || return 0
    if [ ! -d "$PRESERVE_DIR" ] ; then
        mkdir -p "$PRESERVE_DIR"
        if [ $? -ne 0 ] ; then
            echo "could not create directory [$PRESERVE_DIR]"
            return 1
        fi
    fi
    if [ -e "$file" ] ; then
        mv "$file" "$PRESERVE_DIR/."
    fi
    return $?
}

```

```

}
case $(echo $1 | tr [A-Z] [a-z]) in
    -check)    check
                ;;
    -execute)  execute
                ;;
    -describe) describe
                ;;
    *)         echo "unknown option $1"
                usage
                ;;
esac

```

Operazioni negli script di attività

Gli script di pre-task o post-task creati devono seguire una struttura plug-in standard di SnapManager per Oracle.

Gli script di pre-task e post-task devono includere le seguenti operazioni:

- controllare
- descrivi
- eseguire

Se una di queste operazioni non viene specificata nello script di pretask o di post-task, lo script diventa non valido.

Quando si esegue il comando di controllo del plug-in smo per gli script di pre-task o post-task, lo stato restituito degli script visualizza un errore (perché il valore di stato restituito non è zero).

Operazione	Descrizione
controllare	Il server SnapManager esegue il comando plugin.sh -check per garantire che il sistema disponga dell'autorizzazione di esecuzione per gli script dei plug-in. È inoltre possibile includere il controllo delle autorizzazioni del file sul sistema remoto.

Operazione	Descrizione
descrivi	<p data-bbox="820 155 1477 323">Il server SnapManager esegue il comando plugin.sh -describe per ottenere informazioni sullo script e corrispondere agli elementi forniti dal file delle specifiche. Lo script del plug-in deve contenere le seguenti informazioni:</p> <ul data-bbox="844 359 1477 1136" style="list-style-type: none"> • SM_PI_NAME: Nome dello script. Specificare un valore per questo parametro. • SM_PI_DESCRIPTION: Descrizione dello scopo dello script. Specificare un valore per questo parametro. • SM_PI_CONTEXT: Contesto in cui lo script deve essere eseguito, ad esempio root o oracle. Specificare un valore per questo parametro. • SM_PI_TIMEOUT: Il tempo massimo (in millisecondi) in cui SnapManager deve attendere il completamento dell'elaborazione e il termine dell'esecuzione dello script. Specificare un valore per questo parametro. • SM_PI_PARAMETER: Uno o più parametri personalizzati necessari per l'elaborazione dello script del plug-in. Ciascun parametro deve essere elencato in una nuova riga di output e includere il nome del parametro e una descrizione. Al termine dell'elaborazione dello script, il valore del parametro viene fornito allo script da una variabile di ambiente. <p data-bbox="820 1171 1477 1241">Di seguito viene riportato l'output di esempio dello script Followup_Activities.</p> <div data-bbox="820 1276 1477 1818" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre data-bbox="844 1308 1445 1787"> plugin.sh - describe SM_PI_NAME:Followup_activities SM_PI_DESCRIPTION:this script contains follow-up activities to be executed after the clone create operation. SM_PI_CONTEXT:root SM_PI_TIMEOUT:60000 SM_PI_PARAMETER:SCHEMAOWNER:Name of the database schema owner. Command complete.</pre> </div>

Operazione	Descrizione
eeguire	Il server SnapManager esegue il comando plugin.sh -execute per avviare lo script e eseguirlo.

Informazioni correlate

[Il comando smo plugin check](#)

Variabili disponibili negli script delle operazioni per l'operazione di backup

SnapManager fornisce informazioni di contesto sotto forma di variabili di ambiente correlate all'operazione di backup in corso. Ad esempio, lo script può recuperare il nome dell'host originale, il nome del criterio di conservazione e l'etichetta del backup.

La tabella seguente elenca le variabili di ambiente che è possibile utilizzare negli script:

Variabili	Descrizione	Formato
ID_OPERAZIONE_SM	Specifica l'ID dell'operazione corrente	stringa
NOME_PROFILO_SM	Specifica il nome del profilo utilizzato	stringa
SM_SID	Specifica l'identificativo di sistema del database	stringa
SM_HOST	Specifica il nome host del database	stringa
SM_OS_USER	Specifica il proprietario del sistema operativo del database	stringa
SM_OS_GROUP	Specifica il gruppo di sistemi operativi del database	stringa
SM_BACKUP_TYPE	Specifica il tipo di backup (online, offline o automatico)	stringa
SM_BACKUP_LABEL	Specifica l'etichetta del backup	stringa
SM_BACKUP_ID	Specifica l'ID del backup	stringa
SM_BACKUP_RETENTION	Specifica il periodo di conservazione	stringa
SM_BACKUP_PROFILE	Specifica il profilo utilizzato per questo backup	stringa

Variabili	Descrizione	Formato
SM_ALLOW_DATABASE_SHUTDOWN	Specifica se si desidera avviare o chiudere il database. Se necessario, è possibile utilizzare l'opzione -force dall'interfaccia della riga di comando.	booleano
SM_BACKUP_SCOPE	Specifica l'ambito del backup (completo o parziale)	stringa
SM_BACKUP_PROTECTION	Specifica se la protezione del backup è attivata	booleano
SM_TARGET_FILER_NAME	Specifica il nome del sistema di storage di destinazione Nota: se vengono utilizzati più sistemi di storage, i nomi dei sistemi di storage devono essere separati da virgole.	stringa
SM_TARGET_VOLUME_NAME	Specifica il nome del volume di destinazione Nota: il nome del volume di destinazione deve essere preceduto dal nome del dispositivo di archiviazione, ad esempio SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	stringa
SM_HOST_FILE_SYSTEM	Specifica il file system host	stringa
SM_SNAPSHOT_NAMES	Specifica l'elenco Snapshot Nota: il nome delle copie Snapshot deve essere preceduto dal nome del sistema di storage e dal nome del volume. I nomi delle copie Snapshot sono separati da virgole.	array di stringhe
SM_ASM_DISK_GROUPS	Specifica l'elenco dei gruppi di dischi ASM	array di stringhe
SM_ARCHIVE_LOGS_DIRECTORY	Specifica la directory dei log di archiviazione Nota: se i log di archiviazione si trovano in più di una directory, i nomi di tali directory sono separati da virgole.	array di stringhe

Variabili	Descrizione	Formato
SM_REDO_LOGS_DIRECTORY	Specifica la directory dei log di ripristino Nota: se i log di ripristino si trovano in più directory, i nomi di tali directory sono separati da virgole.	array di stringhe
SM_CONTROL_FILES_DIRECTORY	Specifica la directory dei file di controllo Nota: se i file di controllo si trovano in più di una directory, i nomi di tali directory sono separati da virgole.	array di stringhe
SM_DATA_FILES_DIRECTORY	Specifica la directory dei file di dati Nota: se i file di dati si trovano in più di una directory, i nomi di tali directory sono separati da virgole.	array di stringhe
definito_dall'utente	Specifica i parametri aggiuntivi definiti dall'utente. I parametri definiti dall'utente non sono disponibili per i plug-in utilizzati come policy.	definito dall'utente

Variabili disponibili negli script delle operazioni per l'operazione di ripristino

SnapManager fornisce informazioni di contesto sotto forma di variabili di ambiente correlate all'operazione di ripristino in corso. Ad esempio, lo script può recuperare il nome dell'host originale e l'etichetta del backup ripristinato.

La tabella seguente elenca le variabili di ambiente che è possibile utilizzare negli script:

Variabili	Descrizione	Formato
ID_OPERAZIONE_SM	Specifica l'ID dell'operazione corrente	stringa
NOME_PROFILO_SM	Specifica il nome del profilo utilizzato	stringa
SM_HOST	Specifica il nome host del database	stringa
SM_OS_USER	Specifica il proprietario del sistema operativo del database	stringa
SM_OS_GROUP	Specifica il gruppo di sistemi operativi del database	stringa

Variabili	Descrizione	Formato
SM_BACKUP_TYPE	Specifica il tipo di backup (online, offline o automatico)	stringa
SM_BACKUP_LABEL	Specifica l'etichetta di backup	stringa
SM_BACKUP_ID	Specifica l'ID del backup	stringa
SM_BACKUP_PROFILE	Specifica il profilo utilizzato per il backup	stringa
SM_RECOVERY_TYPE	Specifica le informazioni di configurazione del ripristino	stringa
SM_VOLUME_RESTORE_MODE	Specifica la configurazione di ripristino del volume	stringa
SM_TARGET_FILER_NAME	Specifica il nome del sistema di storage di destinazione Nota: se vengono utilizzati più sistemi di storage, i nomi dei sistemi di storage devono essere separati da virgole.	stringa
SM_TARGET_VOLUME_NAME	Specifica il nome del volume di destinazione Nota: il nome del volume di destinazione deve essere preceduto dal nome del dispositivo di archiviazione, ad esempio SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	stringa
SM_HOST_FILE_SYSTEM	Specifica il file system host	stringa
SM_SNAPSHOT_NAMES	Specifica l'elenco Snapshot Nota: il nome delle copie Snapshot deve essere preceduto dal nome del sistema di storage e dal nome del volume. I nomi delle copie Snapshot sono separati da virgole.	array di stringhe
SM_ASM_DISK_GROUPS	Specifica l'elenco dei gruppi di dischi ASM	array di stringhe

Variabili	Descrizione	Formato
SM_ARCHIVE_LOGS_DIRECTORY	Specifica la directory dei log di archiviazione Nota: se i log di archiviazione si trovano in più di una directory, i nomi di tali directory sono separati da virgole.	array di stringhe
SM_REDO_LOGS_DIRECTORY	Specifica la directory dei log di ripristino Nota: se i log di ripristino si trovano in più directory, i nomi di tali directory sono separati da virgole.	array di stringhe
SM_CONTROL_FILES_DIRECTORY	Specifica la directory dei file di controllo Nota: se i file di controllo si trovano in più di una directory, i nomi di tali directory sono separati da virgole.	array di stringhe
SM_DATA_FILES_DIRECTORY	Specifica la directory dei file di dati Nota: se i file di dati si trovano in più di una directory, i nomi di tali directory sono separati da virgole.	array di stringhe

Variabili disponibili negli script di attività per l'operazione di cloni

SnapManager fornisce informazioni di contesto sotto forma di variabili di ambiente correlate all'operazione di cloni eseguita. Ad esempio, lo script può recuperare il nome dell'host originale, il nome del database clone e l'etichetta del backup.

La tabella seguente elenca le variabili di ambiente che è possibile utilizzare negli script:

Variabili	Descrizione	Formato
SM_ORIGINAL_SID	SID del database originale	stringa
SM_ORIGINAL_HOST	Nome host associato al database originale	stringa
SM_ORIGINAL_OS_USER	Proprietario del sistema operativo del database originale	stringa
SM_ORIGINAL_OS_GROUP	Gruppo di sistemi operativi del database originale	stringa
SM_TARGET_SID	SID del database clone	stringa

Variabili	Descrizione	Formato
SM_TARGET_HOST	Nome host associato al database clone	stringa
SM_TARGET_OS_USER	Proprietario del sistema operativo del database clone	stringa
SM_TARGET_OS_GROUP	Gruppo di sistemi operativi del database clone	stringa
SM_TARGET_DB_PORT	Porta del database di destinazione	intero
SM_TARGET_GLOBAL_DB_NAME	Nome del database globale del database di destinazione	stringa
SM_BACKUP_LABEL	Etichetta del backup utilizzato per il clone	stringa

Gestione degli errori negli script personalizzati

SnapManager elabora lo script personalizzato in base ai codici di ritorno specifici. Ad esempio, se lo script personalizzato restituisce un valore pari a 0, 1, 2 o 3, SnapManager continua con il processo di clonazione. Il codice restituito influenza anche il modo in cui SnapManager elabora e restituisce l'output standard dell'esecuzione dello script.

Codice di ritorno	Descrizione	Continuare l'elaborazione dell'operazione
0	Lo script è stato completato correttamente.	Sì
1	Lo script è stato completato correttamente, con messaggi informativi.	Sì
2	Lo script è stato completato, ma include degli avvisi	Sì
3	Lo script non riesce, ma l'operazione continua.	Sì
4 o >4	Lo script non riesce e l'operazione si interrompe.	No

Visualizzazione di script plug-in di esempio

SnapManager include script che è possibile utilizzare come esempio per creare script personalizzati o come base per gli script personalizzati.

Gli script dei plug-in di esempio si trovano nella seguente posizione:

- <default_install_directory>/plugin/esempi/backup/create
- <default_install_directory>/plugin/esempi/clone/create
- <default_install_directory>/plugins/unix/esempi/backup/create/post

La directory che contiene gli script dei plug-in di esempio include le seguenti sottodirectory:

- Policy: Contiene script che, una volta configurati, vengono eseguiti sempre sull'operazione clone.
- Pre: Contiene script che, una volta configurati, vengono eseguiti prima dell'operazione di clonazione.
- Post: Contiene script che, se configurati, vengono eseguiti dopo l'operazione di cloni.

La seguente tabella descrive gli script di esempio:

Nome dello script	Descrizione	Tipo di script
validate_sid.sh	Contiene controlli aggiuntivi per il SID utilizzato nel sistema di destinazione. Lo script verifica che il SID abbia le seguenti caratteristiche: <ul style="list-style-type: none">• Contiene tre caratteri alfanumerici• Inizia con una lettera	Policy
cleanup.sh	Pulisce il sistema di destinazione in modo che sia pronto per memorizzare il clone appena creato. Conserva o elimina file e directory in base alle esigenze.	Pretask
Mirror_the_backup.sh	Esegue il mirroring dei volumi dopo l'esecuzione dell'operazione di backup in un ambiente UNIX quando si utilizza Data ONTAP in 7-Mode o Clustered Data ONTAP.	Post-task
Vault_the_backup_cDOT.sh	Esegue il vault del backup dopo che l'operazione di backup ha luogo in un ambiente UNIX quando si utilizza Clustered Data ONTAP.	Post-task

Gli script forniti con SnapManager utilizzano la shell BASH per impostazione predefinita. Prima di eseguire uno qualsiasi degli script di esempio, è necessario assicurarsi che il supporto per la shell BASH sia installato sul

sistema operativo.

1. Per verificare che si stia utilizzando LA shell BASH, immettere il seguente comando al prompt dei comandi:

```
bash
```

Se non viene visualizzato alcun errore, LA shell BASH funziona correttamente.

In alternativa, è possibile immettere il comando quale-bash al prompt dei comandi.

2. Individuare lo script nella seguente directory:

```
<installdir>/plugin/esempi/clone/create
```

3. Aprire lo script in un editor di script come vi.

Script di esempio

Il seguente script personalizzato di esempio convalida i nomi SID del database e impedisce l'utilizzo di nomi non validi nel database clonato. Include tre operazioni (check, descrivi ed esegui), che vengono chiamate dopo l'esecuzione dello script. Lo script include anche la gestione dei messaggi di errore con i codici 0, 4 e >4.

```
EXIT=0
name="Validate SID"
description="Validate SID used on the target system"
parameter=()

# reserved system IDs
INVALID_SIDS=("ADD" "ALL" "AND" "ANY" "ASC"
              "COM" "DBA" "END" "EPS" "FOR"
              "GID" "IBM" "INT" "KEY" "LOG"
              "MON" "NIX" "NOT" "OFF" "OMS"
              "RAW" "ROW" "SAP" "SET" "SGA"
              "SHG" "SID" "SQL" "SYS" "TMP"
              "UID" "USR" "VAR")

function _exit {
    rc=$1
    echo "Command complete."
    return $rc}

function usage {
    echo "usage: $(basename $0) { -check | -describe | -execute }"
    _exit 99}

function describe {
    echo "SM_PI_NAME:$name"
    echo "SM_PI_DESCRIPTION:$description"
    _exit 0}

function check {
```

```

        _exit 0}

function execute {
    IFS=\$ myEnv=$(env)
    for a in ${parameter[@]}; do
        key=$(echo ${$a} | awk -F':' '{ print $1 }')
        val=$(echo $myEnv | grep -i -w $key 2>/dev/null | awk -F=' ' '{
print $2 }')

        if [ -n "$val" ] ; then
            state="set to $val"
        else
            state="not set"
            #indicate a FATAL error, do not continue processing
            ((EXIT+=4))
        fi
        echo "parameter $key is $state"
    done

    #####
    # additional checks
    # Use SnapManager environment variable of SM_TARGET_SID

    if [ -n "$SM_TARGET_SID" ] ; then
        if [ ${#SM_TARGET_SID} -ne 3 ] ; then
            echo "SID is defined as a 3 digit value, [$SM_TARGET_SID] is not
valid."
            EXIT=4
        else
            echo "${INVALID_SIDS[@]}" | grep -i -w $SM_TARGET_SID >/dev/null
2>&1

            if [ $? -eq 0 ] ; then
                echo "The usage of SID [$SM_TARGET_SID] is not supported by
SAP."

                ((EXIT+=4))
            fi
        fi
    else
        echo "SM_TARGET_SID not set"
        EXIT=4
    fi
    _exit $EXIT}

# Include the 3 required operations for clone plugin
case $(echo "$1" | tr [A-Z] [a-z]) in
-check )      check      ;;
-describe )   describe   ;;

```



```

    -execute )      execute ;;      * )
        echo "unknown option $1"    usage      ;;
esac

```

Creazione di script di attività

È possibile creare gli script di attività di pretask, post-task e policy per le operazioni di backup, ripristino e clonazione, scrivere lo script e includere le variabili di ambiente predefinite nei parametri. È possibile creare un nuovo script o modificare uno degli script di esempio di SnapManager.

Prima di iniziare a creare lo script, assicurarsi che:

- Per eseguire lo script nel contesto di un'operazione SnapManager, è necessario strutturarli in modo particolare.
- È necessario creare lo script in base alle operazioni previste, ai parametri di input disponibili e alle convenzioni del codice di ritorno.
- È necessario includere i messaggi di log e reindirizzare i messaggi ai file di log definiti dall'utente.
 - a. Creare lo script di attività personalizzando lo script di esempio.

Effettuare le seguenti operazioni:

- i. Individuare uno script di esempio nella seguente directory di installazione:

<default_install_directory>/plugin/esempi/backup/create

<default_install_directory>/plugin/esempi/clone/create

- i. Aprire lo script nell'editor degli script.
- ii. Salvare lo script con un nome diverso.
- b. Modificare le funzioni, le variabili e i parametri secondo necessità.
- c. Salvare lo script in una delle seguenti directory:

Script delle operazioni di backup

- <default_install_directory>/plugins/backup/create/pre: Esegue lo script prima che si verifichi l'operazione di backup. Utilizzarlo come opzione quando si specifica la creazione del backup.
- <default_install_directory>/plugins/backup/create/post: Esegue lo script dopo l'operazione di backup. Utilizzarlo come opzione quando si specifica la creazione del backup.
- <default_install_directory>/plugins/backup/create/policy: Esegue sempre lo script prima che si verifichi l'operazione di backup. SnapManager utilizza sempre questo script per tutti i backup nel repository. **Ripristinare gli script delle operazioni**
- <default_install_directory>/plugins/restore/create/pre: Esegue lo script prima che si verifichi l'operazione di backup. Utilizzarlo come opzione quando si specifica la creazione del backup.
- <default_install_directory>/plugins/restore/create/post: Esegue lo script dopo l'operazione di backup. Utilizzarlo come opzione quando si specifica la creazione del backup.
- <default_install_directory>/plugins/restore/create/policy: Esegue sempre lo script prima che si

verifichi l'operazione di backup. SnapManager utilizza sempre questo script per tutti i backup nel repository. **Clone Operation scripts**

- `<default_install_directory>/plugins/clone/create/pre`: Esegue lo script prima che si verifichi l'operazione di backup. Utilizzarlo come opzione quando si specifica la creazione del backup.
- `<default_install_directory>/plugins/clone/create/post`: Esegue lo script dopo l'operazione di backup. Utilizzarlo come opzione quando si specifica la creazione del backup.
- `<default_install_directory>/plugins/clone/create/policy`: Esegue sempre lo script prima che si verifichi l'operazione di backup. SnapManager utilizza sempre questo script per tutti i backup nel repository.

Memorizzazione degli script delle operazioni

È necessario memorizzare gli script delle attività di pre-task, post-task e policy in una directory specifica sul server di destinazione in cui verranno creati i backup o i cloni. Per l'operazione di ripristino, gli script devono essere posizionati nella directory specificata sul server di destinazione in cui si desidera ripristinare il backup.

1. Creare lo script.
2. Salvare lo script in una delle seguenti posizioni:

Per l'operazione di backup

Directory	Descrizione
<code><default_install_directory>/plugins/backup/create/policy</code>	Gli script dei criteri vengono eseguiti prima delle operazioni di backup.
<code><default_install_directory>/plugins/backup/create/pre</code>	Gli script di pre-elaborazione eseguono le operazioni prima del backup.
<code><default_install_directory>/plugins/backup/create/post</code>	Gli script di post-elaborazione vengono eseguiti dopo le operazioni di backup.

Per l'operazione di ripristino

Directory	Descrizione
<code><default_install_directory>/plugins/restore/create/policy</code>	Gli script dei criteri vengono eseguiti prima delle operazioni di ripristino.
<code><default_install_directory>/plugins/restore/create/pre</code>	Gli script di pre-elaborazione vengono eseguiti prima delle operazioni di ripristino.
<code><default_install_directory>/plugins/restore/create/post</code>	Gli script di post-elaborazione vengono eseguiti dopo le operazioni di ripristino.

Per l'operazione di cloni

Directory	Descrizione
<code><default_install_directory>/plugins/clone/create/policy</code>	Gli script dei criteri vengono eseguiti prima delle operazioni di clonazione.
<code><default_install_directory>/plugins/clone/create/pre</code>	Gli script di pre-elaborazione vengono eseguiti prima delle operazioni di cloni.
<code><default_install_directory>/plugins/clone/create/post</code>	Gli script di post-elaborazione vengono eseguiti dopo le operazioni di cloni.

Verifica dell'installazione degli script dei plug-in

SnapManager consente di installare e utilizzare script personalizzati per eseguire varie operazioni. SnapManager fornisce plug-in per le operazioni di backup, ripristino e clonazione, che è possibile utilizzare per automatizzare gli script personalizzati prima e dopo le operazioni di backup, ripristino e clonazione.

1. Immettere il seguente comando:

```
smo plugin check -osaccount nome utente db del sistema operativo
```

Se non si fornisce l'opzione `-osaccount`, la verifica dell'installazione dello script del plug-in avviene per l'utente root piuttosto che per un utente specifico.

Il seguente output indica che gli script `policy1`, `pre-plugin1` e `pre-plugin2` sono stati installati correttamente. Tuttavia, lo script `post-plugin1` non è operativo.

```
smo plugin check
Checking plugin directory structure ...
<installdir>/plugins/clone/policy
  OK: 'policy1' is executable

<installdir>/plugins/clone/pre
  OK: 'pre-plugin1' is executable and returned status 0
  OK: 'pre-plugin2' is executable and returned status 0

<installdir>/plugins/clone/post
  ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

Creazione di un file di specifica dell'attività

È possibile creare i file delle specifiche delle attività utilizzando l'interfaccia utente grafica (GUI), l'interfaccia della riga di comando (CLI) o un editor di testo. Questi file vengono utilizzati per eseguire attività di pre-elaborazione o post-elaborazione delle operazioni di

backup, ripristino o clonazione.

1. Creare un file di specifica dell'attività utilizzando GUI, CLI o un editor di testo.

È possibile creare il file di specifica in base alla struttura del seguente file di esempio:

```
<task-specification>
  <pre-tasks>
    <task>
      <name>name</name>
      <parameter>
        <name>name</name>
        <value>value</value>
      </parameter>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>name</name>
      <parameter>
        <name>name</name>
        <value>value</value>
      </parameter>
    </task>
  </post-tasks>
</task-specification>
```

2. Inserire il nome dello script.
3. Inserire il nome del parametro e il valore assegnato al parametro.
4. Salvare il file XML nella directory di installazione corretta.

Esempio di specifica dell'attività

```

<task-specification>
  <pre-tasks>
    <task>
      <name>clone cleanup</name>
      <description>pre tasks for cleaning up the target
system</description>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>SystemCopy follow-up activities</name>
      <description>SystemCopy follow-up activities</description>
      <parameter>
        <name>SCHEMAOWNER</name>
        <value>SAMSR3</value>
      </parameter>
    </task>
    <task>
      <name>Oracle Users for OS based DB authentication</name>
      <description>Oracle Users for OS based DB
authentication</description>
      <parameter>
        <name>SCHEMAOWNER</name>
        <value>SAMSR3</value>
      </parameter>
      <parameter>
        <name>ORADBUSR_FILE</name>
        <value>\>/mnt/sam/oradbusr.sql</value>\>
      </parameter>
    </task>
  </post-tasks>
</task-specification>

```

Esecuzione di operazioni di backup, ripristino e clonazione utilizzando script prescrittivi e post-script

È possibile utilizzare il proprio script durante l'avvio di un'operazione di backup, ripristino o clonazione. SnapManager visualizza una pagina di abilitazione attività nella procedura guidata di creazione backup, ripristino o ripristino o creazione clone, in cui è possibile selezionare lo script e fornire i valori per i parametri richiesti dallo script.

- Installare gli script dei plug-in nel percorso di installazione corretto di SnapManager.
- Verificare che i plug-in siano installati correttamente utilizzando il comando `smo plugin check`.

- Assicurarsi di utilizzare LA shell BASH.

Nell'interfaccia della riga di comando (CLI), elencare il nome dello script, selezionare i parametri e impostare i valori.

1. Per verificare che si stia utilizzando LA shell BASH, immettere il seguente comando al prompt dei comandi: `bash`

In alternativa, è possibile immettere il comando `qual-bash` al prompt e utilizzare il comando `output` come parametro di avvio dello script.

La shell BASH funziona correttamente se non viene visualizzato un errore.

2. Per l'operazione di backup, inserire l'opzione `-taskspec` e fornire il percorso assoluto del file XML delle specifiche dell'attività per eseguire un'attività di pre-elaborazione o post-elaborazione prima o dopo l'operazione di backup: `smo backup create -profile_name {[full {online | offline | auto} [-retain {hourly | daily | settimanale | mensile | illimitato}] [-verify] | [-data [[filesfiles [files]] | [-tablespaces-tablespaces-tablespaces] [-datalabellabellabel] [-settimanale | {-}-{-}--online | -verify [-sharly] -verify [-sharly] | -sharly] -sharly | -sharing [--untary | -sharly] -sharly | --untary [- [-protect | -noprotect | -protectnow] [-backup-destpath1 [,path2]]] [-exclude-destpath1 [,path2]] [-prunelogs {-all | -untilSCNuntilSCN | -before {dateyyy-MM-dd:mm:ss | -months | -days | -settimane | -she.spacune-spacune-spacune-spaces -}}-spacune -spacune-spaces-spaces] -share -share -share -}-spacing-spaces-spaces-spaces-spaces] -share -share -spacing--`

Se l'operazione del plug-in di backup non riesce, vengono visualizzati solo il nome del plug-in e il codice di ritorno. Lo script del plug-in deve includere i messaggi di log e reindirizzare i messaggi ai file di log definiti dall'utente.

3. Per l'operazione di ripristino del backup, Inserire l'opzione `-taskspec` e fornire il percorso assoluto del file XML della specifica del task per eseguire una pre-elaborazione o un'attività di post-elaborazione prima o dopo l'operazione di ripristino: `smo backup restore -profileprofile_name {-labortologic <label> | -restortunch <id>} {-<files>| -tablespacenglos <tablespaces> | -complete | -controlfiles} [-recover {-alllogs | -<until> | -final | -<restorespec>}] [-from-secondary [-temp-volume <temp_volume>] [-copy-idid][<-taskspec>] [-verify][force] backup restore -fast [require | override | fallback | off] [-preview] -dump [-quiet | -verbose]`

Se l'operazione di ripristino del plug-in non riesce, vengono visualizzati solo il nome del plug-in e il codice di ritorno. Lo script del plug-in deve includere i messaggi di log e reindirizzare i messaggi ai file di log definiti dall'utente.

4. Per l'operazione di creazione del clone, immettere l'opzione `-taskspec` e fornire il percorso assoluto del file XML della specifica del task per eseguire una pre-elaborazione o un'attività di post-elaborazione prima o dopo l'operazione di clonazione: `smo create -profileprofile_name {-backup-labelbackup_name | -backup -data <backup-id>| -current} -newsidnew_sid-clonespecfull_path_to_clonespecfile [-reservaresfile] [-reservaresfile] [-lobosclone <host> <id>] [-laboschet] [-comaskde-<label> <taskspec>-quiet-<yes, no, inherit> <comment>-{[]`

Se l'operazione del plug-in clone non riesce, vengono visualizzati solo il nome del plug-in e il codice di ritorno. Lo script del plug-in deve includere i messaggi di log e reindirizzare i messaggi ai file di log definiti dall'utente.

Esempio di creazione di un backup utilizzando il file XML delle specifiche dell'attività

```
smo backup create -profile SALES1 -full -online -taskspec  
sales1_taskspec.xml -force -verify
```

Aggiornamento del nome del sistema di storage e del nome host del database di destinazione associati a un profilo

SnapManager 3.3 o versione successiva consente di aggiornare il nome host del sistema di storage o l'indirizzo del sistema di storage e il nome host del database di destinazione associato a un profilo SnapManager.

Aggiornamento del nome del sistema di storage associato a un profilo

SnapManager 3.3 o versione successiva consente di aggiornare il nome host o l'indirizzo IP di un sistema di storage associato a un profilo.

È necessario assicurarsi quanto segue:

- Il profilo dispone di almeno un backup.

Se il profilo non dispone di backup, non è necessario aggiornare il nome del sistema di storage per tale profilo.

- Nessuna operazione in esecuzione per il profilo.

È possibile aggiornare il nome del sistema di storage o l'indirizzo IP utilizzando l'interfaccia della riga di comando (CLI) di SnapManager. Durante l'aggiornamento del nome del sistema di storage, i metadati memorizzati nel solo database del repository vengono aggiornati. Dopo aver rinominato il nome del sistema di storage, è possibile eseguire tutte le operazioni SnapManager come in precedenza.



Non è possibile modificare il nome del sistema di storage utilizzando l'interfaccia grafica utente (GUI) di SnapManager.

È necessario assicurarsi che le copie Snapshot siano disponibili nel nuovo sistema di storage. SnapManager non verifica l'esistenza delle copie Snapshot nel sistema di storage.

Tuttavia, è necessario ricordare quanto segue durante l'esecuzione dell'aggiornamento e del rollback dell'host dopo la ridenominazione del nome del sistema di storage:

- Se si esegue un aggiornamento in sequenza dell'host dopo aver rinominato il nome del sistema di storage, è necessario aggiornare il profilo con il nuovo nome del sistema di storage.

Per informazioni su come utilizzare i comandi SnapDrive per modificare il nome del sistema di storage, consultare la sezione *risoluzione dei problemi relativi ai nomi dei sistemi di storage*.

- Se si esegue il rollback dell'host dopo la ridenominazione del sistema di storage, è necessario ripristinare il nome del sistema di storage precedente in modo da poter utilizzare i profili, i backup e i cloni del sistema di storage precedente per eseguire le operazioni SnapManager.



Se SnapDrive non riesce a identificare il sistema storage e visualizza messaggi di errore, è possibile immettere il comando `ipmigrate` con i nomi host precedenti e successivi del sistema storage. Per ulteriori informazioni sui problemi relativi ai nomi dei sistemi di storage, consulta [risoluzione dei problemi relativi ai nomi dei sistemi di storage](#).

1. Immettere il seguente comando: `smo storage rename -profile profile -oldname old_storage_name -newname new_storage_name [-quiet | -verbose]`

Se si desidera...	Quindi...
Aggiornare il nome del sistema di storage associato a un profilo	Specificare l'opzione <code>-profile</code> .
Aggiornare il nome del sistema di storage o l'indirizzo IP associato a un profilo	Specificare le seguenti opzioni e variabili: <ul style="list-style-type: none">• <code>-Oldname old_storage_name</code> è il nome host o l'indirizzo IP del sistema di storage.• <code>-Newname new_storage_name</code> è il nome host o l'indirizzo IP del sistema di storage.

L'esempio seguente mostra il nome del sistema di storage in fase di aggiornamento:

```
smo storage rename -profile mjuillian -oldname lech -newname hudson  
-verbose
```

Informazioni correlate

[Risoluzione dei problemi relativi alla ridenominazione del sistema storage](#)

Visualizzazione di un elenco di sistemi storage associati a un profilo

È possibile visualizzare un elenco dei sistemi storage associati a un particolare profilo.

L'elenco visualizza i nomi dei sistemi di storage associati al profilo specifico.



Se non sono disponibili backup per il profilo, non è possibile visualizzare il nome del sistema di storage associato al profilo.

1. Per visualizzare informazioni sui sistemi storage associati a un particolare profilo, immettere il seguente comando: `smo storage list -profile profile [-quiet | -verbose]`

Esempio

```
smo storage list -profile mjuillian
```



```
Sample Output:
Storage Controllers
-----
STCO1110-RTP07OLD
```

Aggiornamento del nome host del database di destinazione associato a un profilo

SnapManager (3.2 o versione successiva) per Oracle consente di aggiornare il nome host del database di destinazione nel profilo SnapManager.

- La home directory dell'utente locale deve essere consapevole delle mappature da profilo a repository.
- Le sessioni dell'interfaccia grafica utente (GUI) di SnapManager devono essere chiuse.
- In un ambiente RAC (Real Application Clusters), i cloni o i backup montati disponibili sull'host specificato nel profilo devono essere cancellati e rimossi.

È possibile aggiornare il profilo con il nuovo nome host utilizzando solo l'interfaccia CLI.

Scenari non supportati per la modifica del nome host del database di destinazione nel profilo

I seguenti scenari non sono supportati per la modifica del nome host del database di destinazione nel profilo:

- Modifica del nome host del database di destinazione mediante l'interfaccia grafica di SnapManager
- Eseguire il rollback del database del repository dopo aver aggiornato il nome host del database di destinazione del profilo
- Aggiornamento di più profili per un nuovo nome host del database di destinazione mediante un singolo comando
- Modifica del nome host del database di destinazione quando è in esecuzione un'operazione SnapManager
- Modifica del nome host del database di destinazione se SnapManager è installato su Solaris e se i numeri delle unità logiche (LUN) del database vengono creati utilizzando il file system montato su host con stack SVM.



Dopo aver aggiornato il nome host del database di destinazione nel profilo, viene modificato solo il nome host del database di destinazione. Tutti gli altri parametri di configurazione impostati sul profilo vengono conservati.

Dopo aver aggiornato il nuovo nome host del database di destinazione in un profilo abilitato alla protezione, vengono conservati gli stessi set di dati e criteri di protezione per il profilo aggiornato.

Dopo aver modificato il nome host per l'host di destinazione, è necessario aggiornare il nome host per tutti i profili protetti esistenti prima di creare i nuovi profili protetti. Per aggiornare il nome host di un profilo, eseguire il comando di aggiornamento del profilo smo.

Dopo aver aggiornato il nome host del database di destinazione, non è possibile rimuovere o separare il clone o smontare il backup se il clone o il backup montato non sono disponibili nel nuovo host. In tali scenari, l'esecuzione delle operazioni SnapManager dal nuovo host comporta errori e voci obsolete nell'host precedente. Per eseguire operazioni SnapManager, è necessario ripristinare il nome host precedente utilizzando l'aggiornamento del profilo.

1. Immettere il seguente comando: `smo profile update -profileprofile [-profile-passwordprofile_password][-database-dbnamedb_dbname-hostdb_host [-siddb_sid] [-login-usernamedb_username-passworddb_password-portdb_port]] [{-rman{-controlfile | {-login-usernamerman_username-passwordrman_password-tnsnamerman_tnsname}}}] | -remove-rman]-osaccountosaccount-osgrouposgroup [-retain [-hourly [-countn] [-durationm]] [-daily [-countn] [-durationm]] [-weekly [-countn] [-durationm]] [-monthly [-countn] [-durationm]]] [-commentcomment][-snapname-patternpattern][[-protect [-protection-policypolicy_name]] | [-noprotect]] [-summary-notification] [-notification [-success-emailemail_address1, email_address2-subjectsubject_pattern] [-failure-emailemail_address1, email_address2-subjectsubject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hourshours | -daysdays | -weeksweeks| -monthsmonths [-protect [-protection-policypolicy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]`

Le altre opzioni per questo comando sono le seguenti:

`[-force] [-noprompt]`

Se si desidera...	Quindi...
Modificare il nome host del database di destinazione	Specificare <code>-hostnew_db_host</code>

2. Per visualizzare il nome host del database di destinazione del profilo, immettere il seguente comando: `smo profile show`

Mantenere la cronologia delle operazioni SnapManager

SnapManager per Oracle consente di mantenere la cronologia delle operazioni SnapManager associate a uno o più profili. È possibile mantenere la cronologia dall'interfaccia della riga di comando (CLI) di SnapManager o dall'interfaccia grafica utente (GUI). È possibile visualizzare la cronologia delle operazioni sotto forma di report e utilizzare il report per scopi di verifica della conformità.

È possibile mantenere la cronologia per le seguenti operazioni SnapManager:

- Creazione del backup
- Verifica del backup
- Ripristino del backup
- Creazione di cloni
- Suddivisione dei cloni

Le informazioni sulla cronologia delle operazioni SnapManager vengono mantenute in base alla conservazione. È possibile configurare diverse classi di conservazione per ciascuna delle operazioni SnapManager supportate.

Di seguito sono riportate alcune classi di conservazione che è possibile assegnare:

- Numero di giorni
- Numero di settimane
- Numero di mesi
- Numero di operazioni

In base alla conservazione, SnapManager rimuove automaticamente la cronologia. È inoltre possibile eliminare manualmente la cronologia delle operazioni SnapManager. Se si elimina o si distrugge il profilo, tutte le informazioni della cronologia associate al profilo vengono eliminate.



Dopo il rollback dell'host, non è possibile visualizzare i dettagli della cronologia o eseguire operazioni relative alla cronologia associate al profilo configurato per la manutenzione della cronologia.

Configurazione della cronologia per il funzionamento di SnapManager

SnapManager per Oracle consente di mantenere la cronologia delle operazioni SnapManager dalla CLI o dall'interfaccia grafica utente di SnapManager. È possibile visualizzare la cronologia dell'operazione SnapManager come report.

1. Per configurare la cronologia delle operazioni SnapManager, immettere il seguente comando: `smo history set -profile {-name, profile_name [profile_name1, profile_name2] | -all-repository-login [-passwordrepo_password] -usernamerepo_dbnamerepo_dbname-ostrepo_host-portrepo_port} -operation {-conserve -nomesignone -lythemonthesimanale |}_operazione -nomesignone_2_operazioni_manutenzione_settimanale | {_manutenzione -nomesignone_settimanale |}_operazioni_manutenzione_settimanale | _manutenzione_manutenzione_settimanale | _operazioni_settimanale | manutenzione_settimanale -nomesignone_manutenzione_settimanale | _operazioni_manutenzione_settimanale`

```
smo
history set -profile -name PROFILE1 -operation -operations backup -retain
-daily 6 -verbose
```

```
smo
history set -profile -name PROFILE1 -operation -all -retain -weekly 3
-verbose
```

Visualizzazione di un elenco della cronologia delle operazioni SnapManager

È possibile visualizzare la cronologia di una o di tutte le operazioni SnapManager come report in base alle impostazioni di conservazione.

1. Per visualizzare un elenco delle operazioni della cronologia SnapManager, immettere il seguente comando: `smo history list -profile {-name, profile_name [profile_name1,profile_name2] | -all-repository-login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname-hostrepo_host-portrepo_port} -operation {-operationsoperation_name [operation_name1, operation_name2] |`

```
-all} [-delimiterdelimiter] [-quiet | -verbose]
```

Visualizzazione della cronologia dettagliata di un'operazione specifica associata a un profilo

È possibile visualizzare la cronologia dettagliata di una specifica operazione SnapManager associata a un profilo.

1. Per visualizzare informazioni dettagliate sulla cronologia di un'operazione SnapManager specifica associata a un profilo, immettere il seguente comando: `smo history operation-show -profileprofile_name {-labellabel | -idid} [-quiet | -verbose]`

Eliminazione della cronologia delle operazioni SnapManager

È possibile eliminare la cronologia dell'operazione SnapManager, se non sono più necessari i dettagli della cronologia.

1. Per eliminare la cronologia dell'operazione SnapManager, immettere il seguente comando: `smo history purge -profile {-name, profile_nameprofile_name1, profile_name2} | all-repository-login [-passwordrepo_password] -usernamerepo_username -dbnamerepo_dbname-hostrepo_host-portrepo_port} -operation {-operationsoperation_name [operation_name1, operation_name2] | -all} [-quiet | -verbose]`

Rimozione delle impostazioni della cronologia associate a uno o più profili

SnapManager consente di rimuovere le impostazioni della cronologia di un'operazione SnapManager. Questa operazione rimuove tutte le informazioni della cronologia associate a un singolo profilo o a più profili.

1. Per rimuovere la cronologia delle operazioni SnapManager associate a uno o più profili, immettere il seguente comando: `smo history remove -profile {-name, profile_name [profile_name1, profile_name2] | all-repository-login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname-hostrepo_host-portrepo_port} -operation {-operationsoperation_name [operation_name1, operation_name2] | -all} [-quiet | -verbose]`

Visualizzazione dei dettagli di configurazione della cronologia SnapManager

È possibile visualizzare le impostazioni della cronologia per un singolo profilo.

L'operazione SnapManager history visualizza le seguenti informazioni per ciascun profilo:

- Nome dell'operazione
- Classe di conservazione
- Numero di conservazione
 - a. Per visualizzare informazioni sull'operazione SnapManager history per un profilo specifico, immettere il seguente comando: `smo history show -profileprofile_name`

Riferimento al comando SnapManager per Oracle

Il riferimento al comando SnapManager include la sintassi di utilizzo valida, le opzioni, i parametri e gli argomenti da fornire con i comandi, insieme agli esempi.

I seguenti problemi si applicano all'utilizzo dei comandi:

- I comandi sono sensibili al maiuscolo/minuscolo.
- SnapManager accetta fino a 200 caratteri ed etichette fino a 80 caratteri.
- Se la shell sull'host limita il numero di caratteri che possono essere visualizzati su una riga di comando, è possibile utilizzare il comando `cmdfile`.
- Non utilizzare spazi nei nomi dei profili o delle etichette.
- Nella specifica del clone, non utilizzare spazi nella posizione del clone.

SnapManager può visualizzare tre livelli di messaggi per la console:

- Messaggi di errore
- Messaggi di avviso
- Messaggi informativi

È possibile specificare la modalità di visualizzazione dei messaggi. Se non si specifica nulla, SnapManager visualizza solo messaggi di errore e avvisi sulla console. Per controllare la quantità di output che SnapManager visualizza sulla console, utilizzare una delle seguenti opzioni della riga di comando:

- `-Quiet`: Visualizza solo i messaggi di errore sulla console.
- `-Verbose`: Visualizza messaggi di errore, di avviso e informativi sulla console.



Indipendentemente dal comportamento predefinito o dal livello di dettaglio specificato per la visualizzazione, SnapManager scrive sempre tutti i tipi di messaggio nei file di registro.

Il comando `smo_server restart`

Questo comando riavvia il server host SnapManager e viene immesso come root.

Sintassi

```
smo_server restart  
[-quiet | -verbose]
```

Parametri

- **-quiet**

Specifica che sulla console vengono visualizzati solo i messaggi di errore. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Specifica che i messaggi di errore, di avviso e informativi vengono visualizzati sulla console.

Esempio di comando

Nell'esempio seguente viene riavviato il server host.

```
smo_server restart
```

Il comando **smo_server start**

Questo comando avvia il server host che esegue il software SnapManager per Oracle.

Sintassi

```
smo_server start  
\[ -quiet \| -verbose \]
```

Parametri

- **-quiet**

Specifica che sulla console vengono visualizzati solo i messaggi di errore. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Specifica che i messaggi di errore, di avviso e informativi vengono visualizzati sulla console.

Esempio di comando

Nell'esempio seguente viene avviato il server host.

```
smo_server start  
SMO-17100: SnapManager Server started on secure port 25204 with PID 11250
```

Il comando **smo_server status**

È possibile eseguire il comando `smo_server status` per visualizzare lo stato del server host SnapManager.

Sintassi

```
smo_server status  
\[ -quiet \| -verbose \]
```

Parametri

- **-quiet**

Specifica che nella console vengono visualizzati solo i messaggi di errore. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Specifica che i messaggi di errore, di avviso e informativi vengono visualizzati nella console.

Esempio

Nell'esempio seguente viene visualizzato lo stato del server host:

```
smo_server status
SMO-17104: SnapManager Server version 3.3.1 is running on secure port
25204 with PID 11250
and has 0 operations in progress.
```

Il comando **smo_server stop**

Questo comando arresta il server host SnapManager e viene immesso nella directory principale.

Sintassi

```
smo_server stop
\[-quiet \|-verbose\]
```

Parametri

- **-quiet**

Specifica che sulla console vengono visualizzati solo i messaggi di errore. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Specifica che i messaggi di errore, di avviso e informativi vengono visualizzati sulla console.

Esempio di comando

Nell'esempio seguente viene utilizzato il comando `smo_server stop`.

```
smo_server stop
```

Il comando smo backup create

È possibile eseguire il comando di creazione del backup per creare backup del database su uno o più sistemi storage.

Sintassi



Prima di eseguire questo comando, è necessario creare un profilo di database utilizzando il comando di creazione del profilo.

```
smo backup create
-profile profile_name
\[-full\{-auto \| -online \| -offline\}\]\[-retain \{-hourly \| -daily \|
-weekly \| -monthly \| -unlimited\} \[-verify\] \
\[-data \[\[-files files \[files\]\] \
\[-tablespaces tablespaces \[tablespaces\]\] \[-label label\] \{-auto \|
-online \| -offline\}
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\} \[-
verify\] \
\[-archivelogs \[-label label\]\] \[-comment comment\]\}
\[-protect \| -noprotect \| -protectnow\]
\[-backup-dest path1 \[ , path2\]\]
\[-exclude-dest path1 \[ , path2\]\]
\[-prunelogs \{-all \| -until-scnn until-scnn \| -until-date yyyy-MM-
dd:HH:mm:ss\] \| -before \{-months \| -days \| -weeks \| -hours\}\}
-prune-dest prune_dest1,\[prune_dest2\]\]
\[-taskspec taskspec\]
\[-dump\]
-force
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database di cui si desidera eseguire il backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-opzione auto**

Se il database si trova nello stato montato o non in linea, SnapManager esegue un backup non in linea. Se il database si trova nello stato aperto o in linea, SnapManager esegue un backup in linea. Se si utilizza l'opzione -force con l'opzione -offline, SnapManager impone un backup offline anche se il database è attualmente in linea.

- **opzione -online**

Specifica un backup del database online.

È possibile creare un backup online di un database RAC (Real Application Clusters), purché il database primario sia in stato aperto o il database primario sia montato e un'istanza sia in stato aperto. È possibile utilizzare l'opzione `-force` per i backup online se l'istanza locale si trova nello stato di shutdown o se nessuna istanza si trova nello stato di apertura. La versione di Oracle deve essere 10.2.0.5; in caso contrario, il database si blocca se viene montata una qualsiasi istanza del RAC.

- Se l'istanza locale si trova nello stato di shutdown e almeno un'istanza si trova nello stato di apertura, è possibile utilizzare l'opzione `-force` per modificare l'istanza locale nello stato montato.
- Se nessuna istanza è in stato aperto, è possibile utilizzare l'opzione `-force` per modificare l'istanza locale in stato aperto.

- **-opzione offline**

Specifica un backup non in linea mentre il database si trova nello stato di chiusura. Se il database si trova nello stato aperto o montato, il backup non viene eseguito correttamente. Se si utilizza l'opzione `-force`, SnapManager tenta di modificare lo stato del database per arrestare il database per un backup offline.

- **-opzione completa**

Esegue il backup dell'intero database. Sono inclusi tutti i dati, il log archiviato e i file di controllo. Il backup dei log di ripristino e dei file di controllo archiviati viene eseguito indipendentemente dal tipo di backup eseguito. Se si desidera eseguire il backup solo di una parte del database, utilizzare l'opzione `-Files o -tablespaces`.

- **-opzione dati**

Specifica i file di dati.

- **-elenco file**

Esegue il backup solo dei file di dati specificati e dei file di log e di controllo archiviati. Separare l'elenco dei nomi dei file con spazi. Se il database è in stato aperto, SnapManager verifica che gli spazi delle tabelle appropriati siano in modalità di backup online.

- **-tablespaces tablespaces**

Esegue il backup solo degli spazi delle tabelle del database specificati e dei file di log e di controllo archiviati. Separare i nomi di tablespace con gli spazi. Se il database è in stato aperto, SnapManager verifica che gli spazi delle tabelle appropriati siano in modalità di backup online.

- **etichetta ****

Specifica un nome opzionale per questo backup. Questo nome deve essere univoco all'interno del profilo. Il nome può contenere lettere, numeri, caratteri di sottolineatura (`_`) e trattini (`-`). Non può iniziare con un trattino. Se non si specifica un'etichetta, SnapManager crea un'etichetta predefinita nel formato `scope_type_date`:

- L'ambito è `F` per indicare un backup completo o `P` per indicare un backup parziale.
- Digitare `C` per indicare un backup offline (cold), `H` per indicare un backup online (hot) o `A` per indicare un backup automatico, ad esempio `P_A_20081010060037IST`.
- Data indica l'anno, il mese, il giorno e l'ora del backup.

SnapManager utilizza un orologio a 24 ore.

Ad esempio, se è stato eseguito un backup completo con il database offline il 16 gennaio 2007, alle

17:45:16 Ora standard orientale, SnapManager crea l'etichetta F_C_20070116174516EST.

- **-comment string**

Specifica un commento facoltativo per descrivere questo backup. Racchiudere la stringa tra virgolette singole (').



Alcuni shell stripano le virgolette. In questo caso, è necessario includere la virgoletta con una barra rovesciata (). Ad esempio, potrebbe essere necessario immettere quanto segue:
`\' this is a comment\'`.

- **-opzione di verifica**

Verifica che i file nel backup non siano corrotti eseguendo l'utility Oracle dbv.



Se si specifica l'opzione -verify, l'operazione di backup non viene completata fino al completamento dell'operazione di verifica.

- **opzione -force**

Forza una modifica dello stato se il database non si trova nello stato corretto. Ad esempio, SnapManager potrebbe modificare lo stato del database da online a offline, in base al tipo di backup specificato e allo stato in cui si trova il database.

Con un backup online del database RAC, utilizzare l'opzione -force se l'istanza locale si trova nello stato di shutdown o se nessuna istanza si trova nello stato di apertura.



La versione di Oracle deve essere 10.2.0.5; in caso contrario, il database si blocca se viene montata una qualsiasi istanza del RAC.

- Se l'istanza locale si trova nello stato di shutdown e almeno un'istanza si trova nello stato di apertura, utilizzando l'opzione -force l'istanza locale viene modificata nello stato montato.
- Se nessuna istanza si trova nello stato di apertura, l'opzione -force consente di modificare l'istanza locale nello stato di apertura.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

- **-protect | -nprotect | -protectnow**

Indica se il backup deve essere protetto sullo storage secondario. L'opzione -nprotect specifica che il backup non deve essere protetto sullo storage secondario. Sono protetti solo i backup completi. Se non viene specificata alcuna opzione, SnapManager protegge il backup come predefinito se si tratta di un backup completo e il profilo specifica un criterio di protezione. L'opzione -protectnow è disponibile solo per Data ONTAP in modalità 7. L'opzione specifica che il backup deve essere protetto immediatamente sullo storage secondario.

- **-retain { -orario | -giornaliero | -settimanale | -mensile | -illimitato }**

Specifica se il backup deve essere conservato su base oraria, giornaliera, settimanale, mensile o illimitata. Se l'opzione `-retain` non è specificata, la classe di conservazione viene impostata per impostazione predefinita sull'opzione `-hourly`. Per conservare i backup per sempre, utilizza l'opzione `-Unlimited`. L'opzione `-Unlimited` rende il backup non idoneo per l'eliminazione in base al criterio di conservazione.

- opzione **-archivelogs**

Crea backup del registro di archiviazione.

- **-backup-dest path1, [, [path2]]**

Specifica le destinazioni del log di archiviazione di cui eseguire il backup per il log di archiviazione.

- **-exclude-dest path 1, [, [path2]]**

Specifica le destinazioni del registro di archiviazione da escludere dal backup.

- **-prunelogs {-all | -until-scn| -until-dateyyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}}**

Elimina i file di log dell'archivio dalle destinazioni del log dell'archivio in base alle opzioni fornite durante la creazione di un backup. L'opzione `-all` elimina tutti i file di log dell'archivio dalle destinazioni del log dell'archivio. L'opzione `-until-scn` elimina i file di registro dell'archivio fino a quando non viene specificato un numero SCN (System Change Number). L'opzione `-until-date` elimina i file di log dell'archivio fino al periodo di tempo specificato. L'opzione `-before` elimina i file di log dell'archivio prima del periodo di tempo specificato (giorni, mesi, settimane, ore).

- **-prune-dest prune_dest1,prune_dest2**

Elimina i file di log dell'archivio dalle destinazioni del log dell'archivio durante la creazione del backup.

- **-taskspec taskspec**

Specifica il file XML della specifica dell'attività che può essere utilizzato per l'attività di pre-elaborazione o di post-elaborazione dell'operazione di backup. Il percorso completo del file XML deve essere fornito mentre si fornisce l'opzione `-taskspec`.

- opzione **-dump**

Raccoglie i file dump dopo un'operazione di backup del database riuscita o non riuscita.

Esempio di comando

Il seguente comando crea un backup online completo, crea un backup sullo storage secondario e imposta il criterio di conservazione su giornaliero:

```
smo backup create -profile SALES1 -full -online  
-label full_backup_sales_May -profile SALESDB -force -retain -daily  
Operation Id [8abc01ec0e79356d010e793581f70001] succeeded.
```

Informazioni correlate

[Creazione di backup del database](#)

Il comando smo backup delete

È possibile eseguire il comando di eliminazione del backup per rimuovere i backup che non vengono rimossi automaticamente, ad esempio i backup utilizzati per creare un clone o i backup che non sono riusciti. È possibile eliminare i backup conservati senza limiti senza modificare la classe di conservazione.

Sintassi

```
smo backup delete
-profile profile_name
[-label label \[-data \|-archivelogs\] \|\ \[-id guid \|-all\]
-force
\[-dump\]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il database associato al backup che si desidera rimuovere. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-id guid**

Specifica il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando smo backup list per visualizzare il GUID per ciascun backup.

- **etichetta ****

Specifica il backup con l'etichetta specificata. Facoltativamente, specificare l'ambito del backup come file di dati o log di archiviazione.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **-tutto**

Specifica tutti i backup. Per eliminare solo i backup specificati, utilizzare l'opzione -id o -label.

- **-dump**

Raccoglie i file dump dopo un'operazione di eliminazione del backup riuscita o non riuscita.

- **-force**

Forza la rimozione del backup. SnapManager rimuove il backup anche in caso di problemi di liberare le risorse associate al backup. Ad esempio, se il backup è stato catalogato con Oracle Recovery Manager (RMAN), ma il database RMAN non esiste più, incluso -force elimina il backup anche se non riesce a connettersi con RMAN.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Il seguente esempio elimina il backup:

```
smo backup delete -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Informazioni correlate

[Eliminazione dei backup](#)

[Il comando di creazione del profilo smo](#)

[Il comando di aggiornamento del profilo smo](#)

Il comando smo backup free

È possibile eseguire il comando backup free per liberare le copie Snapshot dei backup senza rimuovere i metadati di backup dal repository.

Sintassi

```
smo backup free
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo associato al backup che si desidera liberare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-id guid**

Specifica le risorse del backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando `smo backup list` per visualizzare il GUID per ciascun backup. Includere l'opzione `-verbose` per visualizzare gli ID di backup.

- **etichetta ****

Specifica il backup con l'etichetta specificata.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **-tutto**

Specifica tutti i backup. Per eliminare i backup specificati, utilizzare l'opzione `-id` o `-label`.

- **-force**

Forza la rimozione delle copie Snapshot.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Il seguente esempio libera il backup:

```
smo backup free -profile SALES1 -label full_backup_sales_May  
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Informazioni correlate

[Liberare i backup](#)

Il comando smo backup list

È possibile eseguire il comando dell'elenco di backup per visualizzare le informazioni sui backup di un profilo, incluse le informazioni sulla classe di conservazione e sullo stato di protezione.

Sintassi

```
smo backup list
-profile profile_name
-delimiter character
[-data | -archivelogs | -all]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo per il quale si desidera elencare i backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- carattere **-delimitatore**

Visualizza ogni riga su una riga separata. Gli attributi nella riga sono separati dal carattere specificato.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console. Includere l'opzione -verbose per visualizzare gli ID di backup.

Esempio

Nell'esempio seguente sono elencati i backup per il profilo SALES1:

```
smo backup list -profile SALES1 -verbose
Start Date           Status Scope Mode      Primary Label      Retention
Protection
-----
2007-08-10 14:31:27 SUCCESS FULL    ONLINE EXISTS  backup1    DAILY
PROTECTED
2007-08-10 14:12:31 SUCCESS FULL    ONLINE EXISTS  backup2    HOURLY
NOT PROTECTED
2007-08-10 10:52:06 SUCCESS FULL    ONLINE EXISTS  backup3    HOURLY
PROTECTED
2007-08-05 12:08:37 SUCCESS FULL    ONLINE EXISTS  backup4    UNLIMITED
NOT PROTECTED
2007-08-05 09:22:08 SUCCESS FULL    OFFLINE EXISTS  backup5    HOURLY
PROTECTED
2007-08-04 22:03:09 SUCCESS FULL    ONLINE EXISTS  backup6    UNLIMITED
NOT REQUESTED
2007-07-30 18:31:05 SUCCESS FULL    OFFLINE EXISTS  backup7    HOURLY
PROTECTED
```

Informazioni correlate

[Visualizzazione di un elenco di backup](#)

Il comando di montaggio del backup smo

È possibile eseguire il comando di montaggio del backup per montare un backup al fine di eseguire un'operazione di ripristino utilizzando uno strumento esterno.

Sintassi

```
smo backup mount
-profile profile_name
[-label label \[-data \|-archivelogs\] \|-id id\]
[-host host]
\[-from-secondary \{-copy-id id\}\]
\[-dump\]
[-quiet | -verbose]
```

Parametri

- **-profile_name**

Specifica il profilo associato al backup che si desidera montare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-id guid**

Consente di montare il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando `smo backup list` per visualizzare il GUID per ciascun backup.

- **etichetta ****

Consente di montare il backup con l'etichetta specificata.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **-from-secondary -copy-id id**

Consente di montare il backup dallo storage secondario. Se questa opzione non viene specificata, SnapManager installa il backup dallo storage primario. È possibile utilizzare questa opzione se il backup viene liberato.

Specificare l'opzione `-copy-id` ogni volta che si specifica l'opzione `-from-secondary`. Se nel sistema di storage secondario sono presenti più backup, viene utilizzata l'opzione `-copy-id` per specificare quale copia di backup nello storage secondario utilizzare per montare il backup.



Se si utilizza Data ONTAP in modalità 7, è necessario specificare un valore valido per l'opzione `-copy-id`. Tuttavia, se si utilizza Clustered Data ONTAP, l'opzione `-copy-id` non è richiesta.

- **-host host**

Specifica l'host su cui si desidera montare il backup.

- **-dump**

Raccoglie i file dump dopo l'operazione di montaggio riuscita o non riuscita.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.



Utilizzare questo comando solo se si utilizza uno strumento esterno come Oracle Recovery Manager (RMAN). SnapManager gestisce automaticamente il montaggio dei backup se si utilizza il comando `smo backup restore` per ripristinare il backup. Questo comando visualizza un elenco che mostra i percorsi in cui sono state montate le copie Snapshot. Questo elenco viene visualizzato solo quando viene specificata l'opzione `-verbose`.

Esempio

Nell'esempio seguente viene montato il backup:

```
smo backup mount -profile SALES1 -label full_backup_sales_May -verbose
SMO-13046 [INFO ]: Operation GUID 8abc013111b9088e0111b908a7560001
starting on Profile SALES1
SMO-08052 [INFO ]: Beginning to connect mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/logs from
snapshot SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_logs.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/logs from snapshot
SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_logs.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/data from
snapshot SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_data.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/data from snapshot
SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_data.
SMO-08053 [INFO ]: Finished connecting mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a45066210001.
SMO-13037 [INFO ]: Successfully completed operation: Backup Mount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:01:00.981
Operation Id [8abc013111b9088e0111b908a7560001] succeeded.
```

Informazioni correlate

[Montaggio dei backup](#)

Il comando di ripristino del backup smo

È possibile eseguire il comando di ripristino del backup per ripristinare i backup di un database o di una parte di un database, quindi ripristinare facoltativamente le informazioni del database.

Sintassi

```

smo backup restore
-profile profile_name
\[-label label \| -id id\]
\[-files files \[files...\] \|
-tablespaces tablespaces \[tablespaces...\]\] \|
-complete \| -controlfiles\]
\[-recover \{-alllogs \| -nologs \| -until until\} \[-using-backup-
controlfile\] \|
\[-restorespec restorespec \| -from-secondary \[-temp-volume temp_volume\]
\[-copy-id id\]\]
\[-preview\]
\[-fast \{-require \| -override \| -fallback \| -off\}\]
\[-recover-from-location path1 \[, path2\]\]
\[-taskspec taskspec\]
\[-dump\]
\[-force\]
\[-quiet \| -verbose\]

```

Parametri

- **-profile_name**

Specifica il database che si desidera ripristinare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-label name**

Ripristina il backup con l'etichetta specificata.

- **-id guid**

Ripristina il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando `smo backup list` per visualizzare il GUID per ciascun backup.

- **Scegliere tutti i file o i file specificati**

In alternativa, è possibile utilizzare una delle seguenti opzioni:

- **-Complete (completo):** Ripristina tutti i file di dati nel backup.
- **-Tablespaceslist:** Ripristina dal backup solo i tablespace specificati.

È necessario utilizzare gli spazi per separare i nomi nell'elenco.

- **-Fileslist:** Ripristina solo i file di dati specificati dal backup.

È necessario utilizzare gli spazi per separare i nomi nell'elenco. Se il database è in esecuzione, SnapManager garantisce che lo spazio tabella contenente i file sia offline.

- **-controlfiles**

Ripristina i file di controllo. SnapManager consente di ripristinare i file di controllo insieme ai file di dati dai backup in una singola operazione. L'opzione `-controlfiles` è indipendente da altri parametri dell'ambito di ripristino come `-complete`, `-tablespaces` e `-files`.

- **-ripristinare**

Recupera il database dopo averlo ripristinato. È inoltre necessario specificare il punto in cui si desidera che SnapManager ripristini il database utilizzando una delle seguenti opzioni:

- `-Nologs`: Recupera il database al momento del backup e non applica alcun log.

È possibile utilizzare questo parametro per i backup online o offline.

- `-Alllogs`: Recupera il database all'ultima transazione o commit e applica tutti i log richiesti.
- `-Until date`: Recupera il database fino alla data e all'ora specificate.

È necessario utilizzare il formato anno-mese-data: Ora: Minuto: Secondo (aaaa-mm-gg:hh:mm:ss). Per le ore, utilizzare il formato 12 ore o 24 ore, a seconda dell'impostazione del database.

- `-Until scn`: Esegue il rollforward dei file di dati fino a raggiungere il numero SCN (System Change Number) specificato.
- `-Using-backup-controlfile`: Recupera il database utilizzando il file di controllo del backup.

- **-restorespec**

Consente di ripristinare i dati in un file system attivo e di eseguire il ripristino dai dati specificati, fornendo una mappatura di ciascuna copia Snapshot originale nel file system attivo. Se non si specifica un'opzione, SnapManager ripristina i dati delle copie Snapshot sullo storage primario. È possibile specificare una delle seguenti opzioni:

- `-Restorespec`: Specifica i dati da ripristinare e il formato di ripristino.
- `-Da-secondario`: Ripristina i dati dallo storage secondario.

Non è possibile utilizzare questa opzione se il backup esiste sullo storage primario; il backup primario deve essere liberato prima di poter ripristinare un backup dallo storage secondario. Se si utilizza un volume temporaneo, è necessario specificare il volume utilizzando l'opzione `-temp-volume`.

Specificare l'opzione `-copy-id` ogni volta che si specifica l'opzione `-from-secondary`. Se nel sistema di storage secondario sono presenti più backup, viene utilizzata l'opzione `-copy-id` per specificare quale copia di backup nello storage secondario deve essere utilizzata per l'operazione di ripristino.



Se si utilizza Data ONTAP in modalità 7, è necessario specificare un valore valido per l'opzione `-copy-id`. Tuttavia, se si utilizza Clustered Data ONTAP, l'opzione `-copy-id` non è richiesta.

Durante il ripristino dallo storage secondario, SnapManager tenta innanzitutto di ripristinare i dati direttamente dal sistema di storage secondario al sistema di storage primario (senza coinvolgere l'host). Se SnapManager non è in grado di eseguire questo tipo di ripristino (ad esempio, se i file non fanno parte del file system), SnapManager eseguirà un ripristino della copia del file sul lato host. SnapManager dispone di due metodi per eseguire un ripristino della copia del file lato host da secondario. Il metodo selezionato da SnapManager viene configurato nel file `smo.config`.

- **Diretto**: SnapManager clona i dati sullo storage secondario, monta i dati clonati dal sistema di storage secondario sull'host, quindi copia i dati dal clone nell'ambiente attivo.

Questo è il criterio di accesso secondario predefinito.

- Indiretto: SnapManager copia prima i dati in un volume temporaneo sullo storage primario, monta i dati dal volume temporaneo all'host, quindi copia i dati dal volume temporaneo nell'ambiente attivo.

Questo criterio deve essere utilizzato solo se l'host non dispone di accesso diretto al sistema di storage secondario. I ripristini con il metodo indiretto richiedono il doppio del tempo rispetto al criterio di accesso secondario diretto, poiché vengono eseguite due copie dei dati.

La decisione di utilizzare il metodo diretto o indiretto è controllata dal valore del parametro `restore.secondaryAccessPolicy` nel file di configurazione `smo.config`.

• **-anteprima**

Visualizza le seguenti informazioni:

- Quale meccanismo di ripristino (ripristino rapido, ripristino del file system lato storage, ripristino del file lato storage o ripristino della copia del file lato host) verrà utilizzato per ripristinare ciascun file
- Perché non sono stati utilizzati meccanismi più efficienti per ripristinare ciascun file, quando si specifica l'opzione `-verbose` se si utilizza l'opzione `-preview`, è necessario conoscere quanto segue:
- L'opzione `-force` non ha alcun impatto sul comando.
- L'opzione `-recover` non ha alcun impatto sul comando.
- L'opzione `-fast` (`-request`, `-override`, `-fallback` o `-off`) ha un impatto significativo sull'output. Per visualizzare in anteprima l'operazione di ripristino, è necessario montare il database. Se si desidera visualizzare un'anteprima di un piano di ripristino e il database non è attualmente montato, SnapManager monta il database. Se il database non può essere montato, il comando non riesce e SnapManager riporta il database allo stato originale.

L'opzione `-preview` consente di visualizzare fino a 20 file. È possibile configurare il numero massimo di file da visualizzare nel file `smo.config`.

• **-veloce**

Consente di scegliere il processo da utilizzare nell'operazione di ripristino. È possibile forzare SnapManager a utilizzare il processo di ripristino rapido basato sul volume invece di altri processi di ripristino, se vengono soddisfatte tutte le condizioni di idoneità al ripristino obbligatorie. Se si è a conoscenza dell'impossibilità di eseguire un ripristino del volume, è possibile utilizzare questo processo anche per impedire a SnapManager di eseguire controlli di idoneità e l'operazione di ripristino utilizzando il processo di ripristino rapido.

L'opzione `-FAST` include i seguenti parametri:

- **-Richiedi:** Consente di forzare SnapManager ad eseguire un ripristino del volume, se vengono soddisfatte tutte le condizioni di idoneità per il ripristino.

Se si specifica l'opzione `-fast`, ma non si specifica alcun parametro per `-FAST`, SnapManager utilizza il parametro `-prescrivere` come impostazione predefinita.

- **-Override:** Consente di ignorare i controlli di idoneità non obbligatori ed eseguire il processo di ripristino rapido basato sul volume.
- **-Fallback:** Consente di ripristinare il database utilizzando qualsiasi metodo determinato da SnapManager.

Se non si specifica l'opzione `-fast`, SnapManager utilizza l'opzione predefinita `backup restore -fast fallback`.

- `-Off`: Consente di evitare il tempo necessario per eseguire i controlli di idoneità.

- **-recovery-from-location**

Specifica la posizione del log di archiviazione esterno dei file di log di archiviazione. SnapManager preleva i file di log dell'archivio dalla posizione esterna e li utilizza per il processo di ripristino.

- **-taskspec**

Specifica il file XML della specifica dell'attività per l'attività di pre-elaborazione o di post-elaborazione dell'operazione di ripristino. Specificare il percorso completo del file XML per la specifica dell'attività.

- **-dump**

Specifica di raccogliere i file dump dopo l'operazione di ripristino.

- **-force**

Se necessario, cambia lo stato del database in uno stato inferiore a quello corrente. Per i cluster di applicazioni reali (RAC), è necessario includere l'opzione `-force` se SnapManager deve modificare lo stato di qualsiasi istanza RAC in uno stato inferiore.

Per impostazione predefinita, SnapManager può modificare lo stato del database in uno stato superiore durante un'operazione. Questa opzione non è necessaria per consentire a SnapManager di modificare il database in uno stato superiore.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console. È possibile utilizzare questa opzione per scoprire perché non è stato possibile utilizzare processi di ripristino più efficienti per ripristinare il file.

Esempio

Nell'esempio seguente viene ripristinato un database insieme ai file di controllo:

```
smo backup restore -profile SALES1 -label full_backup_sales_May
-complete -controlfiles -force
```

Informazioni correlate

[Ripristino dei backup del database](#)

[Ripristino dei backup da una posizione alternativa](#)

[Creazione di specifiche di ripristino](#)

Il comando smo backup show

È possibile utilizzare il comando show di backup per visualizzare informazioni dettagliate su un backup, tra cui lo stato di protezione, la classe di conservazione del backup e i backup sullo storage primario e secondario.

Sintassi

```
smo backup show
-profile profile_name
[-label label \[-data \|-archivelogs\] \|-id id\]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo per cui visualizzare i backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **etichetta ****

Specifica l'etichetta del backup.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **id -id**

Specifica l'ID del backup.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console, nonché informazioni su cloni e verifica.

Esempio

L'esempio seguente mostra informazioni dettagliate sul backup:

```
smo backup show -profile SALES1 -label BTNFS -verbose
Backup id: 8abc013111a450480111a45066210001
Backup status: SUCCESS
Primary storage resources: EXISTS
Protection sate: PROTECTED
Retention class: DAILY
Backup scope: FULL
Backup mode: OFFLINE
Mount status: NOT MOUNTED
Backup label: BTNFS
Backup comment:
RMAN Tag: SMO_BTNFS_1175283108815
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Verification status: OK
Backup Retention Policy: NORMAL
Backup database: hsd1
Checkpoint: 2700620
Tablespace: SYSAUX
Datafile: /mnt/ssys1/data/hsdb/sysaux01.dbf [ONLINE]
...
Control Files:
File: /mnt/ssys1/data/control03.ctl
...
Archive Logs:
File: /mnt/ssys1/data/archive_logs/2_131_626174106.dbf
...
Host: Host1
Filesystem: /mnt/ssys1/data
File: /mnt/ssys1/data/hsdb/SMOBakCtl_1175283005231_0
...
Volume: hs_data
Snapshot: SMO_HSDBR_hsd1_F_C_1_
8abc013111a450480111a45066210001_0
File: /mnt/ssys1/data/hsdb/SMOBakCtl_1175283005231_0
...
Protected copies on Secondary Storage:
  14448939 - manow
  88309228 - graffe
```

Informazioni correlate

[Visualizzazione dei dettagli del backup](#)

Il comando smo backup unmount

È possibile eseguire il comando di disinstallazione del backup per smontare un backup.

Sintassi

```
smo backup unmount
-profile profile_name
[-label label \[-data \|-archivelogs\] \|-id id\]
\[-force\]
\[-dump\]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo per il quale si desidera smontare un backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **id -id**

Disinstalla il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando smo backup list per visualizzare il GUID per ciascun backup.

- **etichetta ****

Disinstalla il backup con l'etichetta specificata.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **-dump**

Raccoglie i file dump dopo un'operazione di disinstallazione riuscita o non riuscita.

- **-force**

Consente di rimuovere il backup anche in caso di problemi di liberare le risorse associate al backup. SnapManager tenta di smontare il backup e di ripulire le risorse associate. Il log mostra che l'operazione di disinstallazione ha avuto esito positivo, ma potrebbe essere necessario ripulire manualmente le risorse in caso di errori nel log.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Di seguito viene riportato un esempio di operazione di disinstallazione:

```
# smo backup unmount -label test -profile SALES1 -verbose
```

```
SMO-13046 [INFO ]: Operation GUID 8abc013111b909eb0111b90a02f50001
starting on Profile SALES1
SMO-08028 [INFO ]: Beginning to disconnect connected mount(s)
[/u/user1/mnt/_mnt_ssyl_logs_SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a
45066210001,
 /u/user1/mnt/_mnt_ssyl_data_SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a
45066210001].
SMO-08030 [INFO ]: Done disconnecting connected mount(s)
[/u/user1/mnt/_mnt_ssyl_logs_SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a
45066210001,
 /u/user1/mnt/_mnt_ssyl_data_SMO_SALES1_hsdbs1_F_C_1_8abc013111a450480111a
45066210001].
SMO-13037 [INFO ]: Successfully completed operation: Backup Unmount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:00:33.715
Operation Id [8abc013111b909eb0111b90a02f50001] succeeded.
```

Informazioni correlate

[Smontare i backup](#)

Il comando **smo backup update**

È possibile eseguire il comando di aggiornamento del backup per aggiornare il criterio di conservazione del backup.

Sintassi

```
smo backup update
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-comment comment_text\]
[-quiet | -verbose]
```

Parametri

- **-profile_name**

Specifica il profilo per cui aggiornare i backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-id guid**

Verifica il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando `smo backup list` per visualizzare il GUID per ciascun backup.

- **etichetta ****

Specifica l'etichetta di backup e l'ambito del backup come file di dati o log di archiviazione.

- **-dati**

Specifica i file di dati.

- **-archivelogs**

Specifica i file di log dell'archivio.

- **-comment comment_text**

Inserire testo (fino a 200 caratteri) sull'aggiornamento del backup. È possibile includere spazi.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

- **-retain {-hourly | -giornaliero | -settimanale | -mensile | -illimitato}**

Specifica se il backup deve essere conservato su base oraria, giornaliera, settimanale, mensile o illimitata. Se non viene specificato `-retain`, il valore predefinito della classe retention è `-hourly`. Per conservare i backup per sempre, utilizza l'opzione `-Unlimited`. L'opzione `-Unlimited` rende il backup non idoneo per l'eliminazione.

Esempio

Nell'esempio seguente viene aggiornato il backup per impostare il criterio di conservazione su `Unlimited`:

```
smo backup update -profile SALES1 -label full_backup_sales_May  
-retain -unlimited -comment save_forever_monthly_backup
```

Informazioni correlate

[Modifica del criterio di conservazione del backup](#)

[Conservazione dei backup per sempre](#)

[Liberare o eliminare i backup esenti dai criteri di conservazione](#)

Il comando di verifica del backup smo

È possibile eseguire il comando di verifica del backup per verificare se il backup è in un formato valido per Oracle.

Sintassi

```
smo backup verify
-profile profile_name
[-label backup_name \ \[-id guid\]
\[-retain \{-hourly \ \ -daily \ \ -weekly \ \ -monthly \ \ -unlimited\}\]
\[-force\]
\[-dump\]
\[-quiet \ \ -verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo per il quale si desidera verificare un backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-id guid**

Verifica il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando `smo backup list` per visualizzare il GUID per ciascun backup.

- **-label label nome_etichetta**

Verifica il backup con l'etichetta specificata.

- **-dump**

Raccoglie i file dump dopo l'operazione di verifica del backup riuscita o non riuscita.

- **-force**

Forza il database nello stato necessario per eseguire l'operazione di verifica.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Di seguito viene riportato un esempio di verifica del backup:

```
smo backup verify -profile SALES1 -label full_backup_sales_May -quiet
```

```
DBVERIFY - Verification starting : FILE =  
+SMO_1_1161675083835/smo/datafile/data.277.582482539 ...
```

Informazioni correlate

[Verifica dei backup del database](#)

Comando di creazione del clone smo

È possibile eseguire il comando `clone create` per creare un clone di un database di cui è stato eseguito il backup. È possibile clonare un backup dallo storage primario o secondario.

Sintassi

```
smo clone create  
-profile profile_name  
[-backup-id backup_guid \|-backup-label backup_label_name \|-current\  
-newsid new_sid  
\[-host target_host\  
[-label clone_label]  
\[-comment string\  
-clonespec full_path_to_clonespec_file  
\[-asminstance -asmusername asminstance_username -asmpassword  
asminstance_password\  
\[-syspassword syspassword\  
\[-reserve \{yes \| no \| inherit\}\]  
\[-from-secondary \{-copy-id id\}\]  
\[-no-resetlogs \|-recover-from-location path1 \[, path2\]\]\[-taskspec  
taskspec\  
\[-dump\  
\[-quiet \|-verbose\  

```

Parametri

- **-nome profilo**

Specifica il database che si desidera clonare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-backup-id guid**

Clona il backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. È possibile utilizzare il comando `smo backup list-verbose` per visualizzare il GUID per ciascun backup.

- **-backup-label backup_label_name**

Specifica di clonare il backup con il nome dell'etichetta specificato.

- **-corrente**

Specifica di creare backup e cloni a partire dallo stato corrente del database.



Se il database si trova in modalità `noarchivelog`, SnapManager crea un backup offline.

- **-newsid new_sid**

Specifica un nuovo identificatore di sistema Oracle univoco per il database clonato. Il valore dell'identificatore di sistema è composto da un massimo di otto caratteri. Oracle non consente l'esecuzione simultanea di due database con lo stesso identificatore di sistema sullo stesso host.

- **-host target_host**

Specifica l'host su cui deve essere creato il clone.

- **-label clone_label**

Specifica un'etichetta per il clone.

- **-comment string**

Specifica un commento facoltativo per descrivere questo clone. È necessario racchiudere la stringa tra virgolette singole.



Alcune shell eliminano le virgolette. Se questo è vero per la tua shell, devi escapire la quotazione con una barra rovesciata (`\`). Ad esempio, potrebbe essere necessario immettere:
' Questo è un commento '

- **-clonespec percorso completo al file clonespec**

Specifica il percorso del file XML di specifica del clone. Può essere un nome di percorso relativo o assoluto.

- **-preminenza**

Specifica le credenziali utilizzate per accedere all'istanza di ASM.

- **-asmusername asminstance_username**

Specifica il nome utente utilizzato per accedere all'istanza di ASM.

- **-asmpassword asminstance_password**

Specifica la password utilizzata per accedere all'istanza di ASM.

- **-syspassword syspassword**

Specifica la password per l'utente con privilegi sys.



È necessario fornire la password per l'utente con privilegi di sistema se le credenziali del database fornite non sono le stesse per l'utente con privilegi di sistema.

- **-reserve**

L'impostazione dell'opzione -Reserve su yes garantisce che la riserva di spazio garantita del volume sia attivata per i nuovi volumi clone. L'impostazione dell'opzione -Reserve su no garantisce che la riserva di spazio garantita del volume sia disattivata per i nuovi volumi clone. L'impostazione dell'opzione -Reserve per ereditare garantisce che il nuovo clone erediti le caratteristiche di spazio riservato della copia Snapshot padre. L'impostazione predefinita è no

La tabella seguente descrive i metodi di cloning e il loro effetto sull'operazione di creazione del clone e la relativa opzione -Reserve. È possibile clonare un LUN utilizzando uno dei due metodi.

Metodo di cloning	Descrizione	Risultato
LUN cloning	A new clone LUN is created within the same volume.	When the -reserve option for a LUN is set to yes, space is reserved for the full LUN size within the volume.
Volume cloning	A new FlexClone is created, and the clone LUN exists within the new clone volume. Uses the FlexClone technology.	When the -reserve option for a volume is set to yes, space is reserved for the full volume size within the aggregate.
		+

- **-from-secondary [-copy-idcopy_id]**

Specifica che SnapManager deve clonare una copia di un backup che è stato protetto sullo storage secondario. Se questa opzione non viene specificata, SnapManager clona la copia dallo storage primario.

Specificare l'opzione -copy-id ogni volta che si specifica l'opzione -from-secondary. Se nel sistema di storage secondario sono presenti più backup, viene utilizzata l'opzione -copy-id per specificare quale copia

di backup nello storage secondario deve essere utilizzata per la clonazione.



Se si utilizza Data ONTAP in modalità 7, è necessario specificare un valore valido per l'opzione `-copy-id`. Tuttavia, se si utilizza Clustered Data ONTAP, l'opzione `-copy-id` non è richiesta.

- **-no-resetlog**

Specifica di ignorare il ripristino del database, eseguire l'utilità DBNEWID e non aprire il database con i resetlog durante la creazione del clone.

- **-recovery-from-location**

Specifica la posizione del log di archiviazione esterno dei backup del log di archiviazione in cui SnapManager preleva i file di log di archiviazione dalla posizione esterna e li utilizza per la clonazione.

- **-taskspec**

Specifica il file XML della specifica dell'attività per l'attività di pre-elaborazione o di post-elaborazione dell'operazione clone. Specificare il percorso completo del file XML per la specifica dell'attività.

- **-dump**

Specifica di raccogliere i file dump dopo l'operazione di creazione del clone.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio riportato di seguito viene clonato il backup utilizzando una specifica di cloni creata per questo clone:

```
smo clone create -profile SALES1 -backup-label full_backup_sales_May
-newsid
CLONE -label sales1_clone -clonespec
/opt/<path>/smo/clonespecs/sales1_clonespec.xml
```

```
Operation Id [8abc01ec0e794e3f010e794e6e9b0001] succeeded.
```

Informazioni correlate

[Creazione di specifiche di cloni](#)

Il comando di eliminazione del clone smo

È possibile eseguire il comando di eliminazione dei cloni per eliminare un clone. Non è possibile eliminare un clone se utilizzato da un'operazione.

Sintassi

```
smo clone delete
-profile profile_name
\[-id guid \| -label clone_name\]
[-login
\[-username db_username -password db_password -port db_port\]
\[-asminstance -asmusername asminstance_username -asmpassword
asminstance_password\]]
\[-syspassword syspassword\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo contenente il clone da eliminare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-force**

Elimina il clone anche se sono presenti risorse associate al clone.

- **-id guid**

Specifica il GUID per il clone da eliminare. Il GUID viene generato da SnapManager quando si crea un clone. È possibile utilizzare il comando smo clone list per visualizzare il GUID per ciascun clone.

- **-label name**

Specifica l'etichetta per il clone da eliminare.

- **-preminenza**

Specifica le credenziali utilizzate per accedere all'istanza di Automatic Storage Management (ASM).

- **-asmusername asminstance_username**

Specifica il nome utente utilizzato per accedere all'istanza di ASM.

- **-asmpassword asminstance_password**

Specifica la password utilizzata per accedere all'istanza di ASM.

- **-syspassword syspassword**

Specifica la password per l'utente con privilegi sys.



È necessario fornire la password per l'utente con privilegi di sistema se le credenziali del database fornite non sono le stesse per l'utente con privilegi di sistema.

- **-login**

Consente di immettere i dettagli di accesso al database.

- **-nome utente db_nome utente**

Specifica il nome utente richiesto per accedere al database.

- **-password db_password**

Specifica la password richiesta per accedere al database.

- **-port db_port**

Specifica il numero di porta TCP utilizzato per accedere al database descritto dal profilo.

- **-dump**

Specifica di raccogliere i file dump dopo l'operazione di eliminazione del clone.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Il seguente esempio elimina il clone:

```
smo clone delete -profile SALES1 -label SALES_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Il comando smo clone list

Questo comando elenca i cloni del database per un determinato profilo.

Sintassi

```
smo clone list
-profile profile_name
-delimiter character
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica l'elenco dei cloni associati al profilo. Il profilo contiene l'identificatore del database e altre informazioni del database.

- carattere **-delimitatore**

Quando viene specificato questo parametro, il comando elenca gli attributi in ogni riga separati dal carattere specificato.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente sono elencati i cloni del database nel profilo SALES1.

```
smo clone list -profile SALES1 -verbose
```

```
ID Status SID Host Label Comment
-----
8ab...01 SUCCESS hsdhc server1 backlclone test comment
```

Informazioni correlate

[Visualizzazione di un elenco di cloni](#)

Comando di visualizzazione del clone smo

È possibile eseguire il comando clone show per visualizzare le informazioni sui cloni del database per il profilo specificato.

Sintassi

```
smo clone show
-profile profile_name
\[-id guid \|-label clone_name\]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica l'elenco dei cloni associati al profilo. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-id guid**

Mostra le informazioni sul clone con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un clone. È possibile utilizzare il comando `smo clone show` per visualizzare il GUID per ciascun clone.

- **-label label nome_etichetta**

Mostra le informazioni sul clone con l'etichetta specificata.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente vengono visualizzate informazioni sul clone:

```
smo clone show -profile SALES1 -label full_backup_sales_May -verbose
```

Il seguente output mostra informazioni su un clone di un backup sullo storage primario:

```
Clone id: 8abc013111b916e30111b916ffb40001
Clone status: SUCCESS
Clone SID: hsdbsc
Clone label: hsdbsc
Clone comment: null
Clone start time: 2007-04-03 16:15:50
Clone end time: 2007-04-03 16:18:17
Clone host: Host1
Filesystem: /mnt/ssys1/data_clone
File: /mnt/ssys1/data_clone/hsdb/sysaux01.dbf
File: /mnt/ssys1/data_clone/hsdb/undotbs01.dbf
File: /mnt/ssys1/data_clone/hsdb/users01.dbf
File: /mnt/ssys1/data_clone/hsdb/system01.dbf
File: /mnt/ssys1/data_clone/hsdb/undotbs02.dbf
Backup id: 8abc013111a450480111a45066210001
Backup label: full_backup_sales_May
Backup SID: hsdbs1
Backup comment:
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Backup host: server1
```

Il seguente output mostra informazioni su un clone di un backup protetto su uno storage secondario:

```
clone show -label clone_CLSTEST -profile
TEST_USER_NFSTEST_DIRMAC
Clone id:8abc01ec16514aec0116514af52f0001
Clone status: SUCCESS
Clone SID: CLSTEST
Clone label: clone_CLSTEST
Clone comment:comment_for_clone_CLSTEST
Clone start time: 2007-11-18 00:46:10
Clone end time: 2007-11-18 00:47:54
Clone host: dirmac
Filesystem: /ant/fish/bt_dirmac_nfs_clone
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/sysaux01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/system01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/undotbs01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/users01.dbf
Backup id: 8abc01ec16514883011651488b580001
Backup label:full_backup
Backup SID: NFSTEST
Backup comment:
Backup start time: 2007-11-18 00:43:32
Backup end time: 2007-11-18 00:45:30
Backup host: dirmac
Storage System: fish (Secondary storage)
Volume: bt_dirmac_nfs
Snapshot:smo_user_nfstest_b_nfstest_f_c_1_8abc01ec16511d6a0116511d73590001
_0
File: /ant/fish/bt_dirmac_nfs/archlogs/1_14_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/sysaux01.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/undotbs01.dbf
File: /ant/fish/bt_dirmac_nfs/archlogs/1_13_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/archlogs_2/1_16_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/users01.dbf
File: /ant/fish/bt_dirmac_nfs/controlfiles/SMBakCtl_1195361899651_2
File: /ant/fish/bt_dirmac_nfs/datafiles/system01.dbf
```

Informazioni correlate

[Visualizzazione di informazioni dettagliate sui cloni](#)

Il comando modello clone smo

Questo comando consente di creare un modello di specifica clone.

Sintassi

```
smo clone template
-profile name
\[ -backup-id guid \ | -backup-label backup_name \ ]
\[ -quiet \ | -verbose \ ]
```

Parametri

- **-nome profilo**

Specifica il database di cui si desidera creare una specifica di cloni. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-backup-id guid**

Crea una specifica clone dal backup con il GUID specificato. Il GUID viene generato da SnapManager quando si crea un backup. Utilizzare il comando `smo backup list` per visualizzare il GUID per ciascun backup.

- **-backup-label backup_label_name**

Crea una specifica clone dal backup con l'etichetta di backup specificata.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene creato un modello di specifica clone dal backup con l'etichetta `Full_backup_sales_May`. Una volta completato il comando del modello di clone `smo`, il modello di specifica del clone è completo.

```
smo clone template -profile SALES1 -backup-label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Informazioni correlate

[Creazione di specifiche di cloni](#)

[Clonare i database dai backup](#)

Il comando di aggiornamento del clone smo

Questo comando aggiorna le informazioni sul clone. È possibile aggiornare il commento.

Sintassi

```
smo clone update
-profile profile_name
\[-label label \| -id id\]
-comment comment_text
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo contenente il clone che si desidera aggiornare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **id -id**

Specifica l'ID del clone. L'ID viene generato da SnapManager quando si crea un clone. Utilizzare il comando `smo clone list` per visualizzare l'ID di ciascun clone.

- **etichetta ****

Specifica l'etichetta per il clone.

- **-commento**

Mostra il commento inserito nella creazione del clone. Questo è un parametro facoltativo.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene aggiornato il commento clone.

```
smo clone update -profile anson.pcrac5
-label clone_pcrac51_20080820141624EDT -comment See updated clone
```

Il comando split-delete del clone smo

Questo comando consente di eliminare una voce del ciclo operativo di suddivisione dei cloni da un database di repository.

Sintassi

```
smo clone split-delete
-profile profile \[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo del clone.

- **-host hostname**

Specifica il nome host in cui esiste il clone.

- **-label split-label**

Specifica il nome dell'etichetta generato dal processo di avvio della suddivisione del clone.

- **-id split-id**

Specifica l'ID univoco generato dal processo di avvio del clone split.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Il comando split-estimate clone smo

Questo comando consente di visualizzare la stima della quantità di storage consumata suddivisa in cloni.

Sintassi

```
smo clone split-estimate
-profile profile
\[-host hostname\]
\[-label clone-label \| -id clone-id\]
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo del clone.

- **-host hostname**

Specifica il nome host in cui esiste il clone.

- **-label clone-label**

Specifica il nome dell'etichetta generato dal processo di clonazione.

- **-id clone-id**

Specifica l'ID univoco generato dal processo di clonazione.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Il comando clone split di smo

È possibile eseguire il comando clone split per dividere un clone. Il clone split diventa indipendente dal clone originale. SnapManager genera un nuovo profilo dopo l'operazione di suddivisione del clone ed è possibile utilizzarlo per gestire il clone di divisione.

Sintassi

```

        smo clone split
-profile clone-profile
\[ -host hostname\]
\[ -label clone-label | -id clone-id\] \[ -split-label split-
operation_label\]
\[ -comment comment\]
-new-profile new-profile-name \[ -profile-password new-profile_password\]
-repository -dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database -dbname db_dbname
-host db_host \[ -sid db_sid\] \[ -login -username db_username -password
db_password
-port db_port\]
\[ -rman \{\{-controlfile \| \{-login -username rman_username
-password rman_password\} -tnsname rman_tnsname\}\}\]
-osaccount osaccount
-osgroup osgroup
\[ -retain
\[ -hourly \[ -count n\] \[ -duration m\]\]
\[ -daily \[ -count n\] \[ -duration m\]\]
\[ -weekly \[ -count n\] \[ -duration m\]\]
\[ -monthly \[ -count n\] \[ -duration m\]\] \]
\[ -profile-comment profile-comment\]
\[ -snapname-pattern pattern\]
\[ -protect \[ -protection-policy policy_name\]\] \| \[ -noprotect\]\]
\[ -summary-notification
\[ -notification
\[ -success -email email_address1,email_address2
-subject subject-pattern\]
\[failure -email email_address1,email_address2
-subject subject-pattern\] \]
[-separate-archivelog-backups
-retain-archivelog-backups
    -hours hours |
-days days |
-weeks weeks |
-months months
[-protect \[ -protection-policy policy_name \| -noprotect]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
\[ -quiet \| -verbose\]

```

Parametri

- **-profile clone-profile**

Specifica il nome del profilo da cui viene creato il clone.

- **-host hostname**

Specifica il nome host in cui esiste il clone.

- **-label clone-label**

Specifica il nome dell'etichetta generato dall'operazione di clonazione.

- **-id clone-id**

Specifica l'ID univoco generato dall'operazione di clone.

- **-split-label split-operation_label**

Specifica il nome dell'etichetta generato dall'operazione di clonazione.

- **-new-profile new_profile_name**

Specifica il nuovo nome del profilo che verrà generato da SnapManager dopo un'operazione di suddivisione.

- **-profile-password new-profile_password**

Specifica la password per il profilo.

- **-repository**

Specifica i dettagli del database per il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui risiede il database del repository.

- **-port repo_port**

Specifica il numero di porta TCP (Transmission Control Protocol) utilizzato per accedere all'host su cui risiede il database del repository.

- **-login**

Specifica i dettagli di accesso al repository. Questa opzione è facoltativa. Se non viene specificato, SnapManager passa automaticamente alla modalità di connessione autenticazione del sistema operativo.

- **-nome utente repo_nome utente**

Specifica il nome utente richiesto per accedere all'host su cui risiede il database del repository.

- **-database**

Specifica i dettagli del database di cui verrà eseguito il backup, il ripristino o la clonazione.

- **-dbname db_dbname**

Specifica il nome del database descritto dal profilo. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host db_host**

Specifica il nome o l'indirizzo IP del computer host su cui risiede il database.

- **-sid db_sid**

Specifica l'identificativo di sistema del database descritto dal profilo. Per impostazione predefinita, SnapManager utilizza il nome del database come identificatore di sistema. Se l'identificatore di sistema è diverso dal nome del database, è necessario specificarlo utilizzando l'opzione -sid.

Ad esempio, se si utilizzano i Real Application Clusters (RAC) di Oracle, è necessario specificare l'identificativo di sistema dell'istanza RAC sul nodo RAC da cui viene eseguito SnapManager.

- **-login**

Specifica i dettagli di accesso al database.

- **-nome utente db_nome utente**

Specifica il nome utente necessario per accedere al database descritto dal profilo.

- **-password db_password**

Specifica la password necessaria per accedere al database descritto dal profilo.

- **-rman**

Specifica i dettagli utilizzati da SnapManager per catalogare i backup con Oracle Recovery Manager (RMAN).

- **-controlfile**

Specifica i file di controllo del database di destinazione come repository RMAN anziché come catalogo.

- **-login**

Specifica i dettagli di accesso RMAN.

- **-password rman_password**

Specifica la password utilizzata per accedere al catalogo RMAN.

- **-username rman_username**

Specifica il nome utente utilizzato per accedere al catalogo RMAN.

- **-tnsname tnsname**

Specifica il nome di connessione tnsname (definito nel file tnsname.ora).

- **-osaccount**

Specifica il nome dell'account utente del database Oracle. SnapManager utilizza questo account per eseguire le operazioni Oracle, ad esempio l'avvio e lo spegnimento. In genere, è l'utente che possiede il software Oracle sull'host, ad esempio oracle.

- **-ossgroup**

Specifica il nome del nome del gruppo di database Oracle associato all'account oracle.



Le variabili -osaccount e -osgroup sono necessarie per UNIX ma non sono consentite per i database in esecuzione su Windows.

- **-retain [-hourly [-count n] [-duration m]] [-giornaliero [-count n] [-duration m]] [-settimanale [-count n] [-duration m]] [-mensile [-count n] [-duration m]]**

Specifica il criterio di conservazione per un backup.

Per ciascuna classe di conservazione, è possibile specificare sia il numero di conservazione che la durata della conservazione. La durata è espressa in unità della classe (ad esempio, ore per ora, giorni per giorno). Ad esempio, se si specifica solo una durata di conservazione di 7 per i backup giornalieri, SnapManager non limiterà il numero di backup giornalieri per il profilo (poiché il numero di conservazione è 0), ma SnapManager eliminerà automaticamente i backup giornalieri creati oltre 7 giorni fa.

- **-profile-comment profile-comment**

Specifica il commento per un profilo che descrive il dominio del profilo.

- **-snapname-pattern pattern**

Specifica il modello di denominazione per le copie Snapshot. È inoltre possibile includere testo personalizzato, ad esempio HAOPS per operazioni altamente disponibili, in tutti i nomi delle copie Snapshot. È possibile modificare il modello di denominazione della copia Snapshot quando si crea un profilo o dopo averlo creato. Il modello aggiornato si applica solo alle copie Snapshot non ancora create. Le copie Snapshot esistenti conservano il modello Snapname precedente. È possibile utilizzare diverse variabili nel testo del modello.

- **-protect -protection-policy policy policy_name**

Specifica se il backup deve essere protetto sullo storage secondario.



Se -Protect viene specificato senza -Protection-policy, il dataset non avrà una policy di protezione. Se viene specificato -Protect e -Protection-policy non viene impostato al momento della creazione del profilo, è possibile impostarlo in seguito mediante il comando di aggiornamento del profilo smo o impostarlo dall'amministratore dello storage utilizzando la console di Protection Manager.

- **-summary-notification**

Specifica i dettagli per la configurazione della notifica e-mail di riepilogo per più profili in un database di

repository. SnapManager genera questo messaggio e-mail.

- **-notifica**

Specifica i dettagli per la configurazione della notifica e-mail per il nuovo profilo. SnapManager genera questo messaggio e-mail. La notifica e-mail consente all'amministratore del database di ricevere e-mail sullo stato riuscito o non riuscito dell'operazione del database eseguita utilizzando questo profilo.

- **-successo**

Specifica che la notifica e-mail viene attivata per un profilo per il momento in cui l'operazione SnapManager ha esito positivo.

- **-email address 1 email address 2**

Specifica l'indirizzo e-mail del destinatario.

- **-subject-pattern**

Specifica l'oggetto del messaggio di posta elettronica.

- **-guasto**

Specifica che la notifica e-mail è attivata per un profilo per quando l'operazione SnapManager non riesce.

- **-storage-backup-separati**

Specifica che il backup del registro di archiviazione è separato dal backup del file di dati. Si tratta di un parametro facoltativo che è possibile fornire durante la creazione del profilo. Dopo aver separato i backup utilizzando questa opzione, è possibile creare un backup solo per i file di dati o un backup solo per i registri di archiviazione.

- **-retain-archiveog-backups -ore | -daysdays | -weeksweeks| -monthsmohts**

Specifica che i backup del registro di archiviazione vengono conservati in base alla durata di conservazione del registro di archiviazione (oraria, giornaliera, settimanale o mensile).

- **protect [-protection-policypolicy_name] | -noproduct**

Specifica che i file di log dell'archivio sono protetti in base al criterio di protezione del log dell'archivio.

Specifica che i file di log dell'archivio non sono protetti utilizzando l'opzione -noproduct.

- **-include-with-online-backups | -no-include-with-online-backups**

Specifica che il backup del registro di archiviazione è incluso insieme al backup del database online.

Specifica che i backup del registro di archiviazione non sono inclusi insieme al backup del database online.

- **-dump**

Specifica che i file dump non vengono raccolti dopo l'operazione di creazione del profilo.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita visualizza i messaggi di

errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Il comando clone smo split-risultato

Sintassi

Questo comando consente di visualizzare il risultato del processo di suddivisione dei cloni.

```
smo clone split-result
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo del clone.

- **-host hostname**

Specifica il nome host in cui esiste il clone.

- **-label split-label**

Specifica il nome dell'etichetta generato dal processo di avvio della suddivisione del clone.

- **-id split-id**

Specifica l'ID univoco generato dal processo di avvio della suddivisione del clone.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Il comando split-stop del clone smo

Questo comando interrompe il processo di suddivisione dei cloni in esecuzione.

Sintassi

```
smo clone split-stop
-profile profile
\[-host hostname\]
\[-label split-label \|-id split-id\]
\[-quiet \|-verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo del clone.

- **-host hostname**

Specifica il nome host in cui esiste il clone.

- **-label split-label**

Specifica il nome dell'etichetta generato dal processo di clonazione.

- **-id split-id**

Specifica l'ID univoco generato dal processo di clonazione.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Il comando di split-status del clone smo

Questo comando consente di conoscere l'avanzamento dell'esecuzione del processo di split.

Sintassi

```
smo clone split-status
-profile profile
\[-host hostname\]
\[-label split-label \|-id split-id\]
\[-quiet \|-verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo del clone.

- **-host hostname**

Specifica il nome host in cui esiste il clone.

- **-label split-label**

Specifica il nome dell'etichetta generato dal processo di clonazione.

- **-id split-id**

Specifica l'ID univoco generato dal processo di clonazione.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Il comando **smo clone disstach**

Dopo aver spartito un volume clonato dal volume padre in Data ONTAP, è possibile eseguire il comando clone Detach da SnapManager per far sapere a SnapManager che il volume non è più un clone.

Sintassi

```
clone smo detach -profile_name -label clone_label
```

Parametri

- **-profile_name**

Specifica il nome del profilo da cui viene creato il clone.

- **-label clone_label**

Specifica il nome generato dall'operazione di clonazione.

Esempio

Il seguente comando disconnette il clone:

```
smo clone detach -profile SALES1 -label sales1_clone
```

Il comando cmdfile smo

È possibile utilizzare il comando cmdfile per eseguire qualsiasi comando se la shell sull'host limita il numero di caratteri che possono essere visualizzati su una riga di comando.

Sintassi

```
smo cmdfile
-file file_name
\[-quiet \|-verbose\]
```

È possibile includere il comando in un file di testo e utilizzare il comando cmdfile smo per eseguire il comando. È possibile aggiungere un solo comando in un file di testo. Non includere smo nella sintassi del comando.



Il comando cmdfile smo sostituisce il comando pfile smo. Il cmdfile smo non è compatibile con il comando pfile smo.

Parametri

- **-file_name**

Specifica il percorso del file di testo contenente il comando da eseguire.

- **-quiet**

Specifica che nella console vengono visualizzati solo i messaggi di errore. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Specifica che i messaggi di errore, di avviso e informativi vengono visualizzati nella console.

Esempio

Questo esempio crea un profilo includendo il comando di creazione del profilo in command.txt che si trova in /tmp. È quindi possibile eseguire il comando cmdfile smo.

Il file di testo contiene le seguenti informazioni:

```
profile create -profile SALES1 -repository -dbname SNAPMGR
-login -username server1_user -password ontap -port 1521 -host server1
-database -dbname SMO -sid SMO -login -username sys -password oracle -port
1521
-host Host2 -osaccount oracle -osgroup db2
```

È ora possibile creare il profilo eseguendo il comando cmdfile smo con il file command.txt:

```
smo cmdfile -file /tmp/command.txt
```

Il comando smo credential clear

Questo comando cancella la cache delle credenziali utente per tutte le risorse protette.

Sintassi

```
smo credential clear  
\[ -quiet \| -verbose \]
```

Parametri

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Questo esempio cancella tutte le credenziali dell'utente che esegue il comando.

```
smo credential clear -verbose
```

```
SMO-20024 [INFO ]: Cleared credentials for user "user1".
```

Informazioni correlate

[Cancellazione delle credenziali utente per tutti gli host, i repository e i profili](#)

Il comando smo credential delete

Questo comando elimina le credenziali dell'utente per una particolare risorsa protetta.

Sintassi

```
smo credential delete
\[-host -name host_name
-username username\] \[
[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port\] \[
\[-profile
-name profile_name\]
[-quiet | -verbose]
```

Parametri

- **-host hostname**

Specifica il nome del server host su cui è in esecuzione SnapManager.

Il parametro -host include le seguenti opzioni:

- -Name host_name: Specifica il nome dell'host per il quale si desidera eliminare la password.
- -Nome_utente: Specifica il nome utente sull'host.

- **-repository -dbname**

Specifica il nome del database in cui è memorizzato il profilo. Utilizzare il nome globale o il SID.

Il parametro -repository include le seguenti opzioni:

- -Dbnamerepo_service_name: Specifica il nome del database che memorizza il profilo. Utilizzare il nome globale o il SID.
- -Host repo_host: Specifica il nome o l'indirizzo IP del server host su cui viene eseguito il database del repository.
- -Login-Username repo_Username: Specifica il nome utente necessario per accedere al database che memorizza il repository.
- -Port repo_port: Specifica il numero di porta TCP utilizzato per accedere al database che memorizza il repository.

- **-profile -name profile_name**

Specifica il profilo a cui è associato il database.

Il parametro -profile include la seguente opzione:

- -Name profilename: Specifica il nome del profilo per il quale si desidera eliminare la password.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Questo esempio elimina le credenziali del profilo.

```
smo credential delete -profile -name user1 -verbose
```

```
SMO-20022 [INFO ]: Deleted credentials and repository mapping  
for profile "user1" in user credentials for "user1".
```

Questo esempio elimina le credenziali del repository.

```
smo credential delete -repository -dbname SMOREPO -host Host2  
-login -username user1 -port 1521
```

```
SMO-20023 [INFO ]: Deleted repository credentials for  
"user1@SMOREPO/wasp:1521"  
and associated profile mappings in user credentials for "user1".
```

Questo esempio elimina le credenziali dell'host.

```
smo credential delete -host -name Host2
```

```
SMO-20033 [INFO ]: Deleted host credentials for "Host2" in user  
credentials for "user1".
```

Informazioni correlate

[Eliminazione delle credenziali per le singole risorse](#)

Il comando **smo credential list**

Questo comando elenca tutte le credenziali di un utente.

Sintassi

```
smo credential list
\[-quiet \|-verbose\]
```

Parametri

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

In questo esempio vengono visualizzate tutte le credenziali dell'utente che esegue il comando.

```
smo credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMOREPO/hotspur:1521
Host2_test_user@SMOREPO/hotspur:1521
user1_1@SMOREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]
Hosts:
Host2
Host5
Host4
Host1
```

Informazioni correlate

[Visualizzazione delle credenziali dell'utente](#)

Il comando smo credential set

Questo comando consente di impostare le credenziali per consentire agli utenti di accedere a risorse sicure, come host, repository e profili di database. La password host è la password dell'utente sull'host su cui è in esecuzione SnapManager. La password del repository è la password dell'utente Oracle che contiene lo schema del repository

SnapManager. La password del profilo è una password creata dalla persona che crea il profilo. Per le opzioni host e repository, se l'opzione -password opzionale non è inclusa, verrà richiesto di inserire una password del tipo specificato negli argomenti del comando.

Sintassi

```
smo credential set
\[-host
-name host_name
-username username\]
\[-password password\] \] \[
\[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username\] \[-password repo_password\] \]
-port repo_port \[
\[-profile
-name profile_name\]
\[-password password\] \]
\[-quiet \[ -verbose\]
```

Parametri

- **-host hostname**

Specifica il nome o l'indirizzo IP del server host su cui è in esecuzione SnapManager.

Il parametro -host include le seguenti opzioni:

- -Name host_name: Specifica il nome dell'host per il quale impostare la password.
- -Nome_utente: Specifica il nome utente sull'host.
- -Password password password: Specifica la password dell'utente sull'host.

- **-repository -dbname**

Specifica il nome del database in cui è memorizzato il profilo. Utilizzare il nome globale o il SID.

Il parametro -repository include le seguenti opzioni:

- -Dbnamerepo_service_name: Specifica il nome del database che memorizza il profilo. Utilizzare il nome globale o il SID.
- -Host repo_host: Specifica il nome o l'indirizzo IP del server host su cui viene eseguito il database del repository.
- -Login-Username repo_Username: Specifica il nome utente necessario per accedere al database che memorizza il repository.
- -Password password password: Specifica la password necessaria per accedere al database che memorizza il repository.
- -Port repo_port: Specifica il numero di porta TCP utilizzato per accedere al database che memorizza il

repository.

- **-profile -name profile_name**

Specifica il profilo a cui è associato il database.

Il parametro -profile include la seguente opzione:

- -Name nomefile: Specifica il nome del profilo per cui si desidera impostare la password.
- -Password password: Specifica la password necessaria per accedere al profilo.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando per l'impostazione delle credenziali del repository

Nell'esempio seguente vengono impostate le credenziali per un repository.

```
smo credential set -repository -dbname SMOREPO -host hotspur -port 1521  
-login -username chris  
Password for chris@hotspur:1521/SMOREPO : *****  
Confirm password for chris@hotspur:1521/SMOREPO : *****
```

```
SMO-12345 [INFO ]: Updating credential cache for OS user "admin1"  
SMO-12345 [INFO ]: Set repository credential for user "user1" on  
repol@Host2.  
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

Esempio di comando per l'impostazione delle credenziali dell'host

Poiché una credenziale host rappresenta una credenziale effettiva del sistema operativo, deve includere il nome utente oltre alla password.

```
smo credential set -host -name bismarck -username avida  
Password for avida@bismarck : *****  
Confirm password for avida@bismarck : *****
```

Informazioni correlate

[In che modo SnapManager mantiene la sicurezza](#)

Il comando smo history list

Questo comando consente di visualizzare un elenco dei dettagli della cronologia dell'operazione SnapManager.

Sintassi

```
smo history list
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-database repo_database
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database che memorizza il profilo.

- **-database repo_database**

Specifica il nome del database in cui è memorizzato il profilo. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-operation {-operationsnome_operazione [nome_operazione 1, nome_operazione 2] | -all**

Specifica l'operazione SnapManager per la quale si configura la cronologia.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

```
smo history list -profile -name PROFILE1 -operation -operations
backup -verbose
```

Il comando di visualizzazione delle operazioni della cronologia smo

Questo comando consente di visualizzare la cronologia di un'operazione SnapManager specifica associata a un profilo.

Sintassi

```
smo history operation-show
-profile profile
\{-label label \| -id id\}
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **etichetta * | -id***

Specifica l'ID o l'etichetta dell'operazione SnapManager per la quale si desidera visualizzare la cronologia.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

```
smo history operation-show -profile PROFILE1 -label backup1
-verbose
```

Il comando di eliminazione della cronologia smo

Questo comando consente di eliminare la cronologia delle operazioni SnapManager.

Sintassi

```
smo history purge
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database che memorizza il profilo.

- **-dbname repo_dbname**

Specifica il nome del database in cui è memorizzato il profilo. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-operation {-operations nome_operazione [nome_operazione 1, nome_operazione 2] | -all**

Specifica l'operazione SnapManager per la quale si configura la cronologia.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

```
smo history purge -profile -name PROFILE1 -operation
-operations backup
-verbose
```

Il comando di rimozione della cronologia smo

Questo comando consente di rimuovere la cronologia delle operazioni SnapManager associate a un singolo profilo, a più profili o a tutti i profili in un repository.

Sintassi

```
smo history remove
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-database repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name,
operation_name2\] \| -all\}
\[-quiet \| -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database che memorizza il profilo.

- **-dbname repo_dbname**

Specifica il nome del database in cui è memorizzato il profilo. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-operation {-operationsnome_operazione [nome_operazione 1, nome_operazione 2] | -all**

Specifica l'operazione SnapManager per la quale si configura la cronologia.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

```
smo history purge -profile -name PROFILE1 -operation  
-operations backup  
-verbose
```

Il comando smo history set

È possibile eseguire il comando history set per configurare le operazioni per le quali si desidera visualizzare la cronologia.

Sintassi

```

    smo history set
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
-retain
{-count retain_count \| -daily daily_count \| -monthly monthly_count \|
-weekly weekly_count}
[-quiet | -verbose]

```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Il nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-repository**

Specifica i dettagli del database in cui è memorizzato il profilo.

- **-dbname repo_dbname**

Specifica il nome del database in cui è memorizzato il profilo. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host repo_host**

Specifica il nome o l'indirizzo IP dell'host in cui risiede il database del repository.

- **-login**

Specifica i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente richiesto per accedere al database del repository.

- **-port repo_port**

Specifica il numero di porta TCP (Transmission Control Protocol) utilizzato per accedere al database del repository.

- **-operation {-operations nome_operazione [nome_operazione 1, nome_operazione 2] | -all**

Specifica le operazioni SnapManager per cui si desidera configurare la cronologia.

- **-retain {-countretain_count | -dailydaily_count | -mensile-mensile_count | -settimanale_count}**

Specifica la classe di conservazione delle operazioni di creazione del backup, verifica del backup, ripristino e ripristino, creazione e suddivisione del clone. La classe di conservazione viene impostata in base al numero di operazioni, al numero di giorni, settimane o mesi.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio di comando

Nell'esempio seguente vengono visualizzate informazioni sull'operazione di backup:

```
smo history set -profile -name PROFILE1 -operation -operations backup
-retain -daily 6
-verbose
```

Il comando smo history show

Questo comando consente di visualizzare informazioni dettagliate sulla cronologia di un profilo specifico.

Sintassi

```
smo history show
-profile profile
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

```
smo history show -profile -name PROFILE1  
-verbose
```

Il comando help di smo

È possibile eseguire il comando help per visualizzare informazioni sui comandi SnapManager e sulle relative opzioni. Se non si fornisce un nome di comando, viene visualizzato un elenco di comandi validi. Se si fornisce un nome di comando, viene visualizzata la sintassi per tale comando.

Sintassi

```
smo help  
\[backup\|cmdfile\|clone\|credential\|help\|operation\|profile\|protection  
-policy\|repository\|system\|version\|plugin\|diag\|history\|schedule\|not  
ification\|storage\|get\  
\[ -quiet \| -verbose\]
```

Parametri

Di seguito sono riportati alcuni nomi di comando che è possibile utilizzare con questo comando:

- backup
- clonare
- cmdfile
- credenziale
- diag
- ottieni
- notifica
- aiuto
- storia
- operazione
- plug-in
- profilo
- policy di protezione
- repository
- pianificazione
- storage
- sistema

- versione

Il comando di notifica smo remove-summary-notification

Questo comando disattiva la notifica di riepilogo per più profili in un database repository.

Sintassi

```
smo notification remove-summary-notification
-repository
-dbname repo_service_name
-port repo_port
-host repo_host
-login -username repo_username
\[-quiet \|-verbose\]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login repo_username**

Specifica il nome di accesso necessario per accedere al database in cui è memorizzato il repository.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Nell'esempio seguente viene disattivata la notifica di riepilogo per più profili in un database di repository.

```
smo notification remove-summary-notification -repository -port 1521
-dbname repo2 -host 10.72.197.133 -login -username oba5
```

Il comando `smo notification update-summary-notification`

È possibile eseguire il comando di notifica `update-summary-notification` per attivare la notifica di riepilogo per un database repository.

Sintassi

```
smo notification update-summary-notification
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
-email email-address1,email-address2
-subject subject-pattern
-frequency
[-daily -time daily_time \
-hourly -time hourly_time \
-monthly -time monthly_time -date \[1\|2\|3\|...\|31\] \
-weekly -time weekly_time -day \[1\|2\|3\|4\|5\|6\|7\]\]
-profiles profile1,profile2
-notification-host notification-host
\[ -quiet \| -verbose\]
```

Parametri

- **-repository**

Specifica i dettagli del database del repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database del repository.

- **-dbname repo_service_name**

Specifica il nome del database del repository. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host repo_host**

Specifica il nome o l'indirizzo IP dell'host su cui risiede il database del repository.

- **-login**

Specifica i dettagli di accesso al repository. Questa opzione è facoltativa. Se non viene specificato, SnapManager passa automaticamente alla modalità di connessione autenticazione del sistema operativo.

- **-nome utente repo_nome utente**

Specifica il nome utente richiesto per accedere al database del repository.

- **-email-address1,email-address2**

Specifica gli indirizzi e-mail dei destinatari.

- **-subject-pattern**

Specifica il modello dell'oggetto del messaggio di posta elettronica.

- **-frequency { -daily --time daily_time | -hourly --time hourly_time | -monthly --time mensile_time -date {1|2|3...|31 } | -settimanale --time daily_time -day {1|2|3|4|5|6|7 } }**

Specifica il tipo di pianificazione e l'ora in cui si desidera ricevere la notifica via email.

- **-profile1, profile2**

Specifica i nomi dei profili che richiedono la notifica via email.

- **-notification-host notification-host**

Specifica l'host del server SnapManager da cui viene inviata l'email di notifica di riepilogo ai destinatari. È possibile specificare il nome host o l'indirizzo IP dell'host di notifica. È inoltre possibile aggiornare l'IP host o il nome host.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente viene attivata la notifica di riepilogo per un database di repository:

```
smo notification update-summary-notification -repository -port 1521
-dbname repo2 -host 10.72.197.133 -login -username oba5 -email
admin@org.com -subject success -frequency -daily -time 19:30:45 -profiles
sales1
```

Il comando smo notification set

Per configurare il server di posta, è possibile utilizzare il comando set di notifiche.

Sintassi

```
smo notification set
-sender-email email_address
-mailhost mailhost
-mailport mailport
[-authentication
-username username
-password password]
-repository
-dbname repo_service_name
-port repo_port]
-host repo_host
-login -username repo_username
[-quiet | -verbose]
```

Parametri

- **-sender-email email_address**

Specifica l'indirizzo e-mail del mittente da cui vengono inviati gli avvisi e-mail. Da SnapManager 3.2 per Oracle, è possibile includere un trattino (-) specificando il nome di dominio dell'indirizzo e-mail. Ad esempio, è possibile specificare l'indirizzo e-mail del mittente come [-sender-email07lbfmdatacenter@continental-corporation.com](#).

- **-mailhost mailhost**

Specifica il nome o l'indirizzo IP del server host che gestisce le notifiche e-mail.

- **-mailport mailport**

Specifica il numero di porta del server di posta.

- **-authentication -nome utente -password password**

Specifica i dettagli di autenticazione per l'indirizzo e-mail. Specificare il nome utente e la password.

- **-repository**

Specifica i dettagli del database del repository.

- **-port repo_port**

Specifica il numero di porta TCP (Transmission Control Protocol) utilizzato per accedere al database del repository.

- **-dbname repo_service_name**

Specifica il nome del database del repository. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host repo_host**

Specifica il nome o l'indirizzo IP dell'host in cui risiede il database del repository.

- **-login**

Specifica i dettagli di accesso al repository. Questa opzione è facoltativa. Se non viene specificato, SnapManager passa automaticamente alla modalità di connessione autenticazione del sistema operativo.

- **-nome utente repo_nome utente**

Specifica il nome utente richiesto per accedere al database del repository.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente viene configurato il server di posta:

```
smo notification set -sender-email admin@org.com -mailhost
hostname.org.com -mailport 25 authentication -username davis -password
davis -repository -port 1521 -dbname SMOREPO -host hotspur
-login -username grabal21 -verbose
```

Il comando dump dell'operazione smo

È possibile eseguire il comando dump dell'operazione per creare un file JAR contenente informazioni diagnostiche su un'operazione.

Sintassi

```
smo operation dump
-profile profile_name
\[-label label_name \|-id guid\]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo per cui si desidera creare i file dump. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-label label nome_etichetta**

Crea file dump per l'operazione e assegna l'etichetta specificata.

- **-id guid**

Crea file dump per l'operazione con il GUID specificato. Il GUID viene generato da SnapManager all'inizio dell'operazione.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente viene creato il file dump per il backup:

```
smo operation dump -profile SALES1
-id 8abc01ec0e78f3e2010e78f3fdd00001
```

```
Dump file created
Path:/userhomedirectory/.netapp/smo/3.3/smo_dump_8abc01ec0e78f3e2010e78f3fdd00001.jar
```

Informazioni correlate

[Eseguire il dump dei file](#)

Il comando smo Operation list

Questo comando elenca le informazioni di riepilogo di tutte le operazioni registrate in base a un profilo specifico.

Sintassi

```
smo operation list
-profile profile_name
\[-delimiter character\]
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **carattere -delimitatore**

(Facoltativo) quando viene specificato questo parametro, il comando elenca ogni riga su una riga separata e gli attributi in tale riga sono separati dal carattere specificato.

- **-quiet**

(Facoltativo) Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

(Facoltativo) Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio riportato di seguito sono elencate le informazioni di riepilogo di tutte le operazioni registrate in relazione al profilo specificato.

```
smo operation list -profile myprofile
```

```
Start Date Status Operation ID Type Host
-----
2007-07-16 16:03:57 SUCCESS 8abc01c813d0a1530113d0a15c5f0005 Profile
Create Host3
2007-07-16 16:04:55 FAILED 8abc01c813d0a2370113d0a241230001 Backup Host3
2007-07-16 16:50:56 SUCCESS 8abc01c813d0cc580113d0cc60ad0001 Profile
Update Host3
2007-07-30 15:44:30 SUCCESS 8abc01c81418a88e011418a8973e0001 Remove Backup
Host3
2007-08-10 14:31:27 SUCCESS 8abc01c814510ba20114510bac320001 Backup Host3
2007-08-10 14:34:43 SUCCESS 8abc01c814510e9f0114510ea98f0001 Mount Host3
2007-08-10 14:51:59 SUCCESS 8abc01c814511e6e0114511e78d40001 Unmount Host3
```

Informazioni correlate

[Visualizzazione di un elenco di operazioni](#)

Il comando show dell'operazione smo

È possibile eseguire il comando show dell'operazione per elencare le informazioni di riepilogo di tutte le operazioni eseguite rispetto al profilo specificato. L'output elenca l'utente client (l'utente per il PC client) e l'utente effettivo (l'utente in SnapManager valido sull'host selezionato).

Sintassi

```
smo operation show
-profile profile_name
\[-label label \| -id id\]
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **etichetta ****

Specifica l'etichetta per l'operazione.

- **id -id**

Specifica l'identificativo dell'operazione.

- **-quiet**

Facoltativo: Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Facoltativo: Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

La seguente riga di comando mostra informazioni dettagliate su un'operazione:

```
# smo operation show -profile myprofile -id
ff8080811295eb1c011295eb28230001
```

```
Operation Attempted
  Operation ID: ff8080811295eb1c011295eb28230001
  Type:RestoreFor profile: myprofile
  With Force: No
  Performed on backup
  Operation ID: ff8080811295eb1c011296eb23290001
  Label: mylabel
Operation Runtime Information
  Status: SUCCESS
  Start date: 2007-07-16 13:24:09 IST
  End date: 2007-07-16 14:10:10 IST
  Client user: amorrow
  Effective user: amorrow
Host
  Host Run upon: Host3
  Process ID: 3122
  SnapManager version: 3.3
Repository
  Connection: user1@SMOREPO/hotspur:1521
  Repository version: 3.3
Resources in use
  Volume:
    ssys1:/vol/luke_ES0_0 (FlexClone)
  Filesystems:
    /opt/NetApp/smo/mnt/-
mnt_ssys1_luke_ES0_smo_e_es0_f_c_1_8abc0112129b0f81580001_0
```

Informazioni correlate

[Visualizzazione dei dettagli delle operazioni](#)

Il comando di reimpostazione della password smo

È possibile eseguire il comando di reimpostazione della password per reimpostare la password di un profilo.

Sintassi

```
smo password reset
-profile profile
\[-profile-password profile_password\]
\[-repository-hostadmin-password repository_hostadmin_password\]
[-quiet | -verbose]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo per cui si desidera reimpostare la password.

- **-profile-password profile_password**

Specifica la nuova password per il profilo.

- **-repository-hostadmin-password admin_password**

Specifica la credenziale dell'utente autorizzato con privilegio root per il database del repository.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Il comando smo plugin check

SnapManager consente di installare e utilizzare script personalizzati per varie operazioni. SnapManager offre plug-in di backup, ripristino e clonazione per automatizzare gli script personalizzati prima e dopo le operazioni di backup, ripristino e clonazione. Prima di utilizzare il plug-in di backup, ripristino e clonazione, è possibile eseguire il comando di controllo del plug-in per verificare l'installazione degli script dei plug-in. Gli script personalizzati sono memorizzati in tre directory: Policy (per gli script che devono sempre essere eseguiti prima dell'esecuzione delle operazioni di backup, ripristino o clonazione), pre (per gli script di pre-elaborazione) e post (per gli script di post-elaborazione).

Sintassi

```
smo plugin check  
  
-osaccount os_db_user_name
```

Parametro

- **-osaccount**

Specifica il nome utente del database del sistema operativo. Se non si immette l'opzione -osaccount, SnapManager controlla gli script del plug-in come utente root piuttosto che per un utente specifico.

Esempio

Nell'esempio seguente viene mostrato che il comando di controllo del plug-in ha trovato lo script

personalizzato policy1 memorizzato nella directory dei criteri come eseguibile. L'esempio mostra anche che gli altri due script personalizzati memorizzati nella pre-directory non restituiscono messaggi di errore (visualizzati con lo stato 0); tuttavia, il quarto script personalizzato (post-plugin1), trovato nella directory post, contiene errori (visualizzati con lo stato 3).

```
smo plugin check
Checking plugin directory structure ...
<installdir>/plugins/clone/policy
OK: 'policy1' is executable
<installdir>/plugins/clone/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/clone/post
ERROR: 'post-plugin1' is executable and returned status 3
<installdir>/plugins/backup/policy
OK: 'policy1' is executable
<installdir>/plugins/backup/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/backup/post
ERROR: 'post-plugin1' is executable and returned status 3
<installdir>/plugins/restore/policy
OK: 'policy1' is executable
<installdir>/plugins/restore/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/restore/post
ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

Informazioni correlate

[Clonazione di database e utilizzo di script plug-in personalizzati](#)

Il comando di creazione del profilo smo

È possibile eseguire il comando di creazione del profilo per creare un profilo di un database in un repository. È necessario montare il database prima di eseguire questo comando.

Sintassi

```
smo profile create
-profile profile
\[-profile-password profile_password\]
-repository
```

```

-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database
-dbname db_dbname
-host db_host
[-sid db_sid\]
[-login
\[-username db_username -password db_password -port db_port\]
\[-asminstance -asmusername asminstance_username -asmpassword
asminstance_password\]]
[-rman \{-controlfile \| \{-login
-username rman_username -password rman_password\}
-tnsname rman_tnsname\}\}\}
\[-osaccount osaccount \]
\[-osgroup osgroup\]
[-retain
\[-hourly \[-count n\] \[-duration m\]\]
\[-daily \[-count n\] \[-duration m\]\]
\[-weekly \[-count n\] \[-duration m\]\]
\[-monthly \[-count n\] \[-duration m\]\]\]\]
-comment comment
-snapname-pattern pattern
[-protect \[-protection-policy policy\]]
[-summary-notification]
[-notification
\[-success
-email email_address1,email_address2
-subject subject_pattern\]
\[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups
-retain-archivelog-backups
-hours hours |
-days days |
-weeks weeks |
-months months
[-protect \[-protection-policy policy_name \| -noprotect]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
[-quiet | -verbose]

```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-profile-password profile_password**

Specificare la password per il profilo.

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database che memorizza il profilo.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il profilo. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-sid db_sid**

Specifica l'identificativo di sistema del database descritto dal profilo. Per impostazione predefinita, SnapManager utilizza il nome del database come identificatore di sistema. Se l'identificatore di sistema è diverso dal nome del database, è necessario specificarlo con l'opzione -sid.

Ad esempio, se si utilizzano i Real Application Clusters (RAC) di Oracle, è necessario specificare l'identificativo di sistema dell'istanza RAC sul nodo RAC da cui viene eseguito SnapManager.

- **-login**

Specifica i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database del repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database del repository.

- **-database**

Specifica i dettagli del database descritti dal profilo. Si tratta del database di cui verrà eseguito il backup, il ripristino o il cloning.

- **-dbname db_dbname**

Specifica il nome del database descritto dal profilo. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host db_host db_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database.

- **-preminenza**

Specifica le credenziali utilizzate per accedere all'istanza di Automatic Storage Management (ASM).

- **-asmusername asminstance_username**

Specifica il nome utente utilizzato per accedere all'istanza di ASM.

- **-asmpassword asminstance_password**

Specifica la password utilizzata per accedere all'istanza di ASM.

- **-login**

Specifica i dettagli di accesso al database.

- **-nome utente db_nome utente**

Specifica il nome utente necessario per accedere al database descritto dal profilo.

- **-password db_password**

Specifica la password necessaria per accedere al database descritto dal profilo.

- **-port db_port**

Specifica il numero di porta TCP utilizzato per accedere al database descritto dal profilo.

- **-rman**

Specifica i dettagli utilizzati da SnapManager per catalogare i backup con Oracle Recovery Manager (RMAN).

- **-controlfile**

Specifica i file di controllo del database di destinazione invece di un catalogo come repository RMAN.

- **-login**

Specifica i dettagli di accesso RMAN.

- **-password rman_password**

Specifica la password utilizzata per accedere al catalogo RMAN.

- **-username rman_username**

Specifica il nome utente utilizzato per accedere al catalogo RMAN.

- **-tnsname tnsname**

Specifica il nome di connessione tnsname (definito nel file tnsname.ora).

- **-osaccount**

Specifica il nome dell'account utente del database Oracle. SnapManager utilizza questo account per eseguire le operazioni Oracle, ad esempio l'avvio e lo spegnimento. In genere, è l'utente che possiede il software Oracle sull'host, ad esempio oracle.

- **-ossgroup**

Specifica il nome del nome del gruppo di database Oracle associato all'account oracle.

- **-retain [-hourly [-count n] [-duration m]] [-giornaliero [-count n] [-duration m]] [-settimanale [-count n] [-duration m]] [-mensile [-count n] [-duration m]]**

Specifica il criterio di conservazione per un backup in cui uno o entrambi i conteggi di conservazione insieme alla durata di conservazione per una classe di conservazione (oraria, giornaliera, settimanale, mensile).

Per ciascuna classe di conservazione, è possibile specificare uno o entrambi i valori di un conteggio o di una durata di conservazione. La durata è espressa in unità della classe (ad esempio, ore per ora, giorni per giorno). Ad esempio, se l'utente specifica solo una durata di conservazione di 7 per i backup giornalieri, SnapManager non limiterà il numero di backup giornalieri per il profilo (poiché il numero di conservazione è 0), ma SnapManager eliminerà automaticamente i backup giornalieri creati oltre 7 giorni fa.

- **-commento commento**

Specifica il commento per un profilo che descrive il dominio del profilo.

- **-snapname-pattern pattern**

Specifica il modello di denominazione per le copie Snapshot. È inoltre possibile includere testo personalizzato, ad esempio HAOPS per operazioni altamente disponibili, in tutti i nomi delle copie Snapshot. È possibile modificare il modello di denominazione della copia Snapshot quando si crea un profilo o dopo averlo creato. Il modello aggiornato si applica solo alle copie Snapshot non ancora create. Le copie Snapshot esistenti conservano il modello Snapname precedente. È possibile utilizzare diverse variabili nel testo del modello.

- **-protect -policy-protezione**

Indica se il backup deve essere protetto sullo storage secondario.



Se -protectis viene specificato senza -Protection-policy, il dataset non avrà una policy di protezione. Se viene specificato -Protect e -Protection-policy non viene impostato al momento della creazione del profilo, è possibile impostarlo successivamente tramite il comando di aggiornamento del profilo bysno o impostarlo dall'amministratore dello storage tramite la console di Protection Manager.

- **-summary-notification**

Specifica che la notifica email di riepilogo è attivata per il nuovo profilo.

- **-notification -success-email email email_address1,email address2 -subject subject_pattern**

Specifica che la notifica e-mail è attivata per il nuovo profilo in modo che i destinatari ricevano i messaggi e-mail quando l'operazione SnapManager ha esito positivo. È necessario immettere un singolo indirizzo e-mail o più indirizzi e-mail a cui inviare gli avvisi e-mail e un modello di oggetto e-mail per il nuovo profilo.

È inoltre possibile includere il testo dell'oggetto personalizzato per il nuovo profilo. È possibile modificare il testo dell'oggetto quando si crea un profilo o dopo averlo creato. L'oggetto aggiornato si applica solo ai messaggi e-mail non inviati. È possibile utilizzare diverse variabili per l'oggetto dell'e-mail.

- **-notification -failure -email email_address1,email address2 -subject subject_pattern**

Specifica che l'opzione attiva notifica e-mail è attivata per il nuovo profilo in modo che i destinatari ricevano i messaggi e-mail quando l'operazione SnapManager non riesce. È necessario immettere un singolo indirizzo e-mail o più indirizzi e-mail a cui inviare gli avvisi e-mail e un modello di oggetto e-mail per il nuovo profilo.

È inoltre possibile includere il testo dell'oggetto personalizzato per il nuovo profilo. È possibile modificare il testo dell'oggetto quando si crea un profilo o dopo averlo creato. L'oggetto aggiornato si applica solo ai messaggi e-mail non inviati. È possibile utilizzare diverse variabili per l'oggetto dell'e-mail.

- **-storage-backup-separati**

Specifica che il backup del registro di archiviazione è separato dal backup dei file di dati. Si tratta di un parametro facoltativo che è possibile fornire durante la creazione del profilo. Dopo aver separato il backup utilizzando questa opzione, è possibile eseguire il backup solo dei file di dati o il backup solo dei registri di archiviazione.

- **-retain-archiveog-backups -ore | -daysdays | -weeksweeks| -monthsmonths**

Specifica che i backup del registro di archiviazione vengono conservati in base alla durata di conservazione del registro di archiviazione (oraria, giornaliera, settimanale, mensile).

- **protect [-protection-policypolicy_name] | -noprotect**

Specifica di proteggere i file di log dell'archivio in base al criterio di protezione del log dell'archivio.

L'opzione -noprotect specifica di non proteggere i file di log dell'archivio.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

- **-include-with-online-backups**

Specifica che il backup del registro di archiviazione è incluso insieme al backup del database online.

- **-no-include-with-online-backups**

Specifica che i backup del registro di archiviazione non sono inclusi insieme al backup del database online.

- **-dump**

Specifica che i file dump vengono raccolti dopo l'operazione di creazione del profilo.

Esempio

Nell'esempio seguente viene illustrata la creazione di un profilo con policy di conservazione oraria e notifica via email:

```
smo profile create -profile test_rbac -profile-password netapp -repository  
-dbname SMOREP -host hostname.org.com -port 1521 -login -username smorep  
-database -dbname  
RACB -host saal -sid racb1 -login -username sys -password netapp -port  
1521 -rman -controlfile -retain -hourly -count 30 -verbose  
Operation Id [8abc01ec0e78ebda010e78ebe6a40005] succeeded.
```

Informazioni correlate

[Gestione dei profili per backup efficienti](#)

[Il comando Protection-policy smo](#)

[Naming delle copie Snapshot](#)

[In che modo SnapManager conserva i backup sullo storage locale](#)

Il comando smo profile delete

È possibile eseguire il comando di eliminazione del profilo per eliminare un profilo del database.

Sintassi

```
smo profile delete  
-profile profile  
\[ -quiet \| -verbose \]
```

Parametri

- **-profilo profilo**

Specifica il profilo da eliminare.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Il seguente esempio elimina il profilo:

```
smo profile delete -profile SALES1  
Operation Id [Ncaf00af0242b3e8dba5c68a57a5ae932] succeeded.
```

Informazioni correlate

[Eliminazione dei profili](#)

Il comando smo profile Destroy

Questo comando elimina il clone split (database) insieme al profilo generato da SnapManager durante il processo di split del clone.

Sintassi

```
smo profile destroy  
-profile profile  
\[ -host hostname\  
\[ -quiet \[ -verbose\]
```

Parametri

- **-profilo profilo**

Specifica il profilo generato da SnapManager dopo un processo di suddivisione dei cloni riuscito.

- **-host hostname**

Specifica il nome host in cui esiste il clone di split.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio riportato di seguito viene eliminato il profilo SALES1.

```
smo profile destroy -profile SALES1
```

Il comando di dump del profilo smo

È possibile eseguire il comando dump del profilo per creare il file .jar che contiene informazioni diagnostiche su un profilo.

Sintassi

```
smo profile dump
-profile profile_name
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il profilo per cui si desidera creare i file dump. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente viene creato un dump per il profilo SALES1:

```
smo profile dump -profile SALES1
Dump file created
Path:/userhomedirectory/.netapp/smo/3.3.0/smo_dump_SALES1_hostname.jar
```

Il comando smo profile list

Questo comando visualizza un elenco dei profili correnti.

Sintassi

```
smo profile list
\[-quiet \|-verbose\]
```

Parametri

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente vengono visualizzati i profili esistenti con i relativi dettagli.

```
smo profile list -verbose
Profile name: FGTER
Repository:
  Database name: SMOREPO
  SID: SMOREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: *****
Profile name: TEST_RBAC
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: *****
Profile name: TEST_RBAC_DP_PROTECT
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: *****
Profile name: TEST_HOSTCREDEN_OFF
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: *****
```

```
Profile name: SMK_PRF
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: *****
Profile name: FGLEX
Repository:
  Database name: SMOREPO
  SID: SMOREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: *****
```

Il comando show del profilo smo

È possibile eseguire il comando `profile show` per visualizzare le informazioni relative a un profilo.

Sintassi

```
smo profile show
-profile profile_name
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

L'esempio seguente mostra i dettagli del profilo:

```
smo profile show -profile TEST_RBAC_DP_PROTECT -verbose
Profile name: TEST_RBAC_DP_PROTECT
Comment:
Target database:
  Database name: racb
  SID: racb1
  Host: saal
  Port: 1521
  Username: sys
  Password: *****
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: *****
RMAN:
  Use RMAN via control file
Oracle user account: oracle
Oracle user group: dba
Snapshot Naming:
  Pattern: smo_{profile}_{db-sid}_{scope}_{mode}_{smid}
  Example:
smo_test_rbac_dp_protect_racb1_f_h_1_8abc01e915a55ac50115a55acc8d0001_0
Protection:
  Dataset: smo_saal_racb
  Protection policy: Back up
  Conformance status: CONFORMANT
Local backups to retain:
  Hourly: 4 copies
  Daily: 7 day(s)
  Weekly: 4 week(s)
  Monthly: 12 month(s)
```

Il comando **smo profile Sync**

Questo comando carica le mappature da profilo a repository per quel repository in un file nella home directory dell'host locale.

Sintassi

```
smo profile sync
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login
-username repo_username
\[-quiet \|-verbose\]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-dbname repo_service_name**

Specifica il database repository per il profilo da sincronizzare.

- **-host**

Specifica l'host del database.

- **-porta**

Specifica la porta per l'host.

- **-login**

Specifica il processo di accesso per l'utente host.

- **-nome utente**

Specifica il nome utente dell'host.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene illustrato il risultato del comando per sincronizzare le mappature da profilo a repository per il database.


```
smo profile sync -repository -dbname smrepo -host Host2 -port 1521 -login  
-username user2  
SMO-12345 [INFO ]: Loading profile mappings for repository  
"user2@Host2:smrepo" into cache for OS User "admin".  
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

Il comando di aggiornamento del profilo smo

È possibile eseguire il comando di aggiornamento del profilo per aggiornare le informazioni relative a un profilo esistente.

Sintassi

```

    smo profile update
-profile profile
\[-new-profile new_profile_name\]
\[-profile-password profile_password\]
[-database
-dbname db_dbname
-host db_host
\[-sid db_sid\]
[-login
\[-username db_username -password db_password -port db_port\]
 \[-asminstance -asmusername asminstance_username -asmpassword
asminstance_password\]]
\{\{-rman \{\-controlfile \| \{\{\{-login
-username rman_username
-password rman_password \}
\[-tnsname tnsname\}\}\}\} \|
-remove-rman\}
-osaccount osaccount
-osgroup osgroup
[-retain
\[-hourly \[-count n\] \[-duration m\]\]
\[-daily \[-count n\] \[-duration m\]\]
\[-weekly \[-count n\] \[-duration m\]\]
\[-monthly \[-count n\] \[-duration m\]\]\]
-comment comment
-snapname-patternpattern
[-protect \[-protection-policy policy_name\] \| \[-noprotect\]]
[-summary-notification]
[-notification
\[-success
-email email_address1,email_address2
-subject subject_pattern\]
\[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups
-retain-archivelog-backups
-hours hours |
-days days |
-weeks weeks |
-months months
[-protect \[-protection-policy policy_name\] \| \[-noprotect\]]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
\[-quiet \| -verbose\]

```

Parametri

Se il criterio di protezione è impostato sul profilo, non è possibile modificarlo utilizzando SnapManager. È necessario modificare il criterio utilizzando la console di Protection Manager.

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-profile-password profile_password**

Specifica la password per il profilo.

- **-new-profile new_profile_name**

Specifica il nuovo nome che è possibile fornire per un profilo.

- **-database**

Specifica i dettagli del database descritti dal profilo. Si tratta del database di cui verrà eseguito il backup, il ripristino e così via.

- **-dbname db_dbname**

Specifica il nome del database descritto dal profilo. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host db_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database.

- **-sid db_sid**

Specifica l'identificativo di sistema del database descritto dal profilo. Per impostazione predefinita, SnapManager utilizza il nome del database come identificatore di sistema. Se l'identificatore di sistema è diverso dal nome del database, è necessario specificarlo utilizzando l'opzione -sid.

Ad esempio, se si utilizzano i cluster di applicazioni reali Oracle, è necessario specificare l'identificativo di sistema SID dell'istanza RAC sul nodo RAC da cui viene eseguito SnapManager.

- **-login**

Specifica i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente richiesto per accedere al database del repository.

- **-port repo_port**

Specifica il numero di porta TCP richiesto per accedere al database del repository.

- **-database**

Specifica i dettagli del database descritti dal profilo. Si tratta del database di cui verrà eseguito il backup, il

ripristino o il cloning.

- **-dbname db_dbname**

Specifica il nome del database descritto dal profilo. È possibile utilizzare il nome globale o l'identificatore di sistema.

- **-host db_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database.

- **-login**

Specifica i dettagli di accesso al database.

- **-nome utente db_nome utente**

Specifica il nome utente richiesto per accedere al database descritto dal profilo.

- **-password db_password**

Specifica la password richiesta per accedere al database descritto dal profilo.

- **-port db_port**

Specifica il numero di porta TCP richiesto per accedere al database descritto dal profilo.

- **-preminenza**

Specifica le credenziali utilizzate per accedere all'istanza di Automatic Storage Management (ASM).

- **-asmusername asminstance_username**

Specifica il nome utente utilizzato per accedere all'istanza di ASM.

- **-asmpassword asminstance_password**

Specifica la password utilizzata per accedere all'istanza di ASM.

- **-rman**

Specifica i dettagli utilizzati da SnapManager per catalogare i backup con Oracle Recovery Manager (RMAN).

- **-controlfile**

Specifica i file di controllo del database di destinazione invece di un catalogo come repository RMAN.

- **-login**

Specifica i dettagli di accesso RMAN.

- **-password rman_password**

Specifica la password utilizzata per accedere al catalogo RMAN.

- **-username rman_username**

Specifica il nome utente utilizzato per accedere al catalogo RMAN.

- **-tnsname tnsname**

Specifica il nome di connessione tnsname (definito nel file tnsname.ora).

- **-remove-rman**

Specifica di rimuovere RMAN sul profilo.

- **-osaccount**

Specifica il nome dell'account utente del database Oracle. SnapManager utilizza questo account per eseguire le operazioni Oracle, ad esempio l'avvio e lo spegnimento. In genere, è l'utente che possiede il software Oracle sull'host, ad esempio oracle.

- **-ossgroup**

Specifica il nome del nome del gruppo di database Oracle associato all'account oracle.

- **-retain [-hourly [-countn] [-duration m]] [-giornaliero [-count n] [-duration m]] [-settimanale [-count n][duration m]] [-mensile [-count n][duration m]]**

Specifica la classe di conservazione (oraria, giornaliera, settimanale, mensile) per un backup.

Per ogni classe di conservazione, è possibile specificare un conteggio di conservazione o una durata di conservazione o entrambe. La durata è espressa in unità della classe (ad esempio, ore per ora o giorni per giorno). Ad esempio, se l'utente specifica solo una durata di conservazione di 7 per i backup giornalieri, SnapManager non limiterà il numero di backup giornalieri per il profilo (poiché il numero di conservazione è 0), ma SnapManager eliminerà automaticamente i backup giornalieri creati oltre 7 giorni fa.

- **-commento commento**

Specifica il commento per un profilo.

- **-snapname-pattern pattern**

Specifica il modello di denominazione per le copie Snapshot. È inoltre possibile includere testo personalizzato, ad esempio HAOPS per operazioni altamente disponibili, in tutti i nomi delle copie Snapshot. È possibile modificare il modello di denominazione della copia Snapshot quando si crea un profilo o dopo averlo creato. Il modello aggiornato si applica solo alle copie Snapshot che non si sono ancora verificate. Le copie Snapshot esistenti conservano il modello Snapname precedente. È possibile utilizzare diverse variabili nel testo del modello.

- **-protect [-protection-policypolicy_name] | [-noprotect]**

Indica se il backup deve essere protetto o meno nello storage secondario.



Se -Protect viene specificato senza -Protection-policy, il dataset non avrà una policy di protezione. Se viene specificato -Protect e -Protection-policy non viene impostato al momento della creazione del profilo, è possibile impostarlo successivamente tramite il comando di aggiornamento del profilo bysmo o impostarlo dall'amministratore dello storage utilizzando la console di Protection Manager .

L'opzione -noproduct specifica di non proteggere il profilo sullo storage secondario.

- **-summary-notification**

Specifica che la notifica email di riepilogo è attivata per il profilo esistente.

- **-notification [-success-email email email_address1,email address2 -subject subject_pattern]**

Attiva la notifica e-mail per il profilo esistente in modo che i destinatari ricevano i messaggi e-mail quando l'operazione SnapManager ha esito positivo. È necessario inserire un singolo indirizzo e-mail o più indirizzi e-mail a cui inviare gli avvisi e-mail e un modello di oggetto e-mail per il profilo esistente.

È possibile modificare il testo dell'oggetto durante l'aggiornamento del profilo o includere il testo dell'oggetto personalizzato. L'oggetto aggiornato si applica solo ai messaggi e-mail non inviati. È possibile utilizzare diverse variabili per l'oggetto dell'e-mail.

- **-notification [-failure -email email email_address1,email address2 -subject subject_pattern]**

Attiva la notifica e-mail per il profilo esistente in modo che i destinatari ricevano i messaggi e-mail quando l'operazione SnapManager non riesce. È necessario inserire un singolo indirizzo e-mail o più indirizzi e-mail a cui inviare gli avvisi e-mail e un modello di oggetto e-mail per il profilo esistente.

È possibile modificare il testo dell'oggetto durante l'aggiornamento del profilo o includere il testo dell'oggetto personalizzato. L'oggetto aggiornato si applica solo ai messaggi e-mail non inviati. È possibile utilizzare diverse variabili per l'oggetto dell'e-mail.

- **-storage-backup-separati**

Separa il backup del registro di archiviazione dal backup del file di dati. Si tratta di un parametro facoltativo che è possibile fornire durante la creazione del profilo. Dopo aver separato i backup utilizzando questa opzione, è possibile creare backup solo file di dati o backup solo log di archivio.

- **-retain-archiveog-backups -ore | -daysdays | -weekswweeks | -monthsmmonths**

Specifica che i backup del registro di archiviazione vengono conservati in base alla durata di conservazione del registro di archiviazione (oraria, giornaliera, settimanale, mensile).

- **-protect [-protection-policypolicy_name] | -noproduct**

Specifica che i file di log dell'archivio sono protetti in base al criterio di protezione del log dell'archivio.

Specifica che i file di log dell'archivio non sono protetti utilizzando l'opzione -noproduct.

- **-include-with-online-backups | -no-include-with-online-backups**

Specifica che il backup del registro di archiviazione è incluso insieme al backup del database online.

Specifica che i backup del registro di archiviazione non sono inclusi insieme al backup del database online.

- **-dump**

Specifica che i file dump vengono raccolti dopo l'operazione di creazione del profilo.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione

dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente vengono modificate le informazioni di accesso per il database descritto dal profilo e la notifica e-mail viene configurata per questo profilo:

```
smo profile update -profile SALES1 -database -dbname SALESDB  
-sid SALESDB -login -username admin2 -password d4jPe7bw -port 1521  
-host server1 -profile-notification -success -e-mail Preston.Davis@org.com  
-subject success  
Operation Id [8abc01ec0e78ec33010e78ec3b410001] succeeded.
```

Informazioni correlate

[Modifica delle password del profilo](#)

[In che modo SnapManager conserva i backup sullo storage locale](#)

Il comando di verifica del profilo smo

Per verificare la configurazione del profilo, eseguire il comando di verifica del profilo. È necessario montare il database prima di eseguire questo comando.

Sintassi

```
smo profile verify  
-profile profile_name  
\[ -quiet \| -verbose \]
```

Parametri

- **-profilo**

Specifica il profilo da verificare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Il seguente esempio verifica il profilo:

```
smo profile verify -profile test_profile -verbose
[ INFO] SMO-07431: Saving starting state of the database: racb1(OPEN).
[ INFO] SMO-07431: Saving starting state of the database: racb2(SHUTDOWN),
racb1(OPEN) .
[ INFO] SD-00019: Discovering storage resources for all system devices.
[ INFO] SD-00020: Finished storage discovery for all system devices.
[ INFO] SD-00019: Discovering storage resources for all system devices.
[ INFO] SD-00020: Finished storage discovery for all system devices.
[ INFO] SD-00019: Discovering storage resources for all system devices.
[ INFO] SD-00020: Finished storage discovery for all system devices.
[ INFO] SMO-05070: Database profile test_profile is eligible for fast
restore.
[ INFO] SMO-07433: Returning the database to its initial state:
racb2(SHUTDOWN), racb1(OPEN) .
[ INFO] SMO-13048: Profile Verify Operation Status: SUCCESS
[ INFO] SMO-13049: Elapsed Time: 0:04:14.919
Operation Id [Nffffde14ac88cd1a21597c37e8d21fe90] succeeded.
```

Informazioni correlate

[Verifica dei profili in corso](#)

Il comando Protection-policy smo

È possibile eseguire il comando Protection-policy per elencare i criteri di protezione che possono essere applicati a un profilo. Il criterio di protezione può essere applicato quando viene creato un nuovo profilo o aggiornato un profilo esistente. È inoltre possibile impostare il criterio di protezione per il profilo utilizzando la console di Protection Manager.

Sintassi

```
smo protection-policy list
```



Per utilizzare questo comando, è necessario che Gestione protezione e SnapDrive siano installati sul server.

Parametri

- **elenco**

Visualizza l'elenco dei criteri di protezione che è possibile impostare su un profilo.

Esempio

Nell'esempio seguente sono elencati i criteri di protezione che è possibile impostare su un profilo:

```
smo protection-policy list
```

```
Back up
Back up, then mirror
Chain of two mirrors
DR Back up
DR Back up, then mirror
DR Mirror
DR Mirror and back up
DR Mirror and mirror
DR Mirror, then back up
DR Mirror, then mirror
Local backups only
Mirror
Mirror and back up
Mirror to two destinations
Mirror, then back up
No protection
Partial-volume Mirror
Remote backups only
```

Informazioni correlate

[Gestione dei profili per backup efficienti](#)

Il comando di creazione del repository smo

Sintassi

Questo comando crea un repository in cui memorizzare i profili di database e le credenziali associate. Questo comando verifica inoltre che la dimensione del blocco sia adeguata.

```
smo repository create
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
\[-quiet \|-verbose\]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-force**

Tenta di forzare la creazione del repository. L'utilizzo di questa opzione comporta la richiesta di SnapManager di eseguire il backup del repository prima di creare il repository.

- **-noprompt**

Se si utilizza l'opzione -force, non viene visualizzato il prompt per eseguire il backup del repository prima della creazione. L'opzione -noprompt consente di evitare la visualizzazione del prompt, semplificando la creazione di repository utilizzando uno script.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene creato un repository nel database SMOREPO sull'host hotspur.

```
smo repository create -repository -port 1521 -dbname SMOREPO -host hotspur
-login -username grabal21 -verbose
SMO-09202 [INFO ]: Creating new schema as grabal21 on
jdbc:oracle:thin:@//hotspur:1521/SMOREPO.
SMO-09205 [INFO ]: Schema generation complete.
SMO-09209 [INFO ]: Performing repository version INSERT.
SMO-09210 [INFO ]: Repository created with version: 30
SMO-13037 [INFO ]: Successfully completed operation: Repository Create
SMO-13049 [INFO ]: Elapsed Time: 0:00:08.844
```

Il comando `smo repository delete`

Questo comando elimina un repository utilizzato per memorizzare i profili di database e le credenziali associate. È possibile eliminare un repository solo se non sono presenti profili nel repository.

Sintassi

```
smo repository delete
-repository
-port repo_port
-database repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-force**

Tenta di forzare l'eliminazione del repository, anche in caso di operazioni incomplete. In caso di operazioni incomplete, SnapManager visualizza un messaggio che chiede se si è sicuri di voler eliminare il repository.

- **-noprompt**

Non richiede prima di eliminare il repository. L'opzione -noprompt consente di evitare la visualizzazione del prompt, semplificando l'eliminazione dei repository mediante uno script.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene eliminato il repository nel database SALESDB.

```
smo repository delete -repository -port 1521 -dbname smorep
-host nila -login -username smofresno -force -verbose
This command will delete repository "smofresno@smorep/nila".
Any resources maintained by the repository must be cleaned up manually.
This may include snapshots, mounted backups, and clones.
Are you sure you wish to proceed (Y/N)?Y
[ INFO] SMO-09201: Dropping existing schema as smofresno
on jdbc:oracle:thin:@//nila:1521/smorep.
[ INFO] SMO-13048: Repository Delete Operation Status: SUCCESS
[ INFO] SMO-13049: Elapsed Time: 0:00:06.372
[ INFO] SMO-20010: Synchronizing mapping for profiles in
repository "smofresno@smorep/nila:1521".
[ WARN] SMO-20029: No repository schema exists in
"smofresno@smorep/nila:1521".
Deleting all profile mappings for this repository.
[ INFO] SMO-20012: Deleted stale mapping for profile "TESTPASS".
```

Il comando di rollback del repository smo

Questo comando consente di eseguire il rollback o il ripristino da una versione superiore di SnapManager alla versione originale da cui è stato eseguito l'aggiornamento.

Sintassi

```
smo repository rollback
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-rollbackhost host_with_target_database
[-force]
\[-quiet \|-verbose\]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-rollbackhost host host_with_target_database**

Specifica il nome dell'host che verrà eseguito il rollback da una versione superiore di SnapManager alla versione precedente originale.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-force**

Tenta di forzare l'aggiornamento del repository. SnapManager richiede di eseguire un backup del repository corrente prima dell'aggiornamento.

- **-noprompt**

Non visualizza la richiesta prima di aggiornare il database del repository. L'opzione -noprompt consente di evitare la visualizzazione del prompt, semplificando l'aggiornamento dei repository mediante uno script.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene aggiornato il repository nel database SALESDB.

```
smo repository rollback -repository -dbname SALESDB  
-host server1 -login -username admin -port 1521 -rollbackhost hostA
```

Il comando rolling upgrade del repository smo

Questo comando esegue l'aggiornamento in sequenza su uno o più host e sui database di destinazione associati da una versione inferiore di SnapManager a una versione superiore. L'host aggiornato viene gestito solo con la versione superiore di SnapManager.

Sintassi

```
smo repository rollingupgrade  
-repository  
-dbname repo_service_name  
-host repo_host  
-login -username repo_username  
-port repo_port  
-upgradehost host_with_target_database  
[-force] [-noprompt]  
\[ -quiet \| -verbose \]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-upgrade host host_with_target_database**

Specifica il nome dell'host che verrà aggiornato da una versione inferiore di SnapManager a una versione superiore.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-force**

Tenta di forzare l'aggiornamento del repository. SnapManager richiede di eseguire un backup del repository corrente prima dell'aggiornamento.

- **-noprompt**

Non visualizza la richiesta prima di aggiornare il database del repository. L'opzione -noprompt consente di evitare la visualizzazione del prompt, semplificando l'aggiornamento dei repository mediante uno script.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene aggiornato il repository nel database SALESDB.

```
smo repository rollingupgrade -repository -dbname SALESDB  
-host server1 -login -username admin -port 1521 -upgradehost hostA
```

Il comando show del repository smo

Questo comando visualizza le informazioni sul repository.

Sintassi

```
smo repository show
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
\[-quiet \|-verbose\]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-dbname repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio riportato di seguito vengono illustrati i dettagli relativi al repository nel database SALESDB.


```
smo repository show -repository -dbname SALESDB -host server1
-port 1521 -login -username admin
Repository Definition:
User Name: admin
Host Name: server1
Database Name: SALESDB
Database Port: 1521
Version: 28
Hosts that have run operations using this repository: 2
server2
server3
Profiles defined in this repository: 2
GSF5A
GSF3A
Incomplete Operations: 0
```

Il comando di aggiornamento del repository smo

Questo comando aggiorna il repository che memorizza i profili di database e le credenziali associate quando si aggiorna SnapManager. Ogni volta che si installa una nuova versione di SnapManager, è necessario eseguire il comando di aggiornamento del repository prima di poter utilizzare la nuova versione. È possibile utilizzare questo comando solo se nel repository non sono presenti comandi incompleti.

Sintassi

```
smo repository update
-repository
-database repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
[-force] [-noprompt]
\[-quiet \|-verbose\]
```

Parametri

- **-repository**

Le opzioni che seguono -repository specificano i dettagli del database per il repository.

- **-database repo_service_name**

Specifica il nome del database in cui è memorizzato il repository. Utilizzare il nome globale o il SID.

- **-host repo_host**

Specifica il nome o l'indirizzo IP del computer host su cui viene eseguito il database del repository.

- **-login**

Avvia i dettagli di accesso al repository.

- **-nome utente repo_nome utente**

Specifica il nome utente necessario per accedere al database in cui è memorizzato il repository.

- **-port repo_port**

Specifica il numero di porta TCP utilizzato per accedere al database in cui è memorizzato il repository.

- **-force**

Tenta di forzare l'aggiornamento del repository. SnapManager richiede di eseguire un backup del repository corrente prima dell'aggiornamento.

- **-noprompt**

Non visualizza la richiesta prima di aggiornare il database del repository. L'opzione -noprompt consente di evitare la visualizzazione del prompt, semplificando l'aggiornamento dei repository mediante uno script.

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio di comando

Nell'esempio seguente viene aggiornato il repository nel database SALESDB.

```
smo repository update -repository -dbname SALESDB  
-host server1 -login -username admin -port 1521
```

Il comando di creazione del programma smo

È possibile utilizzare il comando Schedule create per pianificare la creazione di un backup in un'ora specifica.

Sintassi

```

smo schedule create
-profile profile_name
\[-full\{-auto \| -online \| -offline\}
\[-retain -hourly \| -daily \| -weekly \| -monthly \| -unlimited\]
\[-verify\]\] |
\[-data \[\[-files files \[files\]\]\] \|
\[-tablespaces tablespaces \[tablespaces\]\]\] \{-auto \| -online \|
-offline\}
\[-retain -hourly \| -daily \| -weekly \| -monthly \| -unlimited\]
\[-verify\]\] |
\[-archivelogs\]}
\[-label label\]
\[-comment comment\]
\[-protect \| -noprotect \| -protectnow\]
\[-backup-dest path1 \[ , path2\]\]
\[-exclude-dest path1 \[ , path2\]\]
\[-prunelogs \{-all \| -until-scn until-scn \| -until -date yyyy-MM-
dd:HH:mm:ss\] \| -before \{-months \| -days \| -weeks \| -hours\}}
-prune-dest prune_dest1,\[prune_dest2\]\]
-schedule-name schedule_name
\[-schedule-comment schedule_comment\]
-interval \{-hourly \| -daily \| -weekly \| -monthly \| -onetimeonly\}
-cronstring cron_string
-start-time \{start_time <yyyy-MM-dd HH:mm\>\}
-runasuser runasuser
\[-taskspec taskspec\]
-force
\[-quiet \| -verbose\]

```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database per il quale si desidera pianificare il backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-opzione auto**

Se il database si trova nello stato montato o non in linea, SnapManager esegue un backup non in linea. Se il database si trova nello stato aperto o in linea, SnapManager esegue un backup in linea. Se si utilizza l'opzione -force con l'opzione -offline, SnapManager impone un backup offline anche se il database è attualmente in linea.

- **opzione -online**

Specifica un backup del database online.

È possibile creare un backup online di un database RAC (Real Application Clusters), purché il database

primario sia aperto o montato e un'istanza sia aperta. È possibile utilizzare l'opzione -force per i backup online se l'istanza locale si trova nello stato di shutdown o se non è aperta alcuna istanza.

- Se l'istanza locale si trova nello stato di shutdown e almeno un'istanza è aperta, è possibile utilizzare l'opzione -force per modificare l'istanza locale in montato.
- Se nessuna istanza è in stato aperto, è possibile utilizzare l'opzione -force per modificare l'istanza locale in modo che venga aperta.

- **-opzione offline**

Specifica un backup offline mentre il database si trova in stato di arresto. Se il database si trova nello stato aperto o montato, il backup non viene eseguito correttamente. Se si utilizza l'opzione -force, SnapManager tenta di modificare lo stato del database per arrestare il database per un backup offline.

- **-opzione completa**

Esegue il backup dell'intero database. Sono inclusi tutti i dati, il log archiviato e i file di controllo. Il backup dei log di ripristino e dei file di controllo archiviati viene eseguito indipendentemente dal tipo di backup eseguito. Se si desidera eseguire il backup solo di una parte del database, utilizzare l'opzione -Files o -tablespaces.

- **-elenco file**

Esegue il backup solo dei file di dati specificati e dei file di log e di controllo archiviati. Separare l'elenco dei nomi dei file con spazi. Se il database è in stato aperto, SnapManager verifica che gli spazi delle tabelle appropriati siano in modalità di backup online.

- **-tablespaces tablespaces**

Esegue il backup solo degli spazi delle tabelle del database specificati e dei file di log e di controllo archiviati. Separare i nomi di tablespace con gli spazi. Se il database è in stato aperto, SnapManager verifica che gli spazi delle tabelle appropriati siano in modalità di backup online.

- **-label name**

Specifica un nome opzionale per questo backup. Questo nome deve essere univoco all'interno del profilo. Il nome può contenere lettere, numeri, caratteri di sottolineatura (_) e trattini (-). Non può iniziare con un trattino.

Se non si specifica un'etichetta, SnapManager crea un'etichetta predefinita nel formato scope_type_date:

- L'ambito è F per indicare un backup completo o P per indicare un backup parziale.
- Digitare C per indicare un backup offline (cold), H per indicare un backup online (hot) o A per indicare un backup automatico, ad esempio P_A_20081010060037IST.
- Data indica l'anno, il mese, il giorno e l'ora del backup.

SnapManager utilizza un orologio a 24 ore.

Ad esempio, se è stato eseguito un backup completo con il database offline il 16 gennaio 2007, alle 17:45:16 Ora standard orientale, SnapManager crea l'etichetta F_C_20070116174516EST.

- **-comment string**

Specifica un commento facoltativo per descrivere questo backup. Racchiudere la stringa tra virgolette singole (').



Alcuni shell disegna le virgolette. Se questo è vero per la shell, è necessario includere la virgoletta con una barra rovesciata (.). Ad esempio, potrebbe essere necessario immettere:
`\' this is a comment\'`.

- **-opzione di verifica**

Verifica che i file nel backup non siano corrotti eseguendo l'utility Oracle dbv.



Se si specifica l'opzione -verify, l'operazione di backup non viene completata fino al completamento dell'operazione di verifica.

- **opzione -force**

Forza una modifica dello stato se il database non si trova nello stato corretto. Ad esempio, SnapManager potrebbe modificare lo stato del database da online a offline, in base al tipo di backup specificato e allo stato in cui si trova il database.

Con un backup online del database RAC, utilizzare l'opzione -force se l'istanza locale è in stato di shutdown o se non è aperta alcuna istanza.



La versione di Oracle deve essere 10.2.0.5; in caso contrario, il database si blocca se viene montata una qualsiasi istanza del RAC.

- Se l'istanza locale è in stato di arresto e almeno un'istanza è aperta, è possibile modificare l'istanza locale in montato utilizzando l'opzione -force.
- Se non è aperta alcuna istanza, è possibile modificare l'istanza locale per aprirla utilizzando l'opzione -force.

- **-protect | -noprotect | -protectnow**

Indica se il backup deve essere protetto sullo storage secondario. L'opzione -noprotect specifica che il backup non deve essere protetto sullo storage secondario. Sono protetti solo i backup completi. Se non viene specificata alcuna opzione, SnapManager protegge il backup come predefinito se si tratta di un backup completo e il profilo specifica un criterio di protezione. L'opzione -protectnow è disponibile solo per Data ONTAP in modalità 7. L'opzione specifica che il backup deve essere protetto immediatamente sullo storage secondario.

- **-retain { -orario | -giornaliero | -settimanale | -mensile | -illimitato }**

Specifica se il backup deve essere conservato su base oraria, giornaliera, settimanale, mensile o illimitata. Se l'opzione -retain non è specificata, il valore predefinito della classe retention è -hourly. Per conservare i backup per sempre, utilizza l'opzione -Unlimited. L'opzione -Unlimited rende il backup non idoneo per l'eliminazione in base al criterio di conservazione.

- **-archivelogs**

Specifica la creazione di un backup del log di archiviazione.

- **-backup-dest path1, [, [path2]]**

Specifica le destinazioni del registro di archiviazione per il backup del registro di archiviazione.

- **-exclude-dest path 1, [, [path2]]**

Specifica le destinazioni del registro di archiviazione da escludere dal backup.

- **-prunelogs {-all | -until-scn | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}}**

Specifica se eliminare i file di log dell'archivio dalle destinazioni del log dell'archivio in base alle opzioni fornite durante la creazione di un backup. L'opzione -all elimina tutti i file di log dell'archivio dalle destinazioni del log dell'archivio. L'opzione -until-scn elimina i file di registro dell'archivio fino a quando non viene specificato un numero SCN (System Change Number). L'opzione -until-date elimina i file di log dell'archivio fino al periodo di tempo specificato. L'opzione -before elimina i file di log dell'archivio prima del periodo di tempo specificato (giorni, mesi, settimane, ore).

- **-schedule-name nome_schedule**

Specifica il nome fornito per la pianificazione.

- **-schedule-comment schedule_comment**

Specifica un commento facoltativo da descrivere sulla pianificazione del backup.

- **-interval { -oraria | -giornaliera | -settimanale | -mensile | -onetimeonly}**

Specifica l'intervallo di tempo in base al quale vengono creati i backup. È possibile pianificare il backup su base oraria, giornaliera, settimanale, mensile o una sola volta.

- **-cron_string cron_string**

Specifica la pianificazione del backup mediante cronstring. Le espressioni cron vengono utilizzate per configurare le istanze di CronTrigger. Le espressioni cron sono stringhe composte dalle seguenti sottoespressioni:

- 1 si riferisce ai secondi.
- 2 indica i minuti.
- 3 si riferisce alle ore.
- 4 si riferisce a un giorno in un mese.
- 5 si riferisce al mese.
- 6 si riferisce a un giorno in una settimana.
- 7 si riferisce all'anno (facoltativo).

- **-start-time yyyy-MM-dd HH:mm**

Specifica l'ora di inizio dell'operazione pianificata. L'ora di inizio della pianificazione deve essere inclusa nel formato yyyy-MM-dd HH:mm.

- **-runasuser runasuser**

Specifica la modifica dell'utente (utente root o utente Oracle) dell'operazione di backup pianificata durante la pianificazione del backup.

- **-taskspec taskspec**

Specifica il file XML della specifica dell'attività che può essere utilizzato per l'attività di pre-elaborazione o di post-elaborazione dell'operazione di backup. Il percorso completo del file XML deve essere fornito con

l'opzione -taskspec.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Il comando **smo schedule delete**

Questo comando elimina una pianificazione di backup quando non è più necessaria.

Sintassi

```
smo schedule delete
-profile profile_name
-schedule-name schedule_name
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database che si desidera eliminare. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-schedule-name nome_schedule**

Specifica il nome della pianificazione fornito durante la creazione di una pianificazione di backup.

Il comando **smo schedule list**

Questo comando elenca le operazioni pianificate associate a un profilo.

Sintassi

```
smo schedule list
-profile profile_name
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database, utilizzando il quale è possibile visualizzare un elenco di

operazioni pianificate. Il profilo contiene l'identificatore del database e altre informazioni del database.

Il comando **smo schedule resume**

Questo comando ripristina la pianificazione del backup sospeso.

Sintassi

```
smo schedule resume
-profile profile_name
-schedule-name schedule_name
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database che si desidera ripristinare la pianificazione di backup sospesa. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-schedule-name nome_schedule**

Specifica il nome della pianificazione fornito durante la creazione di una pianificazione di backup.

Il comando **smo schedule Suspend**

Questo comando sospende una pianificazione di backup fino al ripristino della pianificazione di backup.

Sintassi

```
smo schedule suspend
-profile profile_name
-schedule-name schedule_name
\[-quiet \|-verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database che si desidera sospendere una pianificazione di backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-schedule-name nome_schedule**

Specifica il nome della pianificazione fornito durante la creazione di una pianificazione di backup.

Il comando smo schedule update

Questo comando aggiorna la pianificazione di un backup.

Sintassi

```
smo schedule update
-profile profile_name
-schedule-name schedule_name
\[-schedule-comment schedule_comment\]
-interval \{-hourly \| -daily \| -weekly \| -monthly \| -onetimeonly\}
-cronstring cron_string
-start-time \{start_time <yyyy-MM-dd HH:mm\>\}
-runasuser runasuser
\[-taskspec taskspec\]
-force
\[-quiet \| -verbose\]
```

Parametri

- **-profile_name**

Specifica il nome del profilo correlato al database che si desidera pianificare il backup. Il profilo contiene l'identificatore del database e altre informazioni del database.

- **-schedule-name nome_schedule**

Specifica il nome fornito per la pianificazione.

- **-schedule-comment schedule_comment**

Specifica un commento facoltativo da descrivere sulla pianificazione del backup.

- **-interval { -oraria | -giornaliera | -settimanale | -mensile | -onetimeonly }**

Indica l'intervallo di tempo entro il quale vengono creati i backup. È possibile pianificare il backup su un orario, giornaliero, settimanale, mensile o una sola volta.

- **-cron_string cron_string**

Specifica di pianificare il backup utilizzando cronstring. Le espressioni cron vengono utilizzate per configurare le istanze di CronTrigger. Le espressioni cron sono stringhe composte da sette sottoespressioni:

- 1 si riferisce ai secondi
- 2 indica i minuti
- 3 si riferisce alle ore
- 4 si riferisce a un giorno in un mese
- 5 si riferisce al mese

- 6 si riferisce a un giorno in una settimana
- 7 si riferisce all'anno (facoltativo)

- **-start-time yyyy-MM-dd HH:mm**

Specifica l'ora di inizio dell'operazione di pianificazione. L'ora di inizio della pianificazione deve essere inclusa nel formato yyyy-MM-dd HH:mm.

- **-runasuser runasuser**

Specifica di modificare l'utente dell'operazione di backup pianificata durante la pianificazione del backup.

- **-taskspec taskspec**

Specifica il file XML delle specifiche dell'attività che può essere utilizzato per l'attività di pre-elaborazione o di post-elaborazione dell'operazione di backup. Il percorso completo del file XML deve essere fornito con l'opzione -taskspec.

Il comando smo storage list

È possibile eseguire il comando Storage list per visualizzare l'elenco dei sistemi di storage associati a un particolare profilo.

Sintassi

```
smo storage list
-profile profile
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Il nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

Esempio

Nell'esempio seguente vengono visualizzati i sistemi di storage associati al profilo mjullian:

```
smo storage list -profile mjullian
```

```
Sample Output:
Storage Controllers
-----
FAS3020-RTP07OLD
```

Comando di ridenominazione dello storage smo

Questo comando aggiorna il nome o l'indirizzo IP del sistema di storage.

Sintassi

```
smo storage rename
-profile profile
-oldname old_storage_name
-newname new_storage_name
\[-quiet \|-verbose\]
```

Parametri

- **-profilo profilo**

Specifica il nome del profilo. Questo nome può contenere fino a 30 caratteri e deve essere univoco all'interno dell'host.

- **-oldname old_storage_name**

Specifica l'indirizzo IP o il nome del sistema di storage prima che venga rinominato. Immettere l'indirizzo IP o il nome del sistema di storage visualizzato quando si esegue il comando `smo storage list`.

- **-newname new_storage_name**

Specifica l'indirizzo IP o il nome del sistema di storage dopo che il sistema viene rinominato.

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio

Nell'esempio seguente viene utilizzato il comando `smo storage rename` per rinominare il sistema di storage:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Il comando di dump del sistema smo

È possibile eseguire il comando `dump` del sistema per creare un file JAR contenente informazioni diagnostiche sull'ambiente del server.

Sintassi

```
smo system dump  
\[ -quiet \| -verbose \]
```

Parametri

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi nella console.

Esempio del comando dump di sistema

Nell'esempio seguente viene utilizzato il comando di dump del sistema smo per creare un file JAR:

```
smo system dump  
Path:/userhomedirectory/.netapp/smo/3.3.0/smo_dump_hostname.jar
```

Il comando di verifica del sistema smo

Questo comando conferma che tutti i componenti dell'ambiente necessari per eseguire SnapManager sono impostati correttamente.

Sintassi

```
smo system verify  
\[ -quiet \| -verbose \]
```

Parametri

- **-quiet**

Visualizza solo i messaggi di errore sulla console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza messaggi di errore, di avviso e informativi sulla console.

Esempio del comando di verifica del sistema

Nell'esempio seguente viene utilizzato il comando di verifica del sistema smo.

```
smo system verify
SMO-13505 [INFO ]: Snapdrive verify passed.
SMO-13037 [INFO ]: Successfully completed operation: System Verify
SMO-13049 [INFO ]: Elapsed Time: 0:00:00.559
Operation Id [N4f4e910004b36cfecee74c710de02e44] succeeded.
```

Il comando smo version

È possibile eseguire il comando version per determinare la versione di SnapManager in esecuzione sull'host locale.

Sintassi

```
smo version
\[-quiet \|-verbose\]
```

Parametri

- **-quiet**

Visualizza solo i messaggi di errore nella console. L'impostazione predefinita prevede la visualizzazione dei messaggi di errore e di avviso.

- **-dettagliato**

Visualizza la data di creazione e il contenuto di ciascun profilo. Visualizza anche messaggi di errore, di avviso e informativi nella console.

Esempio del comando version

Nell'esempio seguente viene visualizzata la versione di SnapManager:

```
smo version
SnapManager for Oracle Version: 3.3.1
```

Risoluzione dei problemi di SnapManager

Sono disponibili informazioni su alcuni dei problemi più comuni che potrebbero verificarsi e su come risolverli.


La seguente tabella descrive i problemi più comuni e le possibili soluzioni:

Domanda basata sui problemi	Soluzione possibile
Il database di destinazione e il listener sono in esecuzione?	Eseguire il comando <code>lsnrctl status</code> . Assicurarsi che l'istanza del database sia registrata con il listener.
Lo storage è visibile?	Eseguire il comando <code>SnapDrive storage show -all</code> .
Lo storage è scrivibile?	Modificare un file nel punto di montaggio appena creato. Utilizzare il comando <code>touch filename</code> . Se il file viene creato, lo storage è scrivibile. È necessario assicurarsi che lo storage sia scrivibile dall'utente con cui viene eseguito SnapManager (ad esempio, come root su UNIX).
Il server SnapManager è in esecuzione?	<p>Eseguire <code>smo_server status</code> e provare ad avviare il server utilizzando il comando <code>smo_server start</code>.</p> <p>Prima di poter utilizzare l'interfaccia grafica utente (GUI) o l'interfaccia della riga di comando (CLI) per avviare i comandi SnapManager relativi ai profili, il server deve essere in esecuzione. È possibile creare o aggiornare repository senza avviare il server, ma per eseguire tutte le altre operazioni SnapManager, il server deve essere in esecuzione.</p> <p>Per avviare il server SnapManager, immettere il seguente comando: <code>smo_server start</code>.</p>
Tutti i componenti necessari per eseguire correttamente SnapManager sono configurati?	Eseguire il comando di verifica del sistema <code>smo</code> per verificare che SnapDrive sia impostato correttamente.
Si dispone della versione corretta di SnapManager?	Utilizzare il comando <code>smo version</code> per controllare la versione di SnapManager.
Hai esaminato i file di log di SnapManager per determinare se i messaggi di errore possono aiutare a isolare il problema?	<p>SnapManager registra tutte le voci di log in un unico set di file di log rotanti. I file di log si trovano in <code>/var/log/smo</code>.</p> <p>I file di log si trovano in <code>C: NetApp SnapManager for Oracle/logs</code>.</p> <p>Potrebbe inoltre essere utile esaminare i log nella seguente posizione:</p> <p><code>/usr_home/.netapp/smo/3.3.0/log/</code></p> <p>Ogni log delle operazioni viene scritto nel proprio file di log sotto forma di <code>smo_of_date_time.log</code>.</p>


Domanda basata sui problemi	Soluzione possibile
<p>Se i registri di archiviazione sono memorizzati in un sistema storage che non esegue Data ONTAP, li hai esclusi dalla considerazione per il backup con SnapManager?</p>	<p>Il file <code>smo.config</code> consente di escludere alcuni file di log dell'archivio. Per UNIX, i file si trovano nella seguente posizione: <code>/Opt/NetApp/smo/properties/smo.config</code></p> <p>Utilizzare il formato indicato nel file per escludere i registri dell'archivio locale. Per ulteriori informazioni, vedere l'argomento "Simpostazione delle proprietà di configurazione".</p> <p>È inoltre possibile escludere le destinazioni del registro di archiviazione durante la creazione di un backup dall'interfaccia utente di SnapManager. Per ulteriori informazioni, vedere l'argomento "creazione di backup del database".</p> <p>È inoltre possibile escludere le destinazioni del registro di archiviazione durante la creazione di un backup dalla GUI di SnapManager.</p>
<p>Se si utilizza SnapManager con database NFS, si dispone di una licenza FlexClone?</p>	<p>È necessaria una licenza FlexClone per sfruttare al meglio SnapManager con i database NFS. SnapManager utilizza la funzionalità FlexClone per eseguire queste attività:</p> <ul style="list-style-type: none"> • Montare i backup dei database NFS • Verificare i backup dei database NFS • Clonare i database NFS • Registrare i backup dei database NFS con RMAN (se si utilizza RMAN)
<p>Impossibile connettersi al repository?</p>	<p>Se la connessione a un repository non riesce, eseguire il comando <code>lsnrctl status</code> sul database del repository e controllare i nomi dei servizi attivi. Quando SnapManager si connette al database del repository, utilizza il nome del servizio del database. A seconda della configurazione del listener, potrebbe trattarsi del nome del servizio breve o del nome del servizio completo. Quando SnapManager si connette a un database per un backup, un ripristino o un'altra operazione, utilizza il nome host e il SID. Se il repository non viene inizializzato correttamente perché attualmente non è raggiungibile, viene visualizzato un messaggio di errore che chiede se si desidera rimuovere il repository. È possibile rimuovere il repository dalla vista corrente in modo da poter eseguire operazioni su altri repository.</p> <p>Inoltre, verificare se l'istanza del repository è in esecuzione eseguendo <code>ps -eaf</code></p>

Domanda basata sui problemi	Soluzione possibile
grepinstance - comando name.	Il sistema è in grado di risolvere il nome host?
Verificare che il nome host specificato si trovi su una subnet diversa. Se viene visualizzato un messaggio di errore che indica che SnapManager non è in grado di risolvere il nome host, aggiungere il nome host nel file host.aggiungere il nome host al file /etc/hosts: xxx.xxx.xxx.xxx indirizzo IP del nome host	SnapDrive è in esecuzione?
Controllare se il daemon SnapDrive è in esecuzione: -Snapdrived status Se il daemon non è in esecuzione, viene visualizzato un messaggio che indica la presenza di un errore di connessione.	Quali sistemi storage sono configurati per l'accesso con SnapDrive?
Eseguire il comando: -SnapDrive config list	In che modo è possibile migliorare le prestazioni dell'interfaccia grafica di SnapManager?

Domanda basata sui problemi	Soluzione possibile
<ul style="list-style-type: none"> Assicurarsi di disporre di credenziali utente valide per il repository, l'host del profilo e il profilo. Se la credenziale non è valida, cancellare le credenziali dell'utente per il repository, l'host del profilo e il profilo. Ripristinare le stesse credenziali utente impostate in precedenza per il repository, l'host del profilo e il profilo. Per ulteriori informazioni sulla nuova impostazione delle credenziali utente, vedere "Simpostazione delle credenziali dopo la cancellazione della cache delle credenziali". Chiudere i profili inutilizzati. Se il numero di profili aperti è maggiore, le prestazioni della GUI di SnapManager rallentano. Verificare che sia stato attivato l'opzione Apri all'avvio nella finestra Preferenze utente nel menu Amministratore, dalla GUI di SnapManager. Se questa opzione è attivata, il file di configurazione utente (user.config) disponibile in /root/.netapp/smo/3.3.0/gui/state viene visualizzato come openOnStartup=PROFILE. Poiché l'opzione Apri all'avvio è attivata, è necessario controllare i profili aperti di recente dalla GUI di SnapManager, utilizzando lastOpenProfiles nel file di configurazione utente (user.config): LastOpenProfiles=PROFILE1,PROFILE2,PROFILE3,... È possibile eliminare i nomi dei profili elencati e mantenere sempre aperto un numero minimo di profili. L'aggiornamento del profilo protetto richiede più tempo rispetto al profilo non protetto. Il profilo protetto viene aggiornato a un intervallo di tempo, in base al valore specificato nel parametro protectionStatusRefreshRate del file di configurazione utente (user.config). È possibile aumentare il valore dal valore predefinito (300 secondi) in modo che i profili protetti vengano aggiornati solo dopo un intervallo di tempo specificato. Prima di installare la nuova versione di SnapManager nell'ambiente basato su UNIX, eliminare le voci sul lato client di SnapManager disponibili nel seguente percorso: 	<p>L'aggiornamento dell'interfaccia grafica di SnapManager richiede più tempo quando vengono avviate e eseguite contemporaneamente più operazioni SnapManager in background. Quando si fa clic con il pulsante destro del mouse sul backup (che è già stato eliminato ma viene ancora visualizzato nella GUI di SnapManager), le opzioni di backup per tale backup non vengono attivate nella finestra Backup o clonazione.</p>

Domanda basata sui problemi	Soluzione possibile
<p>È necessario attendere l'aggiornamento della GUI di SnapManager, quindi verificare lo stato del backup.</p>	<p>Cosa fareste quando il database Oracle non è impostato in inglese?</p>
<p>Le operazioni di SnapManager potrebbero non riuscire se la lingua di un database Oracle non è impostata sull'inglese. Impostare la lingua del database Oracle sull'inglese:</p> <ol style="list-style-type: none"> 1. Aggiungere quanto segue sotto i commenti iniziali in <code>/etc/init.d/smo_server</code> <ul style="list-style-type: none"> ◦ <code>NLS_LANG=America_americana</code> ◦ Esportare <code>NLS_LANG</code> 2. Riavviare il server SnapManager utilizzando il seguente comando: <code>Riavvio smo_server</code> <div>  <p>Se gli script di accesso come <code>.bash_profile</code>, <code>.bashrc</code> e <code>.cshrc</code> per l'utente Oracle sono impostati su <code>NLS_LANG</code>, è necessario modificare lo script in modo da non sovrascrivere <code>NLS_LANG</code>.</p> </div>	<p>Cosa fare quando l'operazione di pianificazione del backup non riesce se il database del repository punta a più di un IP e ciascun IP ha un nome host diverso?</p>
<ol style="list-style-type: none"> 1. Arrestare il server SnapManager. 2. Eliminare i file di pianificazione nella directory del repository dagli host in cui si desidera attivare la pianificazione del backup. <p>I nomi dei file di pianificazione possono essere nei seguenti formati:</p> <ul style="list-style-type: none"> ◦ repository nome database repository host repo porta ◦ Repository-repo_username_database_name-repository_host-repo_port Nota: è necessario assicurarsi di eliminare il file di pianificazione nel formato che corrisponde ai dettagli del repository. <ol style="list-style-type: none"> 3. Riavviare il server SnapManager. 4. Aprire altri profili nello stesso repository dall'interfaccia grafica di SnapManager per assicurarsi di non perdere alcuna informazione di pianificazione di tali profili. 	<p>Cosa fare quando l'operazione SnapManager non riesce e si verifica un errore di blocco del file delle credenziali?</p>

Domanda basata sui problemi	Soluzione possibile
<p>SnapManager blocca il file delle credenziali prima dell'aggiornamento e lo sblocca dopo l'aggiornamento. quando più operazioni vengono eseguite contemporaneamente, una delle operazioni potrebbe bloccare il file delle credenziali per aggiornarlo. Se un'altra operazione tenta di accedere contemporaneamente al file di credenziale bloccato, l'operazione non riesce e viene visualizzato un errore di blocco del file.</p> <p>Configurare i seguenti parametri nel file smo.config in base alla frequenza delle operazioni simultanee:</p> <ul style="list-style-type: none"> • FileLock.RetryInterval = 100 millisecondi • FileLock.timeout = 5000 millisecondi <div data-bbox="167 730 224 783"></div> <div data-bbox="282 724 747 789">I valori assegnati ai parametri devono essere espressi in millisecondi.</div>	<p>Cosa fare quando lo stato intermedio dell'operazione di verifica del backup viene visualizzato come non riuscito nella scheda Monitor anche se l'operazione di verifica del backup è ancora in esecuzione?</p>
<p>Il messaggio di errore viene registrato nel file sm_gui.log. Per determinare i nuovi valori dei parametri Operation.heartbeatInterval e Operation.heartbeatThreshold, consultare il file di log per risolvere il problema.</p> <ol style="list-style-type: none"> 1. Aggiungere i seguenti parametri nel file smo.config: <ul style="list-style-type: none"> ◦ Operation.heartbeatInterval = 5000 ◦ Operation.heartbeatThreshold = 5000 il valore predefinito assegnato da SnapManager è 5000. 2. Assegnare i nuovi valori a questi parametri. <div data-bbox="215 1409 272 1461"></div> <div data-bbox="329 1381 698 1482">I valori assegnati ai parametri devono essere espressi in millisecondi.</div> <ol style="list-style-type: none"> 3. Riavviare il server SnapManager ed eseguire nuovamente l'operazione. 	<p>Cosa fare quando si verifica un problema di spazio heap?</p>

Domanda basata sui problemi	Soluzione possibile
<p>Quando si verifica un problema di spazio heap durante le operazioni di SnapManager per Oracle, è necessario eseguire le seguenti operazioni:</p> <ol style="list-style-type: none"> 1. Accedere alla directory di installazione di SnapManager per Oracle. 2. Aprire il file launchjava dal percorso installationdirectory/bin/launchjava. 3. Aumentare il valore del parametro java -Xmx160m heap-space. <p>Ad esempio, è possibile aumentare il valore predefinito da 160 m a 200 m.</p> <div data-bbox="212 726 269 783">  </div> <p>Se nelle versioni precedenti di SnapManager per Oracle è stato aumentato il valore del parametro Java heap-space, è necessario conservare tale valore.</p>	<p>Cosa fare se non si possono utilizzare i backup protetti per il ripristino o la clonazione?</p>
<p>Questo problema si verifica se si utilizza SnapManager 3.3.1 con Clustered Data ONTAP e si è eseguito l'aggiornamento a SnapManager 3.4. I backup sono stati protetti mediante post-script in SnapManager 3.3.1. A partire da SnapManager 3.4, i backup vengono protetti utilizzando i criteri <i>SnapManager_cDOT_Mirror</i> o <i>SnapManager_cDOT_Vault</i> selezionati durante la creazione di un profilo. dopo l'aggiornamento a SnapManager 3.4, è possibile che si stiano ancora utilizzando i profili precedenti e che i backup siano protetti mediante script di backup. Tuttavia, non è possibile utilizzarli per il ripristino o la clonazione utilizzando SnapManager.</p> <p>Aggiornare il profilo e selezionare la policy <i>SnapManager_cDOT_Mirror</i> o <i>SnapManager_cDOT_Vault</i> ed eliminare il post-script utilizzato per la protezione dei dati in SnapManager 3.3.1.</p>	<p>Cosa fare se i backup pianificati non vengono protetti (SnapVault)?</p>

Eseguire il dump dei file

I file dump sono file di log compressi contenenti informazioni su SnapManager e sul suo ambiente. I diversi tipi di file di log creati sono operazione, profilo e file di dump di sistema.

È possibile utilizzare il comando dump o la scheda **Create Diagnostics** nell'interfaccia grafica utente (GUI) per

raccogliere informazioni su un'operazione, un profilo o l'ambiente. Un dump di sistema non richiede un profilo; tuttavia, i dump del profilo e delle operazioni richiedono profili.

SnapManager include le seguenti informazioni diagnostiche nel file dump:

- Le fasi eseguite
- Il tempo necessario per completare ogni fase
- Il risultato di ciascuna fase
- Se presente, si è verificato un errore durante l'operazione



I file di log o i file dump di SnapManager consentono di ottenere permessi di lettura e scrittura solo per gli utenti root e per gli altri utenti appartenenti al gruppo root.

SnapManager include anche le seguenti informazioni nel file:

- Versione e architettura del sistema operativo
- Variabili di ambiente
- Versione Java
- Versione e architettura di SnapManager
- Preferenze SnapManager
- Messaggi SnapManager
- proprietà log4j
- Versione e architettura di SnapDrive
- File di log di SnapDrive
- Versione di Oracle
- Dettagli dell'inventario locale di Oracle OPatch
- Dettagli dell'inventario locale OPatch dell'istanza di Automatic Storage Management (ASM)
- Versione del sistema storage
- File Oracle oratab
- Stato del listener Oracle
- File di configurazione di rete Oracle (listener.ora e tnsnames.ora)
- Versione Oracle del database repository
- Tipo di database di destinazione (stand aloneo Real Application Clusters (RAC))
- Ruolo del database di destinazione (primario, standby fisico o standby logico)
- Configurazione del database di destinazione Oracle Recovery Manager (RMAN) (nessuna integrazione RMAN, RMAN con file di controllo o RMAN con file di catalogo)
- Versione dell'istanza ASM del database di destinazione
- Versione Oracle del database di destinazione
- Identificatore di sistema (SID) del database di destinazione
- Nome del database RMAN e nome della connessione TNS
- Nome del servizio del database di repository

- Istanze di database installate sull'host
- Descrittore del profilo
- Memoria condivisa massima
- Scambiare le informazioni sullo spazio
- Informazioni sulla memoria
- Versione del kernel
- FSTAB
- Protocollo utilizzato da SnapDrive
- Ambiente multipath
- RAC
- Volume manager supportato
- Versione di Operations Manager
- File system supportato
- Versione delle utility host
- Output del comando di verifica del sistema
- Output del comando `sdconfcheck`

I file dump di SnapManager contengono anche il file di raccolta dati di SnapDrive e il file di log degli avvisi di Oracle. È possibile raccogliere il file di log degli avvisi Oracle utilizzando i comandi di dump dell'operazione smo e di dump del profilo smo.



Il dump del sistema non contiene i log degli avvisi Oracle; tuttavia, i dump del profilo e delle operazioni contengono i log degli avvisi.

Anche se il server host SnapManager non è in esecuzione, è possibile accedere alle informazioni di dump utilizzando l'interfaccia della riga di comando (CLI) o la GUI.

Se riscontri un problema che non puoi risolvere, puoi inviare questi file ai NetApp Global Services.

Creazione di file dump a livello operativo

È possibile utilizzare il comando `dump dell'operazione smo` con il nome o l'ID dell'operazione non riuscita per ottenere informazioni di registro su una determinata operazione. È possibile specificare diversi livelli di log per raccogliere informazioni su un'operazione, un profilo, un host o un ambiente specifico.

1. Immettere il seguente comando: `operazione smo dump -idguid`



Il comando `dump dell'operazione smo` fornisce un super set delle informazioni fornite dal comando `dump del profilo smo`, che a sua volta fornisce un super set delle informazioni fornite dal comando `dump del sistema smo`.

Posizione del file di dump:

```
Path: /<user-home>  
/.netapp/smo/3.3.0/smo_dump_8abc01c814649ebd0114649ec69d0001.jar
```

Creazione di file dump a livello di profilo

È possibile trovare le informazioni di log relative a un particolare profilo utilizzando il comando `smo profile dump` con il nome del profilo.

1. Immettere il seguente comando: `smo profile dump -profile_name`

Posizione del file di dump:

```
Path: /<user-home>  
/.netapp/smo/3.3.0/smo_dump_8abc01c814649ebd0114649ec69d0001.jar
```



Se si verifica un errore durante la creazione di un profilo, utilizzare il comando `smosystem dump`. Una volta creato un profilo, utilizzare i comandi `smooperation dump` e `smoprofile dump`.

Creazione di file dump a livello di sistema

È possibile utilizzare il comando di dump del sistema `smo` per ottenere informazioni di log sull'host e sull'ambiente SnapManager. È possibile specificare diversi livelli di log per raccogliere informazioni su un'operazione, un profilo o un host e un ambiente specifici.

1. Immettere il seguente comando: `System dump smo`

Dump risultante

```
Path: /<user-home>/ .netapp/smo/3.3.0/smo_dump_server_host.jar
```

Come individuare i file dump

Il file dump si trova nel sistema client per un facile accesso. Questi file sono utili per risolvere un problema relativo al profilo, al sistema o a qualsiasi operazione.

Il file dump si trova nella home directory dell'utente sul sistema client.

- Se si utilizza l'interfaccia grafica utente (GUI), il file dump si trova in:

```
user_home/Application Data/NetApp/smo/3.3.0/smo_dump dump_file_type_name  
server_host.jar
```

- Se si utilizza l'interfaccia della riga di comando (CLI), il file dump si trova in:

```
user_home/.netapp/smo/3.3.0/smo_dump_dump_file_type_name server_host.jar
```

Il file dump contiene l'output del comando dump. Il nome del file dipende dalle informazioni fornite. La tabella seguente mostra i tipi di operazioni di dump e i nomi dei file risultanti:

Tipo di operazione di dump	Nome file risultante
Comando dump dell'operazione con ID dell'operazione	smo_dump_operation-id.jar
Comando dump dell'operazione senza ID operazione	<p>Operazione smo dump -profile VH1-verbose viene visualizzato il seguente output:</p> <pre>smo operation dump -profile VH1 -verbose [INFO] SMO-13048: Dump Operation Status: SUCCESS [INFO] SMO-13049: Elapsed Time: 0:00:01.404 Dump file created. Path: /oracle/VH1/<path>/smo/3.3.0/smo_d ump_VH1_kaw.rtp.foo.com.jar</pre>
Comando dump del sistema	smo_dump_host-name.jar
Comando di dump del profilo	smo_dump_profile-name_host-name.jar

Come raccogliere i file dump

È possibile includere -dump nel comando SnapManager per raccogliere i file dump dopo un'operazione SnapManager riuscita o non riuscita.

È possibile raccogliere i file dump per le seguenti operazioni SnapManager:

- Creazione di profili
- Aggiornamento dei profili
- Creazione di backup
- Verifica dei backup
- Eliminazione dei backup
- Liberare i backup

- Montaggio dei backup
- Smontare i backup
- Ripristino dei backup
- Creazione di cloni
- Eliminazione dei cloni
- Suddivisione dei cloni



Quando si crea un profilo, è possibile raccogliere i file dump solo se l'operazione ha esito positivo. Se si verifica un errore durante la creazione di un profilo, è necessario utilizzare il comando `smosystem dump`. Per i profili di successo, è possibile utilizzare i comandi `dump di smooperation` e `dump di smoprofile` per raccogliere i file dump.

Esempio

```
smo backup create -profile targetdb1_prof1 -auto -full -online
-dump
```

Raccolta di informazioni aggiuntive sui log per semplificare il debugging

Se sono necessari log aggiuntivi per eseguire il debug di un'operazione SnapManager non riuscita, è necessario impostare una variabile di ambiente esterna `server.log.level`. Questa variabile sovrascrive il livello di log predefinito e scarica tutti i messaggi di log nel file di log. Ad esempio, è possibile modificare il livello di log in `DEBUG`, che registra messaggi aggiuntivi e può aiutare a risolvere i problemi di debug.

I registri SnapManager sono disponibili nelle seguenti posizioni:

- `/var/log/smo`

Per eseguire l'override del livello di registro predefinito, attenersi alla seguente procedura:

1. Creare un file di testo `platform.override` nella directory di installazione di SnapManager.
2. Aggiungere il parametro `server.log.level` nel file di testo `platform.override`.
3. Assegnare un valore (`TRACCIA`, `DEBUG`, `INFO`, `AVVISO`, `ERRORE`, `FATAL`, o `PROGRESS`) al parametro `server.log.level`.

Ad esempio, per impostare IL livello di log SU `ERROR`, impostare il valore `server.log.level` su `ERROR`.

```
Server.log.level=ERROR
```

4. Riavviare il server SnapManager.



Se le informazioni aggiuntive del registro non sono richieste, è possibile eliminare il parametro `server.log.level` dal file di testo `platform.override`.

SnapManager gestisce il volume dei file di log del server in base ai valori definiti dall'utente dei seguenti parametri nel file `smo.config`:

- log.max_log_files
- log.max_log_file_size
- log.max_rolling_operation_factory_logs

Risoluzione dei problemi relativi ai cloni

Sono disponibili informazioni su ciò che potrebbe verificarsi durante le operazioni di clonazione e su come risolverle.

Sintomo	Spiegazione	Soluzione alternativa
L'operazione di clonazione non riesce quando la destinazione dell'archivio è impostata su USE_DB_RECOVERY_FILE_DEST.	Quando la destinazione dell'archivio fa riferimento a USE_DB_RECOVERY_FILE_DEST, l'area di ripristino flash (fra) gestisce attivamente il registro dell'archivio. SnapManager non utilizza la posizione fra durante le operazioni di cloning o ripristino, pertanto le operazioni non vengono eseguite correttamente.	Impostare la destinazione dell'archivio sulla posizione del registro di archiviazione corrente invece della posizione fra.

Sintomo	Spiegazione	Soluzione alternativa
L'operazione di clonazione non riesce e viene visualizzato il seguente messaggio di errore: Impossibile eseguire l'operazione: Creazione clone. Causa principale: ORACLE-00001: Errore durante l'esecuzione di SQL: [ALTER DATABASE OPEN RESETLOGS;]. Il comando ha restituito: ORA-01195: Il backup online del file 1 necessita di maggiore recovery per essere coerente.	Questo problema si verifica se Oracle listener non riesce a connettersi al database.	<p>Se si utilizza l'interfaccia grafica di SnapManager per clonare un backup, eseguire le seguenti operazioni:</p> <ol style="list-style-type: none"> 1. Dalla struttura ad albero del repository, fare clic su Repository > host > Profilo per visualizzare i backup. 2. Fare clic con il pulsante destro del mouse sul backup che si desidera clonare e selezionare Clone. 3. Nella pagina Clone Initialization (Inizializzazione clone), immettere i valori obbligatori e selezionare il metodo di specifica clone. 4. Nella pagina Clone Specification (specifica clone), selezionare Parameters (parametri). 5. Fare clic sulla scheda +parametro. 6. Nel campo Nome parametro, immettere il nome come local_listener e fare clic su OK. 7. Selezionare la casella di controllo Override Default per la riga local_listener. 8. Fare clic su un parametro qualsiasi, quindi fare doppio clic sul parametro local_listener e immettere il seguente valore: (ADDRESS=(PROTOCOL=TCP)(HOST=<your_host_name>)(PORT=<port#>)) 9. Fare clic su Save to file (Salva su file). 10. Fare clic su Avanti e continuare con la creazione guidata dei cloni. <p>Se si utilizza l'interfaccia CLI per clonare un backup, è necessario includere le seguenti informazioni nel tag <parameters> del file di specifica del clone:</p>


Sintomo	Spiegazione	Soluzione alternativa
L'operazione di clonazione non riesce e viene visualizzato un messaggio di errore che indica che il punto di montaggio in uso è già in uso.	SnapManager non consente di montare un clone su un punto di montaggio esistente. Quindi, un clone incompleto non ha rimosso il punto di montaggio.	Specificare un punto di montaggio diverso da utilizzare per il clone o rimuovere il punto di montaggio problematico.
L'operazione di clonazione non riesce e viene visualizzato un messaggio di errore relativo ai file di dati che non hanno un'estensione .dbf.	Alcune versioni dell'utility Oracle NID non funzionano con i file di dati a meno che non utilizzino un'estensione .dbf.	<ul style="list-style-type: none"> • Rinominare il file di dati in modo da ottenere un'estensione .dbf. • Ripetere l'operazione di backup. • Clonare il nuovo backup.
L'operazione di clonazione non riesce a causa di requisiti non soddisfatti.	Si sta tentando di creare un clone; tuttavia, alcuni prerequisiti non sono stati soddisfatti.	Procedere come descritto in <i>creazione di un clone</i> per soddisfare i prerequisiti.
SnapManager non riesce a generare un nuovo profilo dopo l'operazione di suddivisione del clone e l'utente non sa se il nuovo profilo è stato creato.	SnapManager non visualizza alcun messaggio se non viene creato un nuovo profilo dopo l'operazione di suddivisione del clone. Poiché la richiesta non viene visualizzata, si potrebbe supporre che il profilo sia stato creato.	Dall'interfaccia della riga di comando (CLI) di SnapManager, immettere il comando clone split-risultato per visualizzare il risultato dettagliato dell'operazione di split del clone.
SnapManager per Oracle non riesce a clonare i database fisici di standby Oracle Data Guard 10gR2 (10.2.0.5).	SnapManager per Oracle non disattiva la modalità di ripristino gestito durante l'esecuzione di un backup offline dei database fisici di standby Oracle 10gR2 (10.2.0.5) creati utilizzando i servizi di Oracle Data Guard. A causa di questo problema, il backup offline eseguito non è coerente. Quando SnapManager per Oracle tenta di clonare il backup offline, non tenta nemmeno di eseguire alcun ripristino sul database clonato. Poiché il backup non è coerente, il database clonato richiede il ripristino e quindi Oracle non riesce a creare il clone correttamente.	Aggiornare il database Oracle a Oracle 11gR1 (patch 11.1.0.7).

Sintomo	Spiegazione	Soluzione alternativa
La clonazione di un backup su un host remoto non riesce e viene visualizzato il seguente messaggio di errore errore: Accesso negato.	Durante il montaggio, se l'indirizzo IP dell'host viene fornito al comando snap-mount, l'operazione di cloning potrebbe non riuscire. Questo problema si verifica se l'host su cui risiede il database si trova nel gruppo di lavoro mentre l'host remoto si trova nel dominio o viceversa.	Assicurarsi che l'host remoto e l'host su cui risiede il database si trovino nel dominio e non nel gruppo di lavoro.

Risoluzione dei problemi relativi all'interfaccia utente grafica

Sono disponibili informazioni su alcuni problemi comuni noti relativi all'interfaccia grafica utente (GUI) che potrebbero essere utili per risolverli.

Problema	Spiegazione	Soluzione alternativa
Durante l'accesso alla GUI di SnapManager per eseguire un'operazione, potrebbe essere visualizzato il seguente messaggio di errore: SMO-20111: Autenticazione non riuscita per l'utente sull'host.	Questo problema si verifica se la password dell'utente viene modificata nell'host su cui è in esecuzione il server SnapManager. dopo la modifica della password, la cache delle credenziali creata per l'utente che ha avviato la GUI non diventa valida. L'interfaccia utente grafica di SnapManager utilizza ancora le credenziali nella cache per l'autenticazione e l'autenticazione non riesce.	È necessario eseguire una delle seguenti operazioni: <ul style="list-style-type: none"> • Eliminare le credenziali dell'utente la cui password è stata modificata, quindi aggiungere le nuove credenziali nella cache eseguendo i seguenti comandi: <ol style="list-style-type: none"> a. eliminazione delle credenziali smo b. set di credenziali smo • Cancellare l'intera cache eseguendo il comando smo credential clear. Aprire nuovamente la GUI e impostare le credenziali, se richiesto.
Viene visualizzato un avviso di sicurezza durante l'utilizzo di Avvio Web Java per accedere all'interfaccia grafica di SnapManager.	Durante l'accesso all'interfaccia grafica di SnapManager tramite Java Web Start, viene visualizzato un avviso di sicurezza. Questo problema si verifica perché le jar JNLP sono autofirmati e la versione Java utilizzata da SnapManager non consente l'uso di jar autofirmati a un livello di sicurezza elevato.	Modificare le impostazioni di sicurezza su supporto nel pannello di controllo java o aggiungere l'URL della GUI SnapManager all'elenco delle eccezioni.

Problema	Spiegazione	Soluzione alternativa
La GUI di avvio Web di SnapManager visualizza la versione non corretta.	Dopo aver eseguito il downgrade di SnapManager da una versione successiva a una versione precedente quando si avvia l'interfaccia grafica per l'avvio dal Web, viene avviata la versione successiva dell'interfaccia grafica per l'avvio dal Web di SnapManager.	<p>È inoltre necessario cancellare la cache eseguendo le seguenti operazioni:</p> <ol style="list-style-type: none"> 1. Avviare la console. 2. Immettere quanto segue: Javaws -Viewer 3. Nella schermata Java cache Viewer, fare clic con il pulsante destro del mouse sull'applicazione SnapManager e selezionare Elimina.
Quando si riavvia la GUI e si tenta di controllare i backup per un determinato profilo, vengono visualizzati solo i nomi dei profili.	SnapManager non visualizza alcuna informazione su un profilo finché non viene aperto.	<p>Attenersi alla seguente procedura:</p> <ol style="list-style-type: none"> 1. Fare clic con il pulsante destro del mouse sul profilo e selezionare Apri dal menu. <p>SnapManager visualizza la finestra di dialogo autenticazione del profilo.</p> <ol style="list-style-type: none"> 2. Immettere il nome utente e la password dell'host. <p>SnapManager visualizza l'elenco di backup.</p> <div>  <p>È necessario autenticare il profilo una sola volta, purché le credenziali siano valide e rimangano nella cache.</p> </div>
Quando si apre il primo repository nella GUI, viene visualizzato un messaggio di errore simile al seguente: Il nome del profilo XXXX si scontra con il repository caricato in precedenza.	I profili con nome identico non possono esistere in un repository. Inoltre, è possibile aprire un solo repository alla volta.	Fare riferimento ai profili in conflitto di due diversi utenti del sistema operativo (OS) o rinominare il profilo eseguendo un'istruzione SQL per il repository: UPDATE SMO_33_PROFILE SET NAME = 'NEW_NAME' DOVE NAME = 'OLD_NAME'

Problema	Spiegazione	Soluzione alternativa
Viene visualizzato un messaggio di errore simile al seguente: SMO-01092: Impossibile inizializzare il repository repo1@ non esiste:repo1SMO-11006: Impossibile risolvere l'host non esiste	Il repository non è accessibile, forse perché non esiste più. La GUI inizializza l'elenco dei repository dal file delle credenziali.	Il messaggio di errore chiede se si desidera rimuovere questo repository in modo da non tentare di caricarlo in futuro. Se non è necessario accedere a questo repository, fare clic su Delete (Elimina) per rimuoverlo dalla vista GUI. In questo modo si rimuove il riferimento al repository nel file delle credenziali e la GUI non tenta di caricare nuovamente il repository.
La creazione del profilo non riesce perché le credenziali host non vengono autenticate nelle piattaforme SUSE Linux Enterprise Server 10 e SUSE Linux Enterprise Server 11.	SnapManager utilizza il modulo di autenticazione PAM (Pluggable Authentication Module) per autenticare gli utenti. Nelle piattaforme SUSE Linux Enterprise Server versione 10 e 11, per impostazione predefinita, nella directory /etc/pam.d non è presente alcun file SnapManager che fornisca i dettagli di autenticazione richiesti. In questo modo, le credenziali dell'host non vengono utilizzate.	<p>Per accedere correttamente all'host nelle piattaforme SUSE Linux Enterprise Server 10 e 11, attenersi alla seguente procedura:</p> <ol style="list-style-type: none"> 1. Creare un file SnapManager in /etc/pam.d/. 2. Aggiungere il seguente contenuto al file SnapManager che si trova in /etc/pam.d/snapmanager: <div data-bbox="1107 1037 1487 1461" data-label="Text"> <pre>#%PAM-1.0 auth include common-auth account include common-account password include common-password session include common-session</pre> </div> 3. Salvare il file e riprovare l'operazione di creazione del profilo.

Problema	Spiegazione	Soluzione alternativa
SnapManager impiega più tempo per caricare la struttura ad albero del database e genera un messaggio di errore di timeout visualizzato nell'interfaccia grafica di SnapManager.	Quando si tenta di eseguire un'operazione di backup parziale dall'interfaccia grafica di SnapManager, SnapManager tenta di caricare le credenziali per tutti i profili e, se sono presenti voci non valide, SnapManager tenta di convalidare la voce e viene visualizzato un messaggio di errore di timeout.	Eliminare le credenziali dell'host, del repository e del profilo inutilizzati utilizzando il comando di eliminazione delle credenziali dall'interfaccia della riga di comando (CLI) di SnapManager.
SnapManager non riesce a generare un nuovo profilo dopo l'operazione di suddivisione del clone e non si sa se il nuovo profilo viene creato.	SnapManager non visualizza alcun messaggio se non viene creato un nuovo profilo dopo l'operazione di suddivisione del clone. Poiché non viene visualizzato alcun messaggio per l'operazione non riuscita, si potrebbe supporre che il profilo sia stato creato.	Per sapere se viene creato un nuovo profilo per l'operazione di suddivisione del clone, attenersi alla seguente procedura: <ol style="list-style-type: none"> 1. Fare clic sulla scheda Monitor, fare clic con il pulsante destro del mouse sulla voce clone split operation e selezionare Proprietà. 2. Nella finestra Profile Properties (Proprietà profilo), fare clic sulla scheda Logs (registri) per visualizzare i registri delle operazioni di divisione e di creazione dei profili.
Gli script personalizzati per l'attività di pre-elaborazione o post-elaborazione che si verificano prima o dopo le operazioni di backup, ripristino o clonazione non sono visibili dalla GUI di SnapManager.	Quando si aggiungono script personalizzati nella posizione dello script personalizzato di backup, ripristino o clonazione dopo l'avvio della relativa procedura guidata, gli script personalizzati non vengono visualizzati nell'elenco Available Scripts (script disponibili).	Riavviare il server host SnapManager, quindi aprire l'interfaccia grafica di SnapManager.
Non è possibile utilizzare il file XML delle specifiche dei cloni creato in SnapManager (3.1 o versioni precedenti) per l'operazione di cloni.	A partire da SnapManager 3.2 per Oracle, la sezione relativa alle specifiche delle attività (specifiche delle attività) viene fornita come file XML separato per le specifiche delle attività.	Se si utilizza SnapManager 3.2 per Oracle, è necessario rimuovere la sezione delle specifiche delle attività dal file XML delle specifiche dei cloni o creare un nuovo file XML delle specifiche dei cloni. SnapManager 3.3 o versione successiva non supporta il file XML delle specifiche dei cloni creato in SnapManager 3.2 o versioni precedenti.

Problema	Spiegazione	Soluzione alternativa
L'operazione SnapManager sulla GUI non viene eseguita dopo aver cancellato le credenziali utente utilizzando il comando smo credential clear dalla CLI di SnapManager o facendo clic su Admin > credenziali > Cancella > cache dalla GUI di SnapManager.	Le credenziali impostate per repository, host e profili vengono cancellate. SnapManager verifica le credenziali dell'utente prima di avviare qualsiasi operazione. quando le credenziali dell'utente non sono valide, SnapManager non esegue l'autenticazione. Quando un host o un profilo viene cancellato dal repository, le credenziali utente sono ancora disponibili nella cache. Queste voci di credenziale non necessarie rallentano le operazioni SnapManager dalla GUI.	<p>Riavviare l'interfaccia grafica di SnapManager in base alla modalità di cancellazione della cache. Nota:</p> <ul style="list-style-type: none"> • Se la cache delle credenziali è stata cancellata dalla GUI di SnapManager, non è necessario uscire dalla GUI di SnapManager. • Se la cache delle credenziali è stata cancellata dall'interfaccia utente di SnapManager, è necessario riavviare l'interfaccia utente di SnapManager. • Se il file di credenziale crittografato è stato eliminato manualmente, è necessario riavviare l'interfaccia grafica di SnapManager. <p>Impostare le credenziali fornite per il repository, l'host del profilo e il profilo. Dalla GUI di SnapManager, se non è presente alcun repository mappato nella struttura dei repository, eseguire la seguente procedura:</p> <ol style="list-style-type: none"> 1. Fare clic su Tasks > Add existing repository 2. Fare clic con il pulsante destro del mouse sul repository, fare clic su Open (Apri) e immettere le credenziali utente nella finestra Repository Credentials Authentication (autenticazione credenziali repository). 3. Fare clic con il pulsante destro del mouse sull'host nel repository, fare clic su Open (Apri) e immettere le credenziali utente in host Credentials Authentication (autenticazione credenziali host). 4. Fare clic con il pulsante destro del mouse sul profilo sotto l'host, fare clic su Open (Apri) e immettere le credenziali utente in Profile Credentials Authentication (autenticazione credenziali profilo).

Problema	Spiegazione	Soluzione alternativa
Il messaggio di errore Impossibile elencare i criteri di protezione per il seguente motivo: Protection Manager is temporaneamente non disponibile viene visualizzato quando si seleziona Nessuno dal menu a discesa Protection Manager Protection Policy della finestra Profile Properties (Proprietà profilo) e dalla pagina delle impostazioni dei criteri della creazione guidata profilo.	Protection Manager non è configurato con SnapManager o non è in esecuzione.	Non è necessaria alcuna azione.
Non è possibile aprire l'interfaccia grafica di SnapManager utilizzando l'interfaccia grafica di avvio Web di Java a causa del livello di crittografia SSL (Secure Sockets Layer) più debole del browser.	SnapManager non supporta le crittografie SSL inferiori a 128 bit.	Aggiornare la versione del browser e controllare il livello di crittografia.

Risoluzione dei problemi di SnapDrive

Esistono alcuni problemi comuni che potrebbero verificarsi quando si utilizza SnapManager con i prodotti SnapDrive.

Innanzitutto, devi determinare se il problema riguarda SnapManager per Oracle o SnapDrive. Se il problema riguarda un errore SnapDrive, SnapManager per Oracle visualizza un messaggio di errore simile a:

```
SMO-12111: Error executing snapdrive command "<snapdrive command>":
<snapdrive error>
```

Di seguito viene riportato un esempio di messaggio di errore SnapDrive in cui SMO-12111 è il numero di errore SnapManager. Lo schema di numerazione 0001-770 rappresenta gli errori SnapDrive per UNIX.

```
SMO-12111: Error executing snapdrive command
"/usr/sbin/snapdrive snap restore -file
/mnt/pathname/ar_anzio_name_10gR2_arrac1/data/undotbs02.dbf
-snapname pathname.company.com:
/vol/ar_anzio_name_10gR2_arrac1:
TEST_ARRAC1_YORKTOW_arrac12_F_C_0_8abc01b20f9ec03d010f9ec06bee0001_0":
0001-770
Admin error: Inconsistent number of files returned when listing contents
of
/vol/ar_anzio_name_10gR2_arrac1/.snapshot/
TEST_ARRAC1_YORKTOW_arrac12_F_C_0_8abc01b20f9ec03d010f9ec06bee0001_0/data
on filer pathname.
```

Di seguito sono riportati i messaggi di errore SnapDrive per UNIX più comuni relativi al rilevamento LUN, ai problemi di configurazione e allo spazio. Se si riceve uno di questi errori, consultare il capitolo risoluzione dei problemi della *Guida amministrativa e d'installazione di SnapDrive*.

Sintomo	Spiegazione
0001-136 errore amministratore: Impossibile accedere al filer: <filer> impostare il nome utente e/o la password per <filer>	Configurazione iniziale di SnapDrive
0001-382 errore di amministrazione: Risincronizzazione multipathing non riuscita	Errore di rilevamento LUN
0001-462 errore amministratore: Impossibile disconfigurare multipathing per <LUN>: Spd5: Impossibile arrestare il dispositivo. Dispositivo occupato.	Errore di rilevamento LUN
0001-476 errore amministratore: Impossibile rilevare il dispositivo associato a... 0001-710 errore amministratore: Aggiornamento del sistema operativo del LUN non riuscito...	Errore di rilevamento LUN
0001-680 errore di amministrazione: Il sistema operativo host richiede un aggiornamento dei dati interni per consentire la creazione o la connessione del LUN. Utilizzare 'SnapDrive config prepare lun' o aggiornare queste informazioni manualmente...	Errore di rilevamento LUN
0001-817 errore amministratore: Impossibile creare il clone del volume... : FlexClone non concesso in licenza	Configurazione iniziale di SnapDrive

Sintomo	Spiegazione
0001-878 errore di amministrazione: Assistente HBA non trovato. I comandi che coinvolgono LUN dovrebbero fallire.	Errore di rilevamento LUN

Risoluzione dei problemi relativi alla ridenominazione del sistema storage

Si potrebbero verificare problemi durante la ridenominazione di un sistema storage o dopo aver rinominato correttamente il sistema.

Quando si tenta di rinominare il sistema di storage, l'operazione potrebbe non riuscire e visualizzare il seguente messaggio di errore: SMO-05085 Nessun controller di storage "fas3020-rtp07New" trovato associato al profilo

Immettere l'indirizzo IP o il nome del sistema di storage elencato quando si esegue il comando `smo storage list`.

Dopo aver rinominato il sistema di storage, le operazioni SnapManager potrebbero non riuscire se SnapManager non riconosce il sistema di storage. Per risolvere il problema, è necessario eseguire alcuni passaggi aggiuntivi nell'host del server DataFabric Manager e nell'host del server SnapManager.

Eseguire le seguenti operazioni nell'host del server DataFabric Manager:

1. Eliminare l'indirizzo IP e l'host del sistema di storage precedente nel file host che si trova in `/etc/hosts` nell'host del server DataFabric Manager.
2. Aggiungere il nuovo indirizzo IP e l'host del nuovo sistema di storage nel file host che si trova in `/etc/hosts` nell'host del server DataFabric Manager.
3. Modificare il nome host dello storage immettendo il seguente comando: `dfm host rename -a old_host_name new_host_name`
4. Impostare il nuovo indirizzo IP nell'host immettendo il seguente comando: `host dfm set old_host_name_or_ObjId hostPrimaryAddress = new_storage_controller_ip_address`



Eseguire questa operazione solo se è stato specificato l'indirizzo IP come nuovo nome del sistema di storage.

5. Aggiornare il nuovo nome del sistema di storage nell'host del server DataFabric Manager immettendo il seguente comando: `dfm host diag old_storage_name`

È possibile verificare che il nome del controller di storage precedente venga sostituito con il nuovo nome del controller di storage immettendo il seguente comando: `host dfm Discover new_storage_name`

Eseguire le seguenti operazioni come utente root nell'host del server SnapManager.



Quando si inserisce il nuovo nome del controller di storage, assicurarsi di utilizzare il nome alias del sistema e non il nome di dominio completo (FQDN).

1. Eliminare il nome del sistema di storage precedente immettendo il seguente comando: `SnapDrive config delete old_storage_name`



Se non si elimina il nome del sistema di storage precedente, tutte le operazioni SnapManager non vengono eseguite correttamente.

2. Eliminare l'indirizzo IP e l'host del sistema di storage precedente nel file host situato in etc/hosts nell'host del database di destinazione.
3. Aggiungere il nuovo indirizzo IP e l'host del nuovo sistema di storage nel file host che si trova in /etc/hosts nell'host del database di destinazione.
4. Aggiungere il nuovo nome del sistema di storage immettendo il seguente comando: `SnapDrive config set root new_storage_name`
5. Mappare i nomi dei sistemi di storage precedenti e successivi immettendo il seguente comando: `SnapDrive config migra set old_storage_name new_storage_name`
6. Eliminare il percorso di gestione del sistema di storage precedente immettendo il seguente comando: `snapdrive config delete -mgmtpath old_storage_name`
7. Aggiungere il percorso di gestione per il nuovo sistema di storage immettendo il seguente comando: `SnapDrive config set -mgmtpath new_storage_name`
8. Aggiornare il set di dati per i file di dati e i file di log dell'archivio con il nuovo nome del sistema di storage immettendo il seguente comando: `SnapDrive DataSet changehostname -dndataset_name -oldnameold_storage_name-newnamenew_storage_name`
9. Aggiornare il profilo per il nuovo nome del sistema di storage immettendo il seguente comando: `smo storage rename -profileprofile_name-oldnameold_storage_name-newnamenew_storage_name`
10. Verificare il sistema storage associato al profilo immettendo il seguente comando: `smo storage list -profileprofile_name`

Risoluzione dei problemi noti

È necessario essere a conoscenza di alcuni problemi noti che potrebbero verificarsi quando si utilizza SnapManager e di come risolverli.

SnapManager per Oracle non riesce a identificare i profili in modalità cluster

Se il nome del profilo Cluster-Mode non è presente nel file `cmode_profiles.config` nella directory di installazione di SnapManager per Oracle, potrebbe essere visualizzato il seguente messaggio di errore:

Configurare il server DFM utilizzando il set di configurazione SnapDrive `-nome_utente dfm nome_appliance`.

Inoltre, durante l'aggiornamento di SnapManager per Oracle, se si elimina la cartella `/opt/NetApp/smo/*`, viene eliminato anche il file `cmode_profiles.config` con i nomi dei profili in modalità cluster. Questo problema genera anche lo stesso messaggio di errore.

Soluzione

Aggiorna il profilo: `<profile_name>` di aggiornamento del profilo smo



Se SnapManager per Oracle è installato nel percorso `/opt/NetApp/smo/`, il percorso del file è `/opt/NetApp/smo/cmode_profile/cmode_profiles.config`.

Il server non si avvia

All'avvio del server, potrebbe essere visualizzato un messaggio di errore simile al seguente:

SMO-01104: Errore durante la chiamata del comando: SMO-17107: Impossibile avviare il server SnapManager sulla porta 8074 a causa dei seguenti errori: Indirizzo java.net.BindException: già in uso

Ciò potrebbe essere dovuto al fatto che le porte di ascolto SnapManager (27214 e 27215, per impostazione predefinita) sono attualmente in uso da un'altra applicazione.

Questo errore può verificarsi anche se il comando `smo_server` è già in esecuzione, ma SnapManager non rileva il processo esistente.

Soluzione

È possibile riconfigurare SnapManager o l'altra applicazione per utilizzare porte diverse.

Per riconfigurare SnapManager, modificare il seguente file: `/Opt/NTAP/smo/properties/smo.config`

Vengono assegnati i seguenti valori:

- `SMO Server.port=27214`
- `Server SMO.rmiRegistry.port=27215`
- `remote.registry.ocijdbc.port= 27215`

`Remote.registry.ocijdbc.port` deve essere uguale a `Server.rmiRegistry.port`.

Per avviare il server SnapManager, immettere il seguente comando: `smo_server start`



Se il server è già in esecuzione, viene visualizzato un messaggio di errore.

Se il server è già in esecuzione, attenersi alla seguente procedura:

1. Arrestare il server immettendo il seguente comando: `smo_server stop`
2. Riavviare il server immettendo il seguente comando: `smo_server start`

Interruzione di un'operazione SnapManager in esecuzione

Se il server SnapManager si blocca e non è possibile eseguire correttamente alcuna operazione, è possibile terminare SnapManager e le relative operazioni.

Soluzione

SnapManager funziona sia con SnapManager che con Gestione protezione. Per elencare i diversi processi in esecuzione e interrompere l'ultimo processo in esecuzione, attenersi alla procedura riportata di seguito.

1. Elencare tutti i processi SnapDrive in esecuzione: `ps`

Esempio: `ps | grep SnapDrive`

2. Arrestare il processo o i processi SnapDrive: `Kill <pid>`

`pid` è l'elenco dei processi trovati utilizzando il comando `ps`.



Non interrompere tutti i processi SnapDrive. È possibile terminare solo l'ultimo processo in esecuzione.

3. Se una delle operazioni comporta il ripristino di un backup protetto dallo storage secondario, aprire la console di Protection Manager ed eseguire le seguenti operazioni:
 - a. Dal menu System (sistema), selezionare **Jobs** (processi).
 - b. Selezionare **Restore** (Ripristina).
 - c. Verificare il nome del dataset che corrisponde a quello nel profilo SnapManager.
 - d. Fare clic con il pulsante destro del mouse e selezionare **Annulla**.
4. Elencare i processi SnapManager:
 - a. Accedere come utente root.
 - b. Elencare i processi utilizzando il comando ps.

Esempio: ps | grep java

5. Terminare il processo SnapManager: Uccidere <pid>

Impossibile eliminare o liberare l'ultimo backup protetto

Quando si crea il primo backup per un profilo sullo storage secondario, SnapManager invia tutte le informazioni sul backup a Gestione protezione. Per i backup successivi relativi a questo profilo, SnapManager invia solo le informazioni modificate. Se si rimuove l'ultimo backup protetto, SnapManager perde la capacità di identificare le differenze tra i backup e deve trovare un modo per eseguire una nuova baseline di queste relazioni. Pertanto, se si tenta di eliminare l'ultimo backup protetto, viene visualizzato un messaggio di errore.

Soluzione

È possibile eliminare il profilo o solo il backup del profilo.

Per eliminare il profilo, attenersi alla seguente procedura:

1. Eliminare i backup del profilo.
2. Aggiornare il profilo e disattivare la protezione nel profilo.

In questo modo si elimina il dataset.

3. Eliminare l'ultimo backup protetto.
4. Eliminare il profilo.

Per eliminare solo il backup, attenersi alla seguente procedura:

1. Creare un'altra copia di backup del profilo.
2. Trasferire la copia di backup sullo storage secondario.
3. Eliminare la copia di backup precedente.

Impossibile gestire i nomi di destinazione del file di log dell'archivio se i nomi di destinazione fanno parte di altri nomi di destinazione

Durante la creazione di un backup del registro di archiviazione, se l'utente esclude una destinazione che fa parte di altri nomi di destinazione, vengono esclusi anche gli altri nomi di destinazione.

Ad esempio, si supponga che siano disponibili tre destinazioni da escludere: /Dest, /dest1 e /dest2. Durante la creazione del backup del file di log dell'archivio, se si esclude /dest utilizzando il comando

```
smo backup create -profile almsamp1 -data -online -archivelogs -exclude  
-dest /dest
```

, SnapManager per Oracle esclude tutte le destinazioni che iniziano con /dest.

Soluzione

- Aggiungere un separatore di percorso dopo aver configurato le destinazioni in v€archive_dest. Ad esempio, modificare /dest in /dest/.
- Durante la creazione di un backup, includere le destinazioni invece di escludere qualsiasi destinazione.

Il ripristino dei file di controllo multiplati in ASM (Automatic Storage Management) e storage non ASM non riesce

Quando i file di controllo vengono multiplati su storage ASM e non ASM, l'operazione di backup viene eseguita correttamente. Tuttavia, quando si tenta di ripristinare i file di controllo dal backup eseguito correttamente, l'operazione di ripristino non riesce.

L'operazione di clonazione SnapManager non riesce

Quando si clona un backup in SnapManager, il server DataFabric Manager potrebbe non rilevare i volumi e visualizzare il seguente messaggio di errore:

SMO-13032: Impossibile eseguire l'operazione: Creazione clone. Causa principale: SMO-11007: Clonazione errore da snapshot: FLOW-11019: Errore in ExecuteConnectionSteps: SD-00018 20091122235002515: Errore durante il rilevamento dello storage per /mnt/datafile_clone3: SD-10016: Errore durante l'esecuzione del comando SnapDrive "/usr/sbin/snapdrive storage show -fs /mnt/datafile_clone3": 0002-719 Avviso: Impossibile controllare il volume SD.xfiler.x.v.

Motivo: Risorsa specificata non valida. Impossibile trovare l'ID sul server Operations Manager 10.x.x.x

Ciò si verifica se il sistema di storage dispone di un elevato numero di volumi.

Soluzione

Eseguire una delle seguenti operazioni:

- Dal server Data Fabric Manager, eseguire l'host dfm Discover storage_system.

È inoltre possibile aggiungere il comando in un file di script della shell e pianificare un processo nel server DataFabric Manager per eseguire lo script a intervalli frequenti.

- Aumentare il valore dei tentativi dfm-rbac nel file SnapDrive.conf.

SnapDrive utilizza il valore predefinito dell'intervallo di refresh e il numero predefinito di tentativi. Il valore predefinito di dfm-rbac-RETRY-sleep-secs è 15 secondi e dfm-rbac-RETRY è 12 iterazioni.



L'intervallo di aggiornamento di Operations Manager dipende dal numero di sistemi storage, dal numero di oggetti storage nel sistema storage e dal carico sul server DataFabric Manager.

Come consiglio, eseguire le seguenti operazioni:

- a. Dal server DataFabric Manager, eseguire manualmente il seguente comando per tutti i sistemi di storage secondari associati al dataset: Host dfm Discover storage_system
- b. Raddoppiare il tempo necessario per eseguire l'operazione di rilevamento dell'host e assegnare tale valore a dfm-rbac-RETRY-sleep-secs.

Ad esempio, se l'operazione richiede 11 secondi, è possibile impostare il valore di dfm-rbac-RETRY-sleep-secs su 22 (11*2).

Le dimensioni del database del repository aumentano con il tempo e non con il numero di backup

Le dimensioni del database del repository aumentano con il tempo perché le operazioni SnapManager inseriscono o eliminano i dati all'interno dello schema nelle tabelle del database del repository, il che comporta un elevato utilizzo dello spazio dell'indice.

Soluzione

È necessario monitorare e ricostruire gli indici in base alle linee guida Oracle per controllare lo spazio occupato dallo schema del repository.

Non è possibile accedere all'interfaccia grafica di SnapManager e le operazioni SnapManager non vengono eseguite quando il database del repository non è attivo

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

La tabella seguente elenca le diverse azioni che si desidera eseguire e le relative eccezioni:

Operazioni	Eccezioni
Apertura di un repository chiuso	Il seguente messaggio di errore viene registrato in SM_gui.log: [WARN]: SMO-01106: Si è verificato un errore durante la query del repository: CLOSED Connection java.sql.SQLException: CLOSED Connection.
Aggiornare un repository aperto premendo F5	Nella GUI viene visualizzata un'eccezione di repository e viene inoltre registrato un NullPointerException nel file sm_gui.log.
Aggiornamento del server host	Nel file sumo_gui.log viene registrata un'eccezione NullPointerException.
Creazione di un nuovo profilo	Nella finestra Configurazione profilo viene visualizzata un'eccezione NullPointerException.
Aggiornamento di un profilo	La seguente eccezione SQL viene registrata in SM_gui.log: [WARN]: SMO-01106: Errore durante la query del repository: Connessione chiusa.

Accesso a un backup	Il seguente messaggio di errore viene registrato in SM_gui.log: Impossibile inizializzare una raccolta in modo non corretto.
Visualizzazione delle proprietà dei cloni	Il seguente messaggio di errore viene registrato in sm_gui.log e sumo_gui.log: Impossibile inizializzare una raccolta in modo non corretto.

Soluzione

È necessario assicurarsi che il database del repository sia in esecuzione quando si desidera accedere alla GUI o eseguire operazioni SnapManager.

Impossibile creare file temporanei per il database clonato

Quando i file tablespace temporanei del database di destinazione vengono posizionati in punti di montaggio diversi dal punto di montaggio dei file di dati, l'operazione di creazione del clone ha esito positivo, ma SnapManager non riesce a creare file temporanei per il database clonato.

Soluzione

Eseguire una delle seguenti operazioni:

- Assicurarsi che il database di destinazione sia disposto in modo che i file temporanei siano posizionati nello stesso punto di montaggio dei file di dati.
- Creare o aggiungere manualmente file temporanei nel database clonato.

Impossibile migrare il protocollo da NFSv3 a NFSv4

È possibile migrare il protocollo da NFSv3 a NFSv4 attivando il parametro enable-migra-nfs-version nel file snapdrive.conf. Durante la migrazione, SnapDrive prende in considerazione solo la versione del protocollo, indipendentemente dalle opzioni del punto di montaggio quali rw, largefile, nosuid e così via.

Tuttavia, dopo la migrazione del protocollo a NFSv4, quando si ripristina il backup creato utilizzando NFSv3, si verifica quanto segue:

- Se NFSv3 e NFSv4 sono attivati a livello di storage, l'operazione di ripristino ha esito positivo, ma viene montata con le opzioni del punto di montaggio disponibili durante il backup.
- Se solo NFSv4 è attivato a livello di storage, l'operazione di ripristino ha esito positivo e viene mantenuta solo la versione del protocollo (NFSv4).

Tuttavia, le altre opzioni di mount point come rw, largefile, nosuid e così via non vengono mantenute.

Soluzione

Prima di eseguire il ripristino, è necessario arrestare manualmente il database, smontare i punti di montaggio del database e montarli con le opzioni disponibili.

Il backup del database Standby Data Guard non riesce

Se una posizione del registro di archiviazione è configurata con il nome del servizio del database primario, il backup del database di standby Data Guard non riesce.

Soluzione

Nella GUI, è necessario deselezionare **specificare la posizione del registro archivio esterno** corrispondente al nome del servizio del database primario.

Il montaggio di un volume FlexClone non riesce in ambiente NFS

Quando SnapManager crea un FlexClone di un volume in un ambiente NFS, viene aggiunta una voce nel file `/etc/exports`. Impossibile montare il clone o il backup su un host SnapManager con un messaggio di errore.

Il messaggio di errore è: 0001-034 errore di comando: Montaggio non riuscito: Montaggio: Filer1:/vol/SnapManager_20090914112850837_vol14 su /opt/NTAPsmo/mnt/-ora_data02-20090914112850735_1 - AVVISO opzione sconosciuta "zone=vol14" montaggio nfs: Filer1:/vol/SnapManager_20090914112850837_vol14: Permesso negato.

Allo stesso tempo, sulla console del sistema di storage viene generato il seguente messaggio: LUN Sep 14 23:58:37 PDT [filer1: export.auto.update.disabled: warning]: /Etc/exports non è stato aggiornato per il vol14 quando è stato eseguito il comando di creazione del clone vol. Aggiornare manualmente `/etc/exports` o copiare `/etc/exports.new` in esso.

Questo messaggio potrebbe non essere acquisito nei messaggi AutoSupport.



Potrebbero verificarsi problemi simili durante la clonazione di volumi FlexVol su NFS. Per attivare l'opzione `nfs.export.auto-update`, seguire la stessa procedura.

Cosa fare

1. Impostare l'opzione `nfs.export.auto-update` su on in modo che il file `/etc/exports` venga aggiornato automaticamente. opzioni `nfs.export.auto-updateon`



Nella configurazione ha Pair, assicurarsi di impostare l'opzione NFS exports (esportazioni NFS) su on per entrambi i sistemi storage.

L'esecuzione di più operazioni parallele non riesce in SnapManager

Quando si eseguono più operazioni parallele su database separati che risiedono sullo stesso sistema di storage, l'igroup per le LUN associate a entrambi i database potrebbe essere cancellato a causa di una delle operazioni. In seguito, se l'altra operazione tenta di utilizzare l'igroup cancellato, SnapManager visualizza un messaggio di errore.

Ad esempio, se si eseguono le operazioni di eliminazione e creazione del backup su database diversi quasi contemporaneamente, l'operazione di creazione del backup non riesce. I seguenti passaggi sequenziali mostrano cosa accade quando si eseguono operazioni di eliminazione e creazione di backup su database diversi quasi contemporaneamente.

1. Eseguire il comando di eliminazione del backup.
2. Eseguire il comando di creazione del backup.
3. Il comando `backup create` identifica l'igroup già esistente e utilizza lo stesso igroup per la mappatura del LUN.

4. Il comando di eliminazione del backup elimina il LUN di backup, mappato allo stesso igroup.
5. Il comando di cancellazione del backup elimina quindi l'igroup perché non vi sono LUN associati all'igroup.
6. Il comando backup create crea il backup e tenta di eseguire il mapping all'igroup che non esiste, quindi l'operazione non riesce.

Cosa fare

È necessario creare igroup per ogni sistema storage utilizzato dal database e utilizzare il seguente comando per aggiornare SDU con le informazioni igroup: SnapDrive igroup add

Impossibile ripristinare il database RAC da uno dei nodi RAC in cui non è stato creato il profilo

In un ambiente Oracle RAC in cui entrambi i nodi appartengono allo stesso cluster, se si tenta un'operazione di ripristino da un nodo diverso dal nodo in cui è stato creato il backup, l'operazione di ripristino non riesce.

Ad esempio, se si crea un backup nel nodo A e si tenta di eseguire il ripristino dal nodo B, l'operazione di ripristino non riesce.

Cosa fare

Prima di eseguire l'operazione di ripristino dal nodo B, eseguire le seguenti operazioni nel nodo B:

1. Aggiungere il repository.
2. Sincronizzare il profilo eseguendo il comando smo profile Sync.
3. Impostare la credenziale per il profilo da utilizzare per l'operazione di ripristino eseguendo il comando smo credential set.
4. Aggiornare il profilo per aggiungere il nuovo nome host e il SID corrispondente eseguendo il comando smo profile update.

Dove andare per ulteriori informazioni

Sono disponibili informazioni sulle attività di base relative all'installazione e all'utilizzo di SnapManager.

Documento	Descrizione
Pagina di descrizione di SnapManager	Questa pagina fornisce informazioni su SnapManager, riferimenti alla documentazione online e un collegamento alla pagina di download di SnapManager, da cui è possibile scaricare il software.

Documento	Descrizione
<i>Guida alla configurazione SAN Data ONTAP per 7-Mode</i>	<p>Questo documento è disponibile all'indirizzo "mysupport.netapp.com".</p> <p>Si tratta di un documento dinamico online che contiene le informazioni più aggiornate sui requisiti per la configurazione di un sistema in un ambiente SAN. Fornisce informazioni aggiornate sui sistemi storage e sulle piattaforme host, sui problemi di cablaggio, sui problemi dello switch e sulle configurazioni.</p>
Matrice di compatibilità SnapManager e SnapDrive	<p>Questo documento è disponibile nella sezione interoperabilità all'indirizzo "mysupport.netapp.com/matrix".</p> <p>Si tratta di un documento dinamico e online che contiene le informazioni più aggiornate specifiche di SnapManager e dei suoi requisiti di piattaforma.</p>
Note di rilascio di SnapManager	Questo documento viene fornito con SnapManager. È inoltre possibile scaricare una copia da "mysupport.netapp.com" . Contiene tutte le informazioni dell'ultimo minuto necessarie per eseguire la configurazione senza problemi.
Documentazione dei kit di supporto e collegamento host NetApp	"mysupport.netapp.com" .
<i>Guida alla configurazione del sistema</i>	"mysupport.netapp.com" .
Guida alla gestione degli accessi a blocchi di Data ONTAP	"mysupport.netapp.com"
Informazioni sul sistema operativo host e sul database	Questi documenti forniscono informazioni sul sistema operativo host e sul software del database.

Classificazioni dei messaggi di errore

È possibile determinare la causa di un errore se si conoscono le classificazioni dei messaggi.

La seguente tabella fornisce informazioni sugli intervalli numerici per i diversi tipi di messaggi che potrebbero essere visualizzati con SnapManager:

Gruppo	Raggio d'azione	Utilizzo
AMBIENTE	1000-1999	Utilizzato per registrare lo stato o i problemi con l'ambiente operativo di SnapManager. Questo gruppo include i messaggi sui sistemi con cui interagisce SnapManager, ad esempio l'host, il sistema di storage, il database e così via.
BACKUP	2000-2999	Associato al processo di backup del database.
RIPRISTINARE	3000-3999	Associato al processo di ripristino del database.
CLONARE	4000-4999	Associato al processo di clonazione del database.
PROFILO	5000-5999	Utilizzato per la gestione dei profili.
GESTIRE	6000-6999	Utilizzato per la gestione dei backup.
INTERFACCIA DI DATABASE VIRTUALE	7000-7999	Associato all'interfaccia del database virtuale.
INTERFACCIA DI STORAGE VIRTUALE	8000-8999	Associato all'interfaccia dello storage virtuale.
REPOSITORY	9000-9999	Associato all'interfaccia Repository.
METRICHE	10000-10999	Associato alla dimensione del backup del database, al tempo trascorso per eseguire il backup, al tempo necessario per ripristinare il database, al numero di volte in cui un database è stato clonato e così via.
INTERFACCIA HOST VIRTUALE	11000-11999	Associato all'interfaccia host virtuale. Si tratta dell'interfaccia con il sistema operativo host.
ESECUZIONE	12000-12999	Associato al pacchetto di esecuzione, incluso lo spawning e l'elaborazione delle chiamate del sistema operativo.

Gruppo	Raggio d'azione	Utilizzo
PROCESSO	13000-13999	Associato al componente di processo di SnapManager.
UTILITÀ	14000-14999	Associato alle utility SnapManager, al contesto globale e così via.
DUMP/DIAGNOSTICA	15000-15999	Associato a operazioni di dump o diagnostica.
AIUTO	16000-16999	Associato alla guida.
SERVER	17000-17999	Utilizzato nell'amministrazione del server SnapManager.
API	18000-18999	Associato all'API.
AUTH	20000-20999	Associato all'autorizzazione delle credenziali.

Messaggi di errore

Sono disponibili informazioni sui messaggi di errore associati alle diverse operazioni SnapManager.

Messaggi di errore più comuni

La tabella seguente elenca alcuni degli errori più comuni e importanti associati a SnapManager per Oracle:

Messaggio di errore	Spiegazione	Risoluzione
SD-10038: Il file system non è scrivibile.	Il processo SnapManager non dispone dell'accesso in scrittura al file system.	Assicurarsi che il processo SnapManager disponga dell'accesso in scrittura al file system. Una volta corretto, potrebbe essere necessario acquisire un'altra istantanea.
SMO-05075: Impossibile creare il profilo. È necessario configurare correttamente la relazione DP/XDP o scegliere la policy di protezione corretta in base alla relazione sottostante.	I volumi sottostanti non si trovano in una relazione SnapVault o SnapMirror.	È necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

Messaggio di errore	Spiegazione	Risoluzione
SMO-05503: È stato specificato lo stesso nome per il profilo. Specificare un nome diverso per rinominare il profilo.	I profili con nomi identici non possono esistere in un repository.	Fornire un nome di profilo non in uso.
SMO-05505: Impossibile aggiornare i metadati del dataset.	Il set di dati potrebbe essere stato eliminato o non esistere.	Prima di aggiornare i metadati del set di dati, verificare che il set di dati esista utilizzando la NetApp Management Console.
SMO-05506: Impossibile aggiornare il profilo poiché sono in esecuzione operazioni sul profilo. È necessario attendere il completamento delle operazioni, quindi aggiornare il profilo.	Impossibile aggiornare il profilo durante le operazioni di backup, ripristino e clonazione.	Aggiornare il profilo al termine dell'operazione corrente.
SMO-05509: Durata conservazione primaria archiviatelog non valida - specificare un valore intero positivo.	La durata di conservazione dei backup del log di archiviazione non può essere negativa.	Specificare un valore positivo per la durata di conservazione dei backup del registro di archiviazione.
SMO-07463: Questo ripristino di backup richiede che il database sia nello stato richiesto. Impossibile portare il database nello stato richiesto.	Il database non si trova nello stato richiesto per un'operazione di backup.	Prima di creare una copia di backup, verificare che il database si trovi in uno stato rilevante. Lo stato del database da ripristinare dipende dal tipo di processo di ripristino che si desidera eseguire e dal tipo di file da includere.
SMO-09315: Dopo aver eseguito l'aggiornamento del repository o l'operazione di aggiornamento, è possibile che non si riceva la notifica di riepilogo per le notifiche impostate nella versione precedente, a meno che non si aggiorni la notifica di riepilogo con i dettagli dell'host di notifica.	Le impostazioni di notifica non sono configurate per il repository dopo un aggiornamento in sequenza.	Dopo un aggiornamento in sequenza, aggiorna le impostazioni di notifica riepilogativa per ricevere le notifiche.

Messaggio di errore	Spiegazione	Risoluzione
SM0-02076: Il nome dell'etichetta non deve contenere caratteri speciali diversi dal carattere di sottolineatura.	Il nome dell'etichetta contiene caratteri speciali diversi dal carattere di sottolineatura.	Il nome dell'etichetta deve essere univoco all'interno del profilo. Il nome può contenere lettere, numeri, un carattere di sottolineatura (_) e un trattino (-) (ma non può iniziare con un trattino). Assicurarsi che le etichette non contengano caratteri speciali ad eccezione del carattere di sottolineatura.
SMO-06308: Eccezione quando si tenta di avviare la pianificazione: java.lang.NullPointerException	Il nome di dominio completo (FQDN) dell'host del profilo viene configurato al posto del nome host del sistema e l'FQDN dell'host del profilo non può essere risolto.	Assicurarsi di utilizzare il nome host del sistema e non l'FQDN.
Errore in ExecuteRestoreSteps: ORACLE-10003: Errore nell'esecuzione di SQL "DROP DISKGROUP;control diskgroup name; INCLUDING CONTENTS" nei confronti del database Oracle +ASM1: ORA-15039: Diskgroup non rilasciato ora-15027: Utilizzo attivo del diskgroup; "control diskgroup name;" ne preclude la dismount	L'operazione di ripristino di un backup con file di controllo non consente di eliminare il gruppo di dischi di controllo. Questo problema si verifica se nel gruppo di dischi di controllo sono presenti file di controllo di backup obsoleti.	Identificare i file di controllo di backup obsoleti ed eliminarli manualmente.
RMAN-06004: Errore ORACLE dal database del catalogo di ripristino: ORA-01424: Carattere mancante o non valido che segue il carattere di escape	L'operazione di creazione del backup non è riuscita a rimuovere la copia di backup dal catalogo quando SnapManager è integrato con RMAN.	Controllare se sono presenti script esterni utilizzati per rimuovere i backup da RMAN. Eseguire IL comando CROSSCHECK BACKUP in RMAN per aggiornare il repository RMAN e il comando resync catalog per sincronizzare il file di controllo del database di destinazione con il catalogo di ripristino.
[DEBUG]: Eccezione durante l'eliminazione del backup. java.lang.IllegalStateException: [Assertion failed] - questo stato invariante deve essere true	Vengono create più copie Snapshot per un singolo ID operazione.	Eliminare manualmente le copie Snapshot e utilizzare gli script per eliminare le voci dal repository.

Messaggio di errore	Spiegazione	Risoluzione
L'ora di sistema e l'ora visualizzate da SnapManager nei file di log non corrispondono o non sono sincronizzate.	Java 7 non supporta ancora la modifica del fuso orario.	Applicare la patch tzupdater fornita da Oracle.
DISC-00001: Impossibile rilevare lo storage: Il seguente identificatore non esiste o non è del tipo previsto: File ASM	I file di dati o di controllo o i log di ripristino vengono multiplati in un database ASM.	Rimuovere il multiplazione Oracle.
ORA-01031: Privilegi insufficienti. Verificare che il servizio Windows di SnapManager sia impostato per essere eseguito come utente con i privilegi corretti e che l'utente sia incluso nel gruppo ora_DBA.	Privilegi insufficienti in SnapManager. L'account del servizio SnapManager non fa parte del gruppo ora_DBA.	Fare clic con il pulsante destro del mouse sull'icona computer sul desktop e selezionare Gestisci per verificare che l'account utente per il servizio SnapManager faccia parte del gruppo ora_DBA. Controllare gli utenti e i gruppi locali e assicurarsi che l'account faccia parte del gruppo ora_DBA. Se l'utente è l'amministratore locale, assicurarsi che l'utente sia nel gruppo e non nell'amministratore di dominio.
0001-con-10002: I dischi ASM connessi con percorsi <paths> non sono stati rilevati dall'istanza ASM <asm_instance_sid>. Verificare che il parametro ASM_DISKSTRING e le autorizzazioni del file system consentano di rilevare questi percorsi.	I dischi ASM erano connessi all'host, ma l'istanza ASM non è in grado di rilevarli.	Se si utilizza ASM su NFS, assicurarsi che il parametro ASM_DISKSTRING per l'istanza di ASM includa i file di disco ASM. Ad esempio, se l'errore indica: smo/mnt/<dir_name>/<disk_name>, aggiungere /smo/mnt// a asm_diskstring.
0001-DS-10021: Impossibile impostare il criterio di protezione del set di dati <dataset-name> su <new-protection-policy> perché il criterio di protezione è già impostato su <old-protection-policy>. Utilizzare Protection Manager per modificare la policy di protezione	Una volta impostato il criterio di protezione di un set di dati, SnapManager non consente di modificare il criterio di protezione, in quanto potrebbe richiedere la ridefinizione delle relazioni di base e causare la perdita dei backup esistenti sullo storage secondario.	Aggiornare il criterio di protezione utilizzando la console di gestione di Protection Manager, che fornisce più opzioni per la migrazione da un criterio di protezione a un altro.

Messaggio di errore	Spiegazione	Risoluzione
0001-SD-10028: Errore SnapDrive (id:2618 code:102) Impossibile rilevare il dispositivo associato a "lun_path". Se si utilizza il multipathing, potrebbe essere presente un errore di configurazione multipathing. Verificare la configurazione e riprovare.	L'host non è in grado di rilevare le LUN create sui sistemi storage.	Assicurarsi che il protocollo di trasporto sia installato e configurato correttamente. Assicurarsi che SnapDrive sia in grado di creare e rilevare un LUN sul sistema storage.
0001-SD-10028: Errore SnapDrive (codice id:2836:110) Impossibile acquisire il blocco del set di dati sul volume "nome_storage":"nome_volume_temp"	Si è tentato di eseguire il ripristino utilizzando il metodo di storage indiretto e il volume temporaneo specificato non esiste nello storage primario.	Creare un volume temporaneo sullo storage primario. In alternativa, specificare il nome corretto del volume, se è già stato creato un volume temporaneo.
0001-SMO-02016: Alcune tabelle esterne nel database potrebbero non essere state sottoposte a backup come parte di questa operazione di backup (poiché il database non era APERTO durante questo backup, NON è stato possibile eseguire query SU ALL_EXTERNAL_LOCATIONS per determinare se esistono o meno tabelle esterne).	SnapManager non esegue il backup di tabelle esterne (ad esempio, tabelle non memorizzate in file .dbf). Questo problema si verifica perché il database non è stato aperto durante il backup. SnapManager non è in grado di determinare se vengono utilizzate tabelle esterne.	Nel database potrebbero essere presenti tabelle esterne non sottoposte a backup durante questa operazione (perché il database non è stato aperto durante il backup).
0001-SMO-11027: Impossibile clonare o montare snapshot dallo storage secondario perché le snapshot sono occupate. Provare a clonare o montare da un backup precedente.	Si è tentato di creare un clone o montare copie Snapshot dallo storage secondario dell'ultimo backup protetto.	Clonare o montare da un backup precedente.
0001-SMO-12346: Impossibile elencare i criteri di protezione perché il prodotto Protection Manager non è installato o SnapDrive non è configurato per utilizzarlo. Installare Gestione protezione e/o configurare SnapDrive...	Si è tentato di elencare i criteri di protezione su un sistema in cui SnapDrive non è configurato per l'utilizzo di Gestione protezione.	Installare Gestione protezione e configurare SnapDrive per l'utilizzo di Gestione protezione.

Messaggio di errore	Spiegazione	Risoluzione
0001-SMO-13032: Impossibile eseguire l'operazione: Eliminazione del backup. Causa principale: 0001-SMO-02039: Impossibile eliminare il backup del set di dati: SD-10028: Errore SnapDrive (id:2406 codice:102) Impossibile eliminare l'id di backup: "Backup_id" per il set di dati, errore(23410):Snapshot "nome_snapshot" sul volume "nome_volume" è occupato.	Si è tentato di liberare o eliminare l'ultimo backup protetto o un backup contenente copie Snapshot che sono linee di base in una relazione mirror.	Liberare o eliminare il backup protetto.
0002-332 errore di amministrazione: Impossibile controllare l'accesso a SD.snapshot.Clone sul volume "nome_volume" per il nome utente sui server di Operations Manager "server_dfm". Motivo: Risorsa specificata non valida. Impossibile trovare l'ID sul server di Operations Manager "dfm_server"	I ruoli e i privilegi di accesso corretti non sono impostati.	Impostare i privilegi o i ruoli di accesso per gli utenti che stanno tentando di eseguire il comando.
[WARN] FLOW-11011: Operazione interrotta [ERRORE] FLOW-11008: Operazione non riuscita: Spazio heap Java.	Il numero di file di log di archiviazione nel database è superiore al numero massimo consentito.	<ol style="list-style-type: none"> 1. Accedere alla directory di installazione di SnapManager. 2. Aprire il file java di avvio. 3. Aumentare il valore di java -Xmx160m Java heap space parameter . Ad esempio, è possibile modificare il valore dal valore predefinito 160m a 200m AS java -Xmx200m.
SD-10028: Errore SnapDrive (id:2868 codice:102) impossibile individuare snapshot remoto o qtree remoto.	SnapManager visualizza i backup come protetti anche se il processo di protezione in Gestione protezione ha esito positivo solo parzialmente. Questa condizione si verifica quando è in corso la conformità del dataset (quando le snapshot di riferimento vengono mirrorate).	Eseguire un nuovo backup dopo che il set di dati è conforme.

Messaggio di errore	Spiegazione	Risoluzione
SMO-21019: Eliminazione del log di archiviazione non riuscita per la destinazione: "/mnt/destination_name/" con il motivo: "ORACLE-00101: Errore durante l'esecuzione del comando RMAN: [DELETE NOPROMPT ARCHIVELOG '/mnt/destination_name/']"	L'eliminazione del log di archiviazione non riesce in una delle destinazioni. In uno scenario del genere, SnapManager continua a eseguire l'eliminazione dei file di log dell'archivio dalle altre destinazioni. Se alcuni file vengono eliminati manualmente dal file system attivo, RMAN non riesce a eliminare i file di log dell'archivio da quella destinazione.	Connettersi a RMAN dall'host SnapManager. Eseguire il comando CROSSCHECK ARCHIVELOG ALL di RMAN ed eseguire nuovamente l'operazione di eliminazione dei file di log dell'archivio.
SMO-13032: Impossibile eseguire l'operazione: Log di archiviazione Prune. Causa principale: Eccezione RMAN: ORACLE-00101: Errore durante l'esecuzione del comando RMAN.	I file di log dell'archivio vengono eliminati manualmente dalle destinazioni del log dell'archivio.	Connettersi a RMAN dall'host SnapManager. Eseguire il comando CROSSCHECK ARCHIVELOG ALL di RMAN ed eseguire nuovamente l'operazione di eliminazione dei file di log dell'archivio.
Impossibile analizzare l'output della shell: (java.util.regex.Matcher[pattern=comando completo. Region=0,18 lastmatch=]) non corrisponde (name:backup_script) Impossibile analizzare l'output della shell: (java.util.regex.Matcher[pattern=Command complete. region=0,25 lastmatch=]) non corrisponde (description:backup script) Impossibile analizzare l'output della shell: (java.util.regex.Matcher[pattern=comando completo. region=0,9 lastmatch=]) non corrisponde (timeout:0)	Le variabili di ambiente non sono impostate correttamente negli script pre-task o post-task.	Controllare se gli script pre-task o post-task seguono la struttura standard del plug-in SnapManager. Per ulteriori informazioni sull'utilizzo delle variabili ambientali nello script, vedere Operazioni negli script di attività .

Messaggio di errore	Spiegazione	Risoluzione
ORA-01450: Lunghezza massima chiave superata (6398).	<p>Quando si esegue un aggiornamento da SnapManager 3.2 per Oracle a SnapManager 3.3 per Oracle, l'operazione di aggiornamento non riesce e viene visualizzato questo messaggio di errore. Questo problema potrebbe verificarsi a causa di uno dei seguenti motivi:</p> <ul style="list-style-type: none"> • La dimensione del blocco dello spazio tabella in cui si trova il repository è inferiore a 8k. • Il parametro <code>nls_length_semantics</code> è impostato su <code>char</code>. 	<p>È necessario assegnare i valori ai seguenti parametri:</p> <ul style="list-style-type: none"> • <code>block_size=8192</code> • <code>nls_length=byte</code> <p>Dopo aver modificato i valori dei parametri, è necessario riavviare il database.</p> <p>Per ulteriori informazioni, vedere l'articolo della Knowledge base 2017632.</p>

Messaggi di errore associati al processo di backup del database (serie 2000)

La seguente tabella elenca gli errori comuni associati al processo di backup del database:

Messaggio di errore	Spiegazione	Risoluzione
SMO-02066: Non è possibile eliminare o liberare i "registri dei dati" di backup del registro di archiviazione, poiché il backup è associato ai "registri dei dati" di backup.	Il backup del registro di archiviazione viene eseguito insieme al backup dei file di dati e si è tentato di eliminare il backup del registro di archiviazione.	Utilizzare l'opzione <code>-force</code> per eliminare o liberare il backup.
SMO-02067: Non è possibile eliminare o liberare i "registri dei dati" di backup del registro di archiviazione, poiché il backup è associato ai "registri dei dati" di backup e rientra nella durata di conservazione assegnata.	Il backup del registro di archiviazione è associato al backup del database e rientra nel periodo di conservazione ed è stato tentato di eliminare il backup del registro di archiviazione.	Utilizzare l'opzione <code>-force</code> per eliminare o liberare il backup.
SMO-07142: Registri archiviati esclusi a causa del modello di esclusione <code><exclusion></code> .	Durante l'operazione di creazione del profilo o di backup, si escludono alcuni file di log dell'archivio.	Non è richiesta alcuna azione.
SMO-07155: I file di log archiviati di <code><count></code> non esistono nel file system attivo. Questi file di log archiviati non verranno inclusi nel backup.	I file di log dell'archivio non esistono nel file system attivo durante l'operazione di creazione del profilo o di backup. Questi file di log archiviati non sono inclusi nel backup.	Non è richiesta alcuna azione.

SMO-07148: I file di log archiviati non sono disponibili.	Durante l'operazione di creazione del profilo o di backup, non vengono creati file di log dell'archivio per il database corrente.	Non è richiesta alcuna azione.
SMO-07150: Impossibile trovare i file di log archiviati.	Tutti i file di log dell'archivio sono mancanti nel file system o esclusi durante l'operazione di creazione del profilo o di backup.	Non è richiesta alcuna azione.
SMO-13032: Impossibile eseguire l'operazione: Creazione del backup. Causa principale: ORACLE-20001: Errore nel tentativo di modificare lo stato in OPEN for database instance dfcln1: ORACLE-20004: Attesa di essere in grado di aprire il database senza l'opzione RESETLOGS, ma oracle sta segnalando che il database deve essere aperto con l'opzione RESETLOGS. Per evitare che i registri vengano reimpostati in modo imprevisto, il processo non proseguirà. Assicurarsi che il database possa essere aperto senza l'opzione RESETLOGS e riprovare.	Si tenta di eseguire il backup del database clonato creato con l'opzione -no-resetlogs. Il database clonato non è un database completo.tuttavia, è possibile eseguire operazioni SnapManager come la creazione di profili e backup, la suddivisione di cloni e così via con il database clonato, ma le operazioni SnapManager non riescono perché il database clonato non è configurato come database completo.	Ripristinare il database clonato o convertire il database in un database di standby Data Guard.

Errori di protezione dei dati


La seguente tabella mostra gli errori comuni associati alla protezione dei dati:

Messaggio di errore	Spiegazione	Risoluzione
È richiesta la protezione del backup, ma il profilo del database non dispone di criteri di protezione. Aggiornare il criterio di protezione nel profilo del database o non utilizzare l'opzione "Proteggi" durante la creazione dei backup.	Si tenta di creare un backup con protezione sullo storage secondario; tuttavia, il profilo associato a questo backup non ha un criterio di protezione specificato.	Modificare il profilo e selezionare un criterio di protezione. Ricreare il backup.

Impossibile eliminare il profilo perché la protezione dei dati è attivata, ma Protection Manager non è temporaneamente disponibile. Riprovare più tardi.	Si tenta di eliminare un profilo con la protezione attivata; tuttavia, Protection Manager non è disponibile.	Assicurarsi che i backup appropriati siano memorizzati nello storage primario o secondario. Disattiva la protezione nel profilo. Quando Protection Manager è nuovamente disponibile, tornare al profilo ed eliminarlo.
Impossibile elencare i criteri di protezione perché Protection Manager non è temporaneamente disponibile. Riprovare più tardi.	Durante la configurazione del profilo di backup, è stata attivata la protezione sul backup in modo che il backup venga memorizzato sullo storage secondario. Tuttavia, SnapManager non è in grado di recuperare i criteri di protezione dalla console di gestione di Protection Manager.	Disattivare temporaneamente la protezione nel profilo. Continuare a creare un nuovo profilo o ad aggiornare un profilo esistente. Quando Protection Manager è nuovamente disponibile, tornare al profilo.
Impossibile elencare i criteri di protezione perché il prodotto Protection Manager non è installato o SnapDrive non è configurato per utilizzarlo. Installare Gestione protezione e/o configurare SnapDrive.	Durante la configurazione del profilo di backup, è stata attivata la protezione sul backup in modo che il backup venga memorizzato sullo storage secondario. Tuttavia, SnapManager non può recuperare i criteri di protezione dalla console di gestione di Protection Manager. Protection Manager non è installato o SnapDrive non è configurato.	Installare Protection Manager. Configurare SnapDrive. Tornare al profilo, riabilitare la protezione e selezionare i criteri di protezione disponibili nella console di gestione di Protection Manager.
Impossibile impostare il criterio di protezione perché Protection Manager non è temporaneamente disponibile. Riprovare più tardi.	Durante la configurazione del profilo di backup, è stata attivata la protezione sul backup in modo che il backup venga memorizzato sullo storage secondario. Tuttavia, SnapManager non può recuperare i criteri di protezione dalla console di gestione di Protection Manager.	Disattivare temporaneamente la protezione nel profilo. Continuare a creare o aggiornare il profilo. Quando la console di gestione di Protection Manager è disponibile, tornare al profilo.
Creazione di un nuovo dataset <dataset_name> per il database <dbname> su host <host>.	Si è tentato di creare un profilo di backup. SnapManager crea un dataset per questo profilo.	Nessuna azione necessaria.

La protezione dei dati non è disponibile perché Protection Manager non è installato.	Durante la configurazione del profilo di backup, si è tentato di attivare la protezione sul backup in modo che il backup venga memorizzato sullo storage secondario. Tuttavia, SnapManager non può accedere alle policy di protezione dalla console di gestione di Protection Manager. Protection Manager non è installato.	Installare Protection Manager.
Eliminato il dataset <dataset_name> per questo database.	Hai eliminato un profilo. SnapManager eliminerà il dataset associato.	Non è necessaria alcuna azione.
Eliminazione del profilo con la protezione attivata e Protection Manager non è più configurato. Eliminazione del profilo da SnapManager ma non pulizia del set di dati in Gestione protezione.	Si è tentato di eliminare un profilo con la protezione attivata; tuttavia, Protection Manager non è più installato, non è più configurato o è scaduto. SnapManager eliminerà il profilo, ma non il dataset del profilo dalla console di gestione di Protection Manager.	Reinstallare o riconfigurare Protection Manager. Tornare al profilo ed eliminarlo.
Classe di conservazione non valida. Utilizzare "smo help backup" per visualizzare un elenco delle classi di conservazione disponibili.	Durante l'impostazione del criterio di conservazione, si è tentato di utilizzare una classe di conservazione non valida.	Creare un elenco di classi di conservazione valide immettendo questo comando: Backup della guida smo Aggiornare il criterio di conservazione con una delle classi disponibili.
Policy di protezione specificata non disponibile. Utilizzare "smo Protection-policy list" (elenco criteri di protezione smo) per visualizzare un elenco dei criteri di protezione disponibili.	Durante la configurazione del profilo, è stata attivata la protezione e inserita una policy di protezione non disponibile.	Identificare i criteri di protezione disponibili immettendo il seguente comando: smo Protection-policy list
Utilizzo del set di dati esistente <dataset_name> per il database <dbname> su <host> host poiché il set di dati esiste già.	Si è tentato di creare un profilo; tuttavia, il dataset per lo stesso profilo di database esiste già.	Controllare le opzioni del profilo esistente e assicurarsi che corrispondano a quanto richiesto nel nuovo profilo.

<p>L'utilizzo del dataset <dataset_name> esistente per il database RAC <dbname> poiché il profilo <profile_name> per lo stesso database RAC esiste già, ad esempio, <SID> sul <hostname> host.</p>	<p>Si è tentato di creare un profilo per un database RAC; tuttavia, il dataset per lo stesso profilo di database RAC esiste già.</p>	<p>Controllare le opzioni del profilo esistente e assicurarsi che corrispondano a quanto richiesto nel nuovo profilo.</p>
<p>Il set di dati <dataset_name> con il criterio di protezione <existing_policy_name> esiste già per questo database. È stato specificato il criterio di protezione <new_policy_name>. La policy di protezione del set di dati verrà modificata in <new_policy_name>. È possibile modificare il criterio di protezione aggiornando il profilo.</p>	<p>Si è tentato di creare un profilo con la protezione attivata e una policy di protezione selezionata. Tuttavia, il set di dati per lo stesso profilo di database esiste già, ma ha una policy di protezione diversa. SnapManager utilizzerà la policy appena specificata per il dataset esistente.</p>	<p>Esaminare questo criterio di protezione e determinare se si tratta del criterio che si desidera utilizzare per il dataset. In caso contrario, modificare il profilo e il criterio.</p>
<p>Protection Manager elimina i backup locali creati da SnapManager per Oracle</p>	<p>La console di gestione di Protection Manager elimina o libera i backup locali creati da SnapManager in base ai criteri di conservazione definiti in Protection Manager. La classe di conservazione impostata per i backup locali non viene presa in considerazione durante l'eliminazione o la liberazione dei backup locali. quando i backup locali vengono trasferiti a un sistema di storage secondario, la classe di conservazione impostata per i backup locali sul sistema di storage primario non viene presa in considerazione. La classe di conservazione specificata nella pianificazione del trasferimento viene assegnata al backup remoto.</p>	<p>Eseguire il comando dfpm dataset fix_smo dal server Protection Manager ogni volta che viene creato un nuovo dataset. ora i backup non vengono cancellati in base al criterio di conservazione impostato nella console di gestione di Protection Manager.</p>

<p>Hai scelto di disattivare la protezione per questo profilo. Ciò potrebbe potenzialmente eliminare il dataset associato in Protection Manager e distruggere le relazioni di replica create per tale dataset. Inoltre, non sarà possibile eseguire operazioni SnapManager come il ripristino o la clonazione dei backup secondari o terziari per questo profilo. Continuare (S/N)?</p>	<p>Si è tentato di disattivare la protezione per un profilo protetto durante l'aggiornamento del profilo dalla CLI o dalla GUI di SnapManager. È possibile disattivare la protezione per il profilo utilizzando l'opzione -noprotect dall'interfaccia utente di SnapManager o deselezionando la casella di controllo criterio di protezione gestore protezione nella finestra delle proprietà dei criteri dall'interfaccia utente di SnapManager. Quando si disattiva la protezione per il profilo, SnapManager per Oracle elimina il dataset dalla console di gestione di Protection Manager, che annulla la registrazione di tutte le copie di backup secondarie e terziarie associate al dataset.</p> <p>Dopo l'eliminazione di un set di dati, tutte le copie di backup secondarie e terziarie vengono orfane. Né Protection Manager né SnapManager per Oracle possono accedere a tali copie di backup. Le copie di backup non possono più essere ripristinate utilizzando SnapManager per Oracle.</p> <div data-bbox="621 1199 992 1409">  <p>Lo stesso messaggio di avviso viene visualizzato anche quando il profilo non è protetto.</p> </div>	<p>Si tratta di un problema noto in SnapManager per Oracle e del comportamento previsto in Protection Manager quando si distrugge un dataset. Non esiste alcuna soluzione alternativa. I backup orfani devono essere gestiti manualmente.</p>
---	--	---

Messaggi di errore associati al processo di ripristino (serie 3000)

La seguente tabella mostra gli errori più comuni associati al processo di ripristino:

Messaggio di errore	Spiegazione	Risoluzione
SMO-03031:la specifica di ripristino è necessaria per ripristinare il <variable> di backup perché le risorse di storage per il backup sono già state liberate.	Si è tentato di ripristinare un backup con le risorse di storage liberate senza specificare una specifica di ripristino.	Specificare una specifica di ripristino.

<p>SMO-03032:la specifica Restore deve contenere mappature per i file da ripristinare perché le risorse di storage per il backup sono già state liberate. I file che necessitano di mappature sono: <variable> da Snapshot: <variable></p>	<p>Si è tentato di ripristinare un backup che ha liberato le risorse di storage e una specifica di ripristino che non contiene il mapping per tutti i file da ripristinare.</p>	<p>Correggere il file delle specifiche di ripristino in modo che le mappature corrispondano ai file da ripristinare.</p>
<p>ORACLE-30028: Impossibile eseguire il dump del file di log <filename>. Il file potrebbe essere mancante/inaccessibile/corrotto. Questo file di log non verrà utilizzato per il ripristino.</p>	<p>I file di log di ripristino online o i file di log dell'archivio non possono essere utilizzati per il ripristino. questo errore si verifica per i seguenti motivi:</p> <ul style="list-style-type: none"> • I file di log di ripristino online o i file di log archiviati menzionati nel messaggio di errore non dispongono di numeri di modifica sufficienti per richiedere il ripristino. Ciò si verifica quando il database è online senza transazioni. Il log di ripristino o i file di log archiviati non hanno numeri di modifica validi che possono essere applicati per il ripristino. • Il file di log di ripristino online o il file di log archiviato menzionato nel messaggio di errore non dispone di privilegi di accesso sufficienti per Oracle. • Il file di log di ripristino online o il file di log archiviato menzionato nel messaggio di errore è corrotto e non può essere letto da Oracle. • Il file di log di ripristino online o il file di log archiviato menzionato nel messaggio di errore non viene trovato nel percorso indicato. 	<p>Se il file menzionato nel messaggio di errore è un file di log archiviato e se è stato fornito manualmente per il ripristino, assicurarsi che il file disponga delle autorizzazioni di accesso completo a Oracle. anche se il file dispone delle autorizzazioni complete, e il messaggio continua, il file di log dell'archivio non dispone di numeri di modifica da applicare per il ripristino e questo messaggio può essere ignorato.</p>
<p>SMO-03038: Impossibile eseguire il ripristino da secondario perché le risorse di storage sono ancora presenti su primario. Eseguire il ripristino da primario.</p>	<p>Si è tentato di eseguire il ripristino dallo storage secondario, ma sullo storage primario sono presenti copie Snapshot.</p>	<p>Eseguire sempre il ripristino dal primario se il backup non è stato liberato.</p>

SMO-03054: Montaggio di archbcp1 di backup per alimentare gli archivi. DS-10001: Collegamento dei punti di montaggio. [ERRORE] FLOW-11019: Errore in ExecuteConnectionSteps: SD-10028: Errore SnapDrive (id:2618 codice:305). Impossibile eliminare i seguenti file. I volumi corrispondenti potrebbero essere di sola lettura. Riprovare il comando con le snapshot meno recenti.[ERRORE] FLOW-11010: Operazione in transizione per interrompere a causa di un guasto precedente.	Durante il ripristino, SnapManager tenta di montare l'ultimo backup da secondario per alimentare i file di log dell'archivio da secondario.tuttavia, se sono presenti altri backup, il ripristino può avere esito positivo. Tuttavia, se non sono presenti altri backup, il ripristino potrebbe non riuscire.	Non eliminare i backup più recenti da primario, in modo che SnapManager possa utilizzare il backup primario per il ripristino.
--	---	--

Messaggi di errore associati al processo di clonazione (serie 4000)

La seguente tabella mostra gli errori comuni associati al processo di clonazione:

Messaggio di errore	Spiegazione	Risoluzione
SMO-04133: La destinazione di dump non deve esistere	Si utilizza SnapManager per creare nuovi cloni; tuttavia, le destinazioni di dump da utilizzare per il nuovo clone esistono già. SnapManager non può creare un clone se esistono destinazioni di dump.	Rimuovere o rinominare le vecchie destinazioni di dump prima di creare un clone.
SMO-04908: Non è un FlexClone.	Il clone è un clone del LUN. Questo vale per Data ONTAP 8.1 7-mode e Clustered Data ONTAP.	SnapManager supporta la suddivisione dei cloni solo sulla tecnologia FlexClone.
SMO-04904: Nessuna operazione di split clone eseguita con split-idsplit_id	L'ID operazione non è valido o non è in corso alcuna operazione di suddivisione del clone.	Fornire un ID di divisione o un'etichetta di divisione validi per lo stato di divisione del clone, il risultato e le operazioni di arresto.
SMO-04906: Operazione di interruzione del clone split non riuscita con split-idsplit_id	L'operazione di divisione è completata.	Controllare se il processo di split è in corso utilizzando il comando clone split-status o clone split-risultato.

SMO-13032:Impossibile eseguire l'operazione: Creazione clone. Causa principale: ORACLE-00001: Errore durante l'esecuzione di SQL: [ALTER DATABASE OPEN RESETLOGS;]. Il comando ha restituito: ORA-38856: Cannot mark instance UNNAMED_INSTANCE_2 (redo thread 2) as enabled.	<p>La creazione del clone non riesce quando si crea il clone dal database di standby utilizzando la seguente configurazione:</p> <ul style="list-style-type: none"> • Il database principale è un'installazione RAC e il database di standby è standalone. • Lo standby viene creato utilizzando RMAN per eseguire il backup dei file di dati. 	Aggiungere il parametro <code>_no_recovery_through_resetlogs=TRUE</code> nel file di specifica del clone prima di creare il clone. Per ulteriori informazioni, consultare la documentazione Oracle (ID 334899.1). Assicurarsi di disporre del nome utente e della password Oracle metalink.
	Non è stato fornito un valore per un parametro nel file di specifica del clone.	È necessario fornire un valore per il parametro o eliminarlo se non è richiesto dal file di specifica del clone.

Messaggi di errore associati al processo di gestione del profilo (serie 5000)

La seguente tabella mostra gli errori comuni associati al processo di clonazione:

Messaggio di errore	Spiegazione	Risoluzione
SMO-20600: Profilo "profile1" non trovato nel repository "repo_name". Eseguire la sincronizzazione del profilo per aggiornare le mappature da profilo a repository.	L'operazione di dump non può essere eseguita quando la creazione del profilo non riesce.	USA smosystem dump.

Messaggi di errore associati alla liberazione delle risorse di backup (backup serie 6000)

La seguente tabella mostra gli errori comuni associati alle attività di backup:

Messaggio di errore	Spiegazione	Risoluzione
SMO-06030: Impossibile rimuovere il backup perché è in uso: <variable>	Si è tentato di eseguire l'operazione senza backup utilizzando i comandi, quando il backup è montato, o ha cloni, o è contrassegnato per essere conservato su una base illimitata.	Smontare il backup o modificare il criterio di conservazione senza limiti. Se esistono cloni, eliminarli.
SMO-06045: Impossibile liberare <variable> di backup perché le risorse di storage per il backup sono già state liberate	Si è tentato di eseguire l'operazione senza backup utilizzando i comandi, quando il backup è già stato liberato.	Non è possibile liberare il backup se è già stato liberato.

SMO-06047: È possibile liberare solo i backup riusciti. Lo stato del <ID> di backup è <status>.	Si è tentato di eseguire l'operazione senza backup utilizzando i comandi, quando lo stato del backup non è riuscito.	Riprovare dopo aver eseguito correttamente il backup.
SMO-13082: Impossibile eseguire Operation <variable> su <ID> di backup perché le risorse di storage per il backup sono state liberate.	Utilizzando i comandi, si è tentato di montare un backup con le risorse di storage liberate.	Non è possibile montare, clonare o verificare un backup che abbia liberato le risorse di storage.

Errori dell'interfaccia dello storage virtuale (interfaccia dello storage virtuale serie 8000)

La seguente tabella mostra gli errori comuni associati alle attività dell'interfaccia dello storage virtuale:

Messaggio di errore	Spiegazione	Risoluzione
SMO-08017 errore durante il rilevamento dello storage per /.	SnapManager ha tentato di individuare le risorse di storage, ma ha trovato file di dati, file di controllo o log nella directory root/. Questi file devono risiedere in una sottodirectory. Il file system root potrebbe essere un disco rigido nel computer locale. SnapDrive non può eseguire copie Snapshot in questa posizione e SnapManager non può eseguire operazioni su questi file.	Controllare se i file di dati, i file di controllo o i log di ripristino si trovano nella directory principale. In tal caso, spostarli nelle posizioni corrette o ricreare i file di controllo o ripetere i log nelle posizioni corrette. Ad esempio: Spostare redo.log in /data/oracle/redo.log, dove /data/oracle è il punto di montaggio.

Messaggi di errore associati al processo di aggiornamento in corso (serie 9000)

La seguente tabella mostra gli errori comuni associati al processo di aggiornamento in sequenza:

Messaggio di errore	Spiegazione	Risoluzione
SMO-09234:gli host seguenti non esistono nel vecchio repository. <hostnames>.	Si è tentato di eseguire l'aggiornamento in sequenza di un host, che non esiste nella versione precedente del repository.	Controllare se l'host esiste nel repository precedente utilizzando il comando repository show-repository della versione precedente dell'interfaccia utente di SnapManager.
SMO-09255:gli host seguenti non esistono nel nuovo repository. <hostnames>.	Si è tentato di eseguire il rollback di un host, che non esiste nella nuova versione del repository.	Controllare se l'host esiste nel nuovo repository utilizzando il comando show-repository del repository della versione successiva dell'interfaccia utente di SnapManager.

SMO-09256:rollback non supportato, poiché esistono nuovi profili <profilenames>.per gli host specificati <hostnames>.	Si è tentato di eseguire il rollback di un host che contiene nuovi profili esistenti nel repository. Tuttavia, questi profili non esistevano nell'host della versione precedente di SnapManager.	Eliminare i nuovi profili nella versione successiva o aggiornata di SnapManager prima del rollback.
SMO-09257:rollback non supportato, in quanto i backup <backupid> sono montati nei nuovi host.	Si è tentato di eseguire il rollback di una versione successiva dell'host SnapManager che ha montato i backup. Questi backup non sono montati nella versione precedente dell'host SnapManager.	Smontare i backup nella versione successiva dell'host SnapManager, quindi eseguire il rollback.
SMO-09258:rollback non supportato, in quanto i backup <backupid> sono smontati nei nuovi host.	Si è tentato di eseguire il rollback di una versione successiva dell'host SnapManager in cui sono stati disinstallati i backup.	Montare i backup nella versione successiva dell'host SnapManager, quindi eseguire il rollback.
SMO-09298:Impossibile aggiornare questo repository, in quanto dispone già di altri host nella versione successiva. Eseguire il rollingupdgrade per tutti gli host.	È stato eseguito un aggiornamento in sequenza su un singolo host, quindi è stato aggiornato il repository per tale host.	Eseguire un aggiornamento in sequenza su tutti gli host.
SMO-09297: Errore durante l'abilitazione dei vincoli. Il repository potrebbe essere in uno stato incoerente. Si consiglia di ripristinare il backup del repository eseguito prima dell'operazione corrente.	Si è tentato di eseguire un'operazione di rollback o aggiornamento in sequenza se il database del repository viene lasciato in uno stato incoerente.	Ripristinare il repository di cui è stato eseguito il backup in precedenza.

Esecuzione delle operazioni (serie 12,000)

La seguente tabella mostra gli errori comuni associati alle operazioni:

Messaggio di errore	Spiegazione	Risoluzione
SMO-12347 [ERRORE]: Server SnapManager non in esecuzione su host <host> e porta <port>. Eseguire questo comando su un host che esegue il server SnapManager.	Durante la configurazione del profilo, sono state immesse informazioni sull'host e sulla porta. Tuttavia, SnapManager non può eseguire queste operazioni perché il server SnapManager non è in esecuzione sull'host e sulla porta specificati.	Immettere il comando su un host che esegue il server SnapManager. È possibile controllare la porta con il comando <code>lsnrctl status</code> e visualizzare la porta su cui viene eseguito il database. Modificare la porta nel comando di backup, se necessario.

Esecuzione dei componenti di processo (serie 13,000)

La seguente tabella mostra gli errori comuni associati al componente di processo di SnapManager:

Messaggio di errore	Spiegazione	Risoluzione
SMO-13083: Il modello Snapname con valore "x" contiene caratteri diversi da lettere, numeri, caratteri di sottolineatura, trattini e parentesi graffe.	Durante la creazione di un profilo, è stato personalizzato il modello Snapname; tuttavia, sono stati inclusi caratteri speciali non consentiti.	Rimuovere caratteri speciali diversi da lettere, numeri, caratteri di sottolineatura, trattini e parentesi graffe.
SMO-13084: Il modello Snapname con valore "x" non contiene lo stesso numero di parentesi graffe sinistra e destra.	Durante la creazione di un profilo, è stato personalizzato il modello Snapname; tuttavia, le parentesi graffe sinistra e destra non corrispondono.	Inserire le parentesi di apertura e chiusura corrispondenti nel modello Snapname.
SMO-13085: Il modello Snapname con valore "x" contiene un nome di variabile non valido "y".	Durante la creazione di un profilo, è stato personalizzato il modello Snapname; tuttavia, è stata inclusa una variabile non consentita.	Rimuovere la variabile che causa l'offendere. Per visualizzare un elenco di variabili accettabili, vedere Naming delle copie Snapshot .
SMO-13086 il modello Snapname con valore "x" deve contenere la variabile "smid".	Durante la creazione di un profilo, è stato personalizzato il modello Snapname; tuttavia, è stata omessa la variabile smid richiesta.	Inserire la variabile smid richiesta.
SMO-13902: Avvio split clone non riuscito.	Questo errore potrebbe essere causato da diversi motivi: <ul style="list-style-type: none">• Spazio non disponibile nel volume.• SnapDrive non è in esecuzione.• Il clone potrebbe essere un clone del LUN.• Il volume FlexVol ha copie Snapshot limitate.	Verificare lo spazio disponibile nel volume utilizzando il comando clone split-estimate. Verificare che il volume FlexVol non disponga di copie Snapshot limitate.
SMO-13904: Risultato clone split non riuscito.	Ciò potrebbe essere dovuto a un guasto nel sistema SnapDrive o di storage.	Provare a lavorare su un nuovo clone.
SMO-13906: Operazione di split già in esecuzione per clone labelclone-label o IDclone-ID.	Si sta tentando di separare un clone già diviso.	Il clone è già diviso e i relativi metadati verranno rimossi.

SMO-13907: Operazione di split già in esecuzione per clone labelclone-label o IDclone-ID.	Si sta tentando di suddividere un clone in fase di split.	È necessario attendere il completamento dell'operazione di divisione.
---	---	---

Messaggi di errore associati alle utilità SnapManager (serie 14,000)

La seguente tabella mostra gli errori più comuni associati alle utility SnapManager:

Messaggio di errore	Spiegazione	Risoluzione
SMO-14501: L'ID e-mail non può essere vuoto.	L'indirizzo e-mail non è stato immesso.	Immettere un indirizzo e-mail valido.
SMO-14502: L'oggetto della posta non può essere vuoto.	L'oggetto dell'e-mail non è stato immesso.	Inserire l'oggetto dell'e-mail appropriato.
SMO-14506: Il campo del server di posta non può essere vuoto.	Non è stato immesso il nome host o l'indirizzo IP del server di posta elettronica.	Immettere il nome host o l'indirizzo IP del server di posta valido.
SMO-14507: Il campo Mail Port (porta di posta) non può essere vuoto.	Il numero della porta e-mail non è stato immesso.	Inserire il numero della porta del server di posta elettronica.
SMO-14508: L'ID di posta da non può essere vuoto.	Non hai inserito l'indirizzo e-mail del mittente.	Immettere un indirizzo e-mail valido per il mittente.
SMO-14509: Il nome utente non può essere vuoto.	È stata attivata l'autenticazione e non è stato fornito il nome utente.	Immettere il nome utente per l'autenticazione tramite posta elettronica.
SMO-14510: La password non può essere vuota. Inserire la password.	È stata attivata l'autenticazione e non è stata fornita la password.	Inserire la password di autenticazione dell'email.
SMO-14550: Email status <success/failure>.	Il numero di porta, il server di posta o l'indirizzo e-mail del destinatario non sono validi.	Fornire i valori corretti durante la configurazione dell'e-mail.
SMO-14559: Invio notifica e-mail non riuscito: <error>.	Ciò potrebbe essere dovuto a un numero di porta non valido, a un server di posta non valido o a un indirizzo di posta del destinatario non valido.	Fornire i valori corretti durante la configurazione dell'e-mail.
SMO-14560: Notifica non riuscita: Configurazione della notifica non disponibile.	Invio della notifica non riuscito, perché la configurazione della notifica non è disponibile.	Aggiungere la configurazione delle notifiche.

SMO-14565: Formato ora non valido. Inserire il formato dell'ora nel formato HH:mm.	L'ora è stata immessa in un formato non corretto.	Inserire l'ora nel formato: hh:mm.
SMO-14566: Valore data non valido. L'intervallo di date valido è compreso tra 1 e 31.	La data configurata non è corretta.	La data deve essere compresa tra 1 e 31.
SMO-14567: Valore del giorno non valido. L'intervallo di giorni valido è compreso tra 1 e 7.	Il giorno configurato non è corretto.	Immettere l'intervallo di giorni compreso tra 1 e 7.
SMO-14569: Il server non è riuscito ad avviare il programma Summary Notification.	Il server SnapManager è stato arrestato per motivi sconosciuti.	Avviare il server SnapManager.
SMO-14570: Notifica di riepilogo non disponibile.	La notifica di riepilogo non è stata configurata.	Configurare la notifica di riepilogo.
SMO-14571: Non è possibile attivare la notifica di profilo e riepilogo.	Sono state selezionate le opzioni di notifica del profilo e del riepilogo.	Attivare la notifica del profilo o la notifica di riepilogo.
SMO-14572: Fornire un'opzione di successo o errore per la notifica.	Non sono state attivate le opzioni di successo o di errore.	Selezionare l'opzione Success (riuscita) o failure (errore) oppure entrambe.

Messaggi di errore comuni di SnapDrive per UNIX

La seguente tabella mostra gli errori più comuni relativi a SnapDrive per UNIX:

Messaggio di errore	Spiegazione
0001-136 errore amministratore: Impossibile accedere al filer: <filer> impostare il nome utente e/o la password per <filer>	Errore di configurazione iniziale
0001-382 errore di amministrazione: Risincronizzazione multipathing non riuscita	Errore di rilevamento LUN
0001-462 errore amministratore: Impossibile disconfigurare multipathing per <LUN>: Spd5: Impossibile arrestare il dispositivo. Dispositivo occupato.	Errore di rilevamento LUN
0001-476 errore amministratore: Impossibile rilevare il dispositivo associato a...	Errore di rilevamento LUN

0001-680 errore di amministrazione: Il sistema operativo host richiede un aggiornamento dei dati interni per consentire la creazione o la connessione del LUN. Utilizzare 'SnapDrive config prepare lun' o aggiornare queste informazioni manualmente...	Errore di rilevamento LUN
0001-710 errore amministratore: Aggiornamento del sistema operativo del LUN non riuscito...	Errore di rilevamento LUN
0001-817 errore amministratore: Impossibile creare il clone del volume... : FlexClone non concesso in licenza	Errore di configurazione iniziale
0001-817 errore amministratore: Impossibile creare il clone del volume... : Richiesta non riuscita in quanto lo spazio non può essere garantito per il clone.	Problema di spazio
0001-878 errore di amministrazione: Assistente HBA non trovato. I comandi che coinvolgono LUN dovrebbero fallire.	Errore di rilevamento LUN
SMO-12111: Errore durante l'esecuzione del comando SnapDrive "<comando SnapDrive>": <errore SnapDrive>	Errore generico di SnapDrive per UNIX

Informazioni correlate

[Naming delle copie Snapshot](#)

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.