SnapManager per Oracle utilizza Protection Manager per proteggere un backup del database

SnapManager Oracle

NetApp
October 04, 2023

Sommario

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**

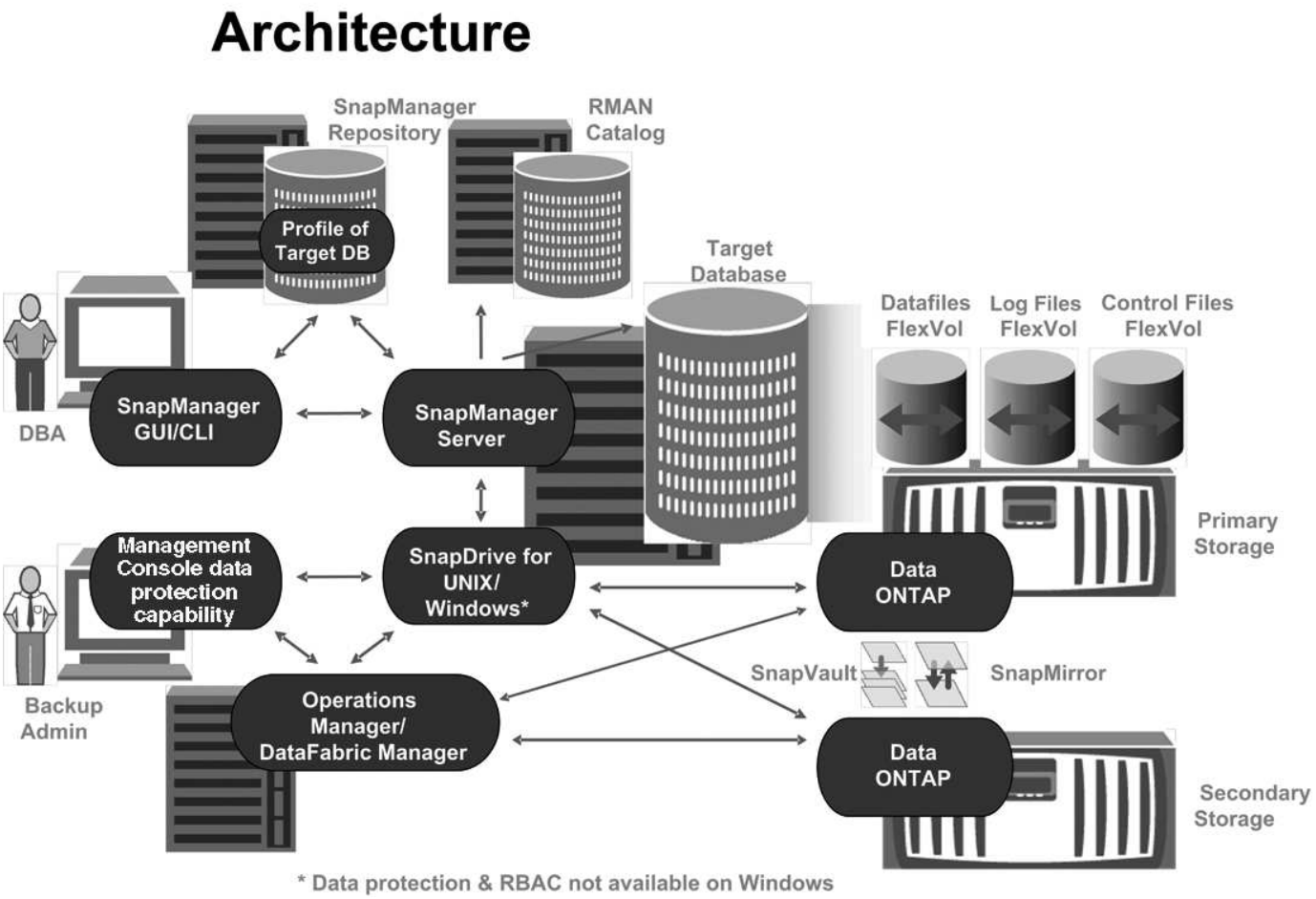
  Quando si crea un profilo in SnapManager, sono necessari i seguenti dati:

  - 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_smoprofile_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.



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**.