Geschützte Backup-Konfiguration und -Ausführung

SnapManager Oracle

NetApp
October 04, 2023

Inhalt

Geschützte Backup-Konfiguration und -Ausführung

Sie müssen SnapManager und Protection Manager konfigurieren, um die Datenbank-Sicherung auf dem sekundären Storage zu unterstützen. Der Datenbank-Administrator und der Storage-Administrator müssen ihre Aktionen koordinieren.

Verwenden von SnapManager für Oracle, um das Datenbankprofil für ein lokales Backup zu erstellen

Die Datenbankadministratoren erstellen mithilfe von SnapManager ein Datenbankprofil, mit dem ein Backup im lokalen Storage eines primären Storage-Systems initiiert wird. Die gesamte Profilerstellung und Backup-Erstellung werden in SnapManager vollständig durchgeführt – einschließlich Protection Manager ist also nicht erforderlich.

Ein Profil enthält die Informationen über die zu verwaltende Datenbank, einschließlich der Anmeldeinformationen, Backup-Einstellungen und Sicherungseinstellungen für Backups. Wenn Sie ein Profil erstellen, müssen Sie bei jeder Operation in dieser Datenbank keine Datenbankdetails angeben, sondern nur den Profilnamen angeben. Ein Profil kann nur auf eine Datenbank verweisen. Auf dieselbe Datenbank kann von mehr als einem Profil verwiesen werden.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Klicken Sie in der Struktur SnapManager-Repositories mit der rechten Maustaste auf den Host, der mit diesem Profil verknüpft werden soll, und wählen Sie **Profil erstellen** aus.
3. Geben Sie auf der Seite Profilkonfigurationsinformationen die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - Profilname: Gehaltsabrechnung_Prod
   - Profilpasswort: Payrol123
   - Kommentar: Production Payroll Datenbank
4. Geben Sie auf der Seite Datenbankkonfigurationsinformationen die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - Datenbankname: PAYDB
   - Datenbank-SID: Payrolldb
   - Datenbank-Host: Standard akzeptieren

     Da Sie ein Profil von einem Host in der Repository-Struktur erstellen, zeigt SnapManager den Hostnamen an.
5. Akzeptieren Sie auf der zweiten Seite Datenbankkonfigurationsinformationen die folgenden Datenbankinformationen und klicken Sie auf **Weiter**:
   - Host-Konto, Vertretung des Oracle-Benutzerkontos: oracle
   - Host-Gruppe, die die Oracle-Gruppe repräsentiert: dba
6. Wählen Sie auf der Seite Datenbankverbindungsinformationen die Option **Datenbankauthentifizierung verwenden** aus, damit Benutzer sich mit Datenbankinformationen authentifizieren können.

Geben Sie für dieses Beispiel die folgenden Informationen ein und klicken Sie auf **Weiter**.

- SYSDBA Privileged User Name, der den Systemadministrator der Systemdatenbank repräsentiert, der über Administratorrechte verfügt: Sys
- Kennwort (SYSDBA-Kennwort): oracle
- Port zur Verbindung mit Datenbank-Host: 1521

7. Wählen Sie auf der Seite RMAN-Konfigurationsinformationen die Option **nicht RMAN verwenden** aus, und klicken Sie auf **Weiter**.

   Oracle Recovery Manager (RMAN) ist ein Oracle Tool für das Backup und Recovery von Oracle Datenbanken mithilfe der Erkennung auf Blockebene.

8. Geben Sie auf der Seite Snapshot Naming Information eine Namenskonvention für die mit diesem Profil verknüpften Snapshots an, indem Sie Variablen auswählen. Die einzige Variable, die benötigt wird, ist die **smid**-Variable, die eine eindeutige Snapshot-Kennung erstellt.

   Gehen Sie in diesem Beispiel wie folgt vor:

   a. Wählen Sie in der Liste Variable Token die Variable **{usertext}** aus und klicken Sie auf **Hinzufügen**.
   b. Geben Sie „payroll.techco.com_" als Host-Name ein und klicken Sie auf **OK**.
   c. Klicken Sie auf **links**, bis der Hostname kurz nach "Smo" im Feld Format angezeigt wird.
   d. Klicken Sie Auf **Weiter**.

   Die Snapshot Namenskonvention von smo_hostname_smoprofile_dbsid_scope_Mode_smid wird „smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (wo der „f“ ein vollständiges Backup anzeigt, das „A“ den automatischen Modus angibt, und das „x“ stellt den einzigartigen SMID dar).

9. Überprüfen Sie auf der Seite Vorgang durchführen die Informationen und klicken Sie auf **Erstellen**.
10. Klicken Sie auf **Operation Details**, um Informationen über den Vorgang zum Erstellen von Profilen und zur Volume-basierten Wiederherstellung anzuzeigen.

Konfigurieren eines sekundären Ressourcen-Pools mit Protection Manager

Um das Backup der Datenbank auf dem sekundären Storage zu unterstützen, verwendet der Storage-Administrator Protection Manager, um die sekundären Storage-Systeme, die mit der sekundären SnapVault-Lizenz aktiviert sind, in einem Ressourcen-Pool für die Backups zu organisieren.

Idealerweise können Storage-Systeme in einem Ressourcen-Pool mit Blick auf ihre Akzeptanz als Ziele für Backups ausgetauscht werden. Wenn Sie zum Beispiel die Sicherungsstrategie für die Gehaltsabrechndatenbank entwickeln, identifizierten Sie als Storage-Administrator sekundäre Storage-Systeme mit einer ähnlichen Performance und Servicequalität, die als Mitglieder desselben Ressourcen-Pools geeignet wären.

Sie haben bereits Aggregate mit ungenutztem Speicherplatz auf Storage-Systemen erstellt, die Sie Ressourcen-Pools zuweisen möchten. Dadurch wird sichergestellt, dass ausreichend Platz zum Einhalten der Backups vorhanden ist.

1. Gehen Sie zur NetApp Management Console des Protection Manager.

2. Klicken Sie in der Menüleiste auf **Daten** > **Ressourcen-Pools**.

   Das Fenster Ressourcen-Pools wird angezeigt.

3. Klicken Sie Auf **Hinzufügen**.

   Der Assistent zum Hinzufügen von Ressourcen-Pools wird gestartet.

4. Führen Sie die Schritte im Assistenten aus, um den Ressourcen-Pool **paydb_Backup_Resource** zu erstellen.

   Verwenden Sie folgende Einstellungen:

   - Name: Verwenden Sie **paydb-Backup_Resource**
   - Speicherplatzschwellenwerte (verwenden Sie die Standardeinstellungen):
     - Schwellenwerte für die Speicherplatzauslastung: Aktiviert
     - Schwellenwert fast erreicht (für Ressourcenpool): 80 %
     - Schwellenwert (für Ressourcenpool): 90 %

Mit Protection Manager können Sie sekundäre Backup-Pläne konfigurieren

Um das Backup der Datenbank auf dem sekundären Storage zu unterstützen, verwendet der Storage-Administrator Protection Manager zum Konfigurieren eines Backup-Zeitplans.

Vor der Konfiguration des Zeitplans für sekundäre Backups gibt der Storage-Administrator folgende Informationen mit dem DBA-Partner:

- Den Zeitplan, den der DBA die sekundären Backups befolgen möchte.

  In diesem Fall finden einmal täglich Sicherungen um 7 Uhr statt Und einmal wöchentlich erfolgen Backups samstags um 1 Uhr

  a. Wechseln Sie zur NetApp Management-Konsole des Protection Manager.
  b. Klicken Sie in der Menüleiste auf **Richtlinien** > **Schutz** > **Zeitpläne**.

     Die Registerkarte Zeitpläne im Fenster Schutzrichtlinien wird angezeigt.

  c. Wählen Sie in der Terminliste den Tagesplan**täglich um 8:00 Uhr** aus.
  d. Klicken Sie Auf **Kopieren**.

     Ein neuer Tagesplan, **Kopie des Tages um 8:00 Uhr**, wird in der Liste angezeigt. Sie ist bereits ausgewählt.

  e. Klicken Sie Auf **Bearbeiten**.

     Die Eigenschaftenblatt „Tagesplan bearbeiten“ wird auf der Registerkarte „Zeitplan“ geöffnet.

  f. Ändern Sie den Terminplannamen um 7 Uhr auf **Payroll Daily**, aktualisieren Sie die Beschreibung und klicken Sie dann auf **Apply**.

Ihre Änderungen werden gespeichert.

g. Klicken Sie auf die Registerkarte * Tagesereignisse*.

   Die aktuelle tägliche Backup-Zeit des Zeitplans liegt bei 8:00 Uhr Wird angezeigt.

h. Klicken Sie auf **Hinzufügen** und geben Sie **7:00 PM** in das neue Zeitfeld ein, und klicken Sie dann auf **Anwenden**.

   Die aktuelle tägliche Backup-Zeit des Zeitplans ist jetzt 7:00 Uhr

i. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Eigenschaftenblatt zu verlassen.

   Ihr neuer Tagesplan, **Payroll Daily um 7 Uhr**, wird in der Terminliste angezeigt.

j. Wählen Sie den Wochenplan**Sonntag um 8:00 Uhr plus täglich** in der Terminliste aus.

k. Klicken Sie Auf **Kopieren**.

   Ein neuer Wochenplan, **Kopie des Sonntags um 8:00 Uhr plus täglich**, wird in der Liste angezeigt. Sie ist bereits ausgewählt.

l. Klicken Sie Auf **Bearbeiten**.

   Das Eigenschaftenblatt Wochenplan bearbeiten wird auf der Registerkarte Zeitplan geöffnet.

m. Ändern Sie den Terminplannamen in **Payroll Samstag um 1 UHR plus täglich um 7 Uhr** und aktualisieren Sie die Beschreibung.

n. Wählen Sie aus der Dropdown-Liste **Tagesplan** den soeben erstellten Tagesplan **Payroll Daily um 7 Uhr** aus.

   Wenn Sie **Payroll Daily um 7 Uhr** auswählen, wird in diesem Zeitplan festgelegt, wann der tägliche Betrieb stattfinden soll, wenn der **Gehaltsabrechnungsplan Samstag um 1 UHR plus täglich um 7 Uhr** auf eine Richtlinie angewendet wird.

o. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Eigenschaftenblatt zu verlassen.

   Ihr neuer Wochenplan, **Payroll Samstag um 1:00 Uhr plus täglich um 7:00 Uhr**, wird in der Terminliste angezeigt.

Konfigurieren einer sekundären Backup-Sicherungsrichtlinie mit Protection Manager

Nach der Konfiguration des Backup-Zeitplans konfiguriert der Storage-Administrator eine geschützte Backup-Storage-Richtlinie, in die dieser Zeitplan aufgenommen werden soll.

Vor der Konfiguration der Schutzrichtlinie gibt der Storage-Administrator folgende Informationen an den DBA-Partner:

- Aufbewahrungsdauer zur Angabe für sekundären Storage
- Typ des erforderlichen sekundären Storage-Schutzes

Die Sicherungsrichtlinie, die erstellt wird, kann vom DBA-Partner in SnapManager für Oracle aufgelistet und

einem Datenbankprofil für die zu sichernden Daten zugewiesen werden.

1. Gehen Sie zur NetApp Management Console des Protection Manager.
2. Klicken Sie in der Menüleiste auf **Richtlinien** > **Schutz** > **Übersicht**.

   Die Registerkarte Übersicht im Fenster Schutzrichtlinien wird angezeigt.

3. Klicken Sie auf **Richtlinie hinzufügen**, um den Assistenten zum Hinzufügen von Schutzrichtlinien zu starten.
4. Führen Sie den Assistenten mit den folgenden Schritten aus:

   a. Geben Sie einen beschreibenden Richtliniennamen an.

      Geben Sie in diesem Beispiel **TechCo Payroll Data: Backup** und eine Beschreibung ein und klicken Sie dann auf **Next**.

   b. Wählen Sie eine Basisrichtlinie aus.

      Wählen Sie für dieses Beispiel **Sichern** aus und klicken Sie auf **Weiter**.

   c. Akzeptieren Sie im Eigenschaftenblatt Richtlinie für den primären Datenknoten die Standardeinstellungen und klicken Sie auf **Weiter**.

      > In diesem Beispiel wird der in SnapManager konfigurierte lokale Backup-Zeitplan angewendet. Jeder lokale Backup-Zeitplan, der mit dieser Methode angegeben wird, wird ignoriert.

   d. Wählen Sie im Eigenschaftenblatt primäre Daten zu Sicherungsverbindung einen Backup-Zeitplan aus.

      Wählen Sie in diesem Beispiel **Payroll Samstag um 1 UHR plus täglich um 7 Uhr** als Backup-Zeitplan aus und klicken Sie dann auf **Weiter**.

      In diesem Beispiel enthält der ausgewählte Zeitplan sowohl die wöchentlichen als auch die täglichen Zeitpläne, die Sie zuvor konfiguriert haben.

   e. Geben Sie im Eigenschaftenblatt Backup Policy den Namen des Backup-Knotens und die Aufbewahrungszeiten für tägliche, wöchentliche oder monatliche Backups an.

      Geben Sie in diesem Beispiel eine tägliche Backup-Aufbewahrung von 10 Tagen und eine wöchentliche Backup-Aufbewahrung von 52 Wochen an. Klicken Sie nach dem Ausfüllen jedes Eigenschaftenblatts auf **Weiter**.

   Nachdem alle Eigenschaftenblätter abgeschlossen sind, zeigt der Assistent zum Hinzufügen von Schutzrichtlinien eine Zusammenfassung für die Schutzrichtlinie an, die Sie erstellen möchten.

5. Klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Die **TechCo Payroll Data: Backup** Protection Policy ist unter den anderen Richtlinien für Protection Manager aufgelistet.

Der DBA-Partner kann nun mit SnapManager für Oracle diese Richtlinie auflisten und zuweisen, wenn das Datenbankprofil für die zu sichernden Daten erstellt wird.

Verwenden von SnapManager für Oracle, um das Datenbankprofil zu erstellen und eine Sicherungsrichtlinie zuzuweisen

Sie müssen in SnapManager für Oracle ein Profil erstellen, den Schutz im Profil aktivieren und eine Sicherungsrichtlinie zuweisen, um ein geschütztes Backup zu erstellen.

Ein Profil enthält Informationen über die zu verwaltende Datenbank, einschließlich der Anmeldeinformationen, Backup-Einstellungen und Sicherungseinstellungen für Backups. Nachdem Sie ein Profil erstellt haben, müssen Sie bei jedem Vorgang keine Datenbankdetails angeben. Ein Profil kann nur auf eine Datenbank verweisen, auf die dieselbe Datenbank kann jedoch mehrere Profile verweisen.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf den Host, und wählen Sie **Profil erstellen**.
3. Geben Sie auf der Seite Profilkonfigurationsinformationen die Profildetails ein, und klicken Sie auf **Weiter**.

   Sie können die folgenden Informationen eingeben:

   - Profilname: Payroll_prod2
   - Profilpasswort: Payrol123
   - Kommentar: Production Payroll Datenbank
4. Geben Sie auf den Seiten Datenbankkonfigurationsinformationen die Datenbankdetails ein, und klicken Sie auf **Weiter**.

   Sie können die folgenden Informationen eingeben:

   - Datenbankname: PAYDB
   - Datenbank-SID: Payrolldb
   - Datenbank-Host: Standard akzeptieren. Da Sie ein Profil von einem Host in der Repository-Struktur erstellen, zeigt SnapManager den Hostnamen an.
   - Host-Konto, Vertretung des Oracle-Benutzerkontos: oracle
   - Host-Gruppe, die die Oracle-Gruppe repräsentiert: dba
5. Klicken Sie auf der Seite Datenbankverbindungsinformationen auf **Datenbankauthentifizierung verwenden**, um Benutzern die Authentifizierung anhand von Datenbankinformationen zu ermöglichen.
6. Geben Sie die Daten zur Datenbankverbindung ein und klicken Sie auf **Weiter**.

   Sie können die folgenden Informationen eingeben:

   - SYSDBA Privileged User Name, der den Systemadministrator der Systemdatenbank repräsentiert, der über Administratorrechte verfügt: Sys
   - Kennwort (SYSDBA-Kennwort): oracle
   - Port zur Verbindung mit Datenbank-Host: 1521
7. Klicken Sie auf der Seite RMAN-Konfigurationsinformationen auf **nicht RMAN verwenden** und klicken Sie auf **Weiter**.

Oracle Recovery Manager (RMAN) ist ein Oracle Tool für das Backup und Recovery von Oracle Datenbanken mithilfe der Erkennung auf Blockebene.

8. Geben Sie auf der Seite Snapshot Naming Information eine Namenskonvention für die mit diesem Profil verknüpften Snapshots an, indem Sie Variablen auswählen.

   Die smid-Variable erstellt eine eindeutige Snapshot-ID.

   Führen Sie Folgendes aus:

   a. Wählen Sie in der Liste Variable Token den Benutzertext aus und klicken Sie auf **Hinzufügen**.
   b. Geben Sie payroll.techco.com_ als Host-Name ein und klicken Sie auf **OK**.
   c. Klicken Sie auf **links**, bis der Hostname kurz nach dem Smo im Feld Format angezeigt wird.
   d. Klicken Sie Auf **Weiter**.

   Die Snapshot Namenskonvention von smo_hostname_smoprofile_dbsid_scope_Mode_smid wird „smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (wo „f“ auf ein vollständiges Backup hinweist, „A“ den automatischen Modus angibt, und „x“ stellt den einzigartigen SMID dar).

9. Wählen Sie **Protection Manager Protection Policy** Aus.

   Mit der **Protection Manager Protection Policy** können Sie eine Schutzrichtlinie auswählen, die mithilfe der NetApp Management Console konfiguriert wurde.

10. Wählen Sie aus den Schutzrichtlinien der NetApp Management Console **TechCo Payroll Data: Backup** aus und klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite Vorgang durchführen die Informationen und klicken Sie auf **Erstellen**.
12. Klicken Sie auf **Operation Details**, um Informationen über den Vorgang zum Erstellen von Profilen und zur Volume-basierten Wiederherstellung anzuzeigen.
    - Die Zuweisung einer NetApp Management Console Sicherungsrichtlinie für das Datenbankprofil erstellt automatisch einen nicht konformen Datensatz, der für den NetApp Management Console Operator sichtbar ist. Dabei wird der Name convention smo_<hostname>_<profilname> oder in diesem Beispiel: smo_payroll.tech.com_PAYDB angegeben.
    - Falls das Profil nicht für die Wiederherstellung von Volumes geeignet ist (auch als „schnelle Wiederherstellung“ bezeichnet), geschieht Folgendes:
      - Die Registerkarte **Ergebnisse** zeigt an, dass die Profilerstellung erfolgreich war und dass während des Vorgangs Warnungen aufgetreten sind.
      - Die Registerkarte **Operation Details** enthält ein WARNPROTOKOLL, in dem angegeben wird, dass das Profil nicht für eine schnelle Wiederherstellung geeignet ist und warum.

Verwenden von Protection Manager, um den neuen Datensatz bereitzustellen

Nachdem der smo_paydb-Datensatz erstellt wurde, verwendet der Storage-Administrator Protection Manager, um Storage-System-Ressourcen zuzuweisen, um den Backup-Node des Datensatzes bereitzustellen.

Vor dem Bereitstellen des neu erstellten Datensatzes vergibt der Storage-Administrator den Namen des im Profil angegebenen Datensatzes mit dem DBA-Partner.

In diesem Fall lautet der Datensatzname smo_payroll.tech.com_PAYDB.

1. Gehen Sie zur NetApp Management Console des Protection Manager.
2. Klicken Sie in der Menüleiste auf **Daten** > **Datensätze** > **Übersicht**.

   Auf der Registerkarte „Datensätze“ des Fensters „Datensätze“ wird eine Liste mit Datensätzen angezeigt, zu denen auch der Datensatz gehört, der gerade über SnapManager erstellt wurde.

3. Suchen Sie den **smo_payroll.tech.com_PAYDB**-Datensatz und wählen Sie ihn aus.

   Wenn Sie diesen Datensatz auswählen, zeigt der Diagrammbereich den smo_paydb-Datensatz mit seinem Datensicherungs-Knoten nicht bereitgestellt an. Der Konformitätsstatus wird als nicht-konform gekennzeichnet.

4. Wenn der smo_paydb-Datensatz noch hervorgehoben ist, klicken Sie auf **Bearbeiten**.

   Die NetApp Management Console des Protection Manager zeigt das Datensatz-Fenster Bearbeiten für den **smo_payroll.tech.com_PAYDB** Datensatz an. Im Navigationsbereich des Fensters werden Konfigurationsoptionen für den primären Knoten des Datensatzes, die Sicherungsverbindung und den Backup-Knoten angezeigt.

5. Suchen Sie im Navigationsbereich die Optionen für den Backup-Knoten des Datensatzes und wählen Sie **Provisioning/Resource-Pools**.

   Im Fenster Datensatz bearbeiten wird eine Einstellung für die Standard-Provisionierungsrichtlinie und eine Liste verfügbarer Ressourcen-Pools angezeigt.

6. Wählen Sie für dieses Beispiel den Ressourcen-Pool **paydb_Backup_Resource** aus, und klicken Sie auf **>**.

   Der ausgewählte Ressourcen-Pool wird im Feld „Ressourcen-Pools für diesen Node“ aufgelistet.

7. Klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Der Protection Manager stellt den sekundären Backup-Knoten automatisch mit Ressourcen aus dem Paydb_Backup_Resource-Pool bereit.

Verwendung von SnapManager für Oracle zur Erstellung eines geschützten Backups

Bei der Erstellung eines Backups für dieses Beispiel wählt der DBA die Erstellung eines vollständigen Backups, die Einstellung von Backup-Optionen und die Auswahl des Schutzes auf dem sekundären Speicher aus. Obwohl das Backup zunächst auf einem lokalen Storage erstellt wird, da dieses Backup auf einem schutzfähigen Profil basiert, wird das Backup dann gemäß dem Zeitplan der Sicherungsrichtlinie wie in Protection Manager definiert auf Sekundär-Storage übertragen.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Klicken Sie im SnapManager Repository-Baum mit der rechten Maustaste auf das Profil, das die Datenbank enthält, die Sie sichern möchten, und wählen Sie **Backup** aus.

   Der Backup-Assistent SnapManager für Oracle wird gestartet.

3. Geben Sie Production_Payroll als Beschriftung ein.
4. Geben Sie die Produktionsabrechnung Jan 19 Backup als Kommentar ein.
5. Wählen Sie als Backup-Typ die Option **Auto** aus, die Sie erstellen möchten.

   So kann SnapManager bestimmen, ob ein Online- oder Offline-Backup durchgeführt wird.

6. Wählen Sie **Daily** oder **Weekly** als Häufigkeit des Backups aus.
7. Um zu bestätigen, dass der Backup ein gültiges Format für Oracle hat, aktivieren Sie das Kontrollkästchen neben **Backup überprüfen**.

   Bei diesem Vorgang wird das Blockformat und die -Struktur mit Oracle DBVerify überprüft.

8. Um den Status der Datenbank in den entsprechenden Modus zu versetzen (z. B. von öffnen auf gemountet), wählen Sie **Start erlauben oder Herunterfahren der Datenbank, falls erforderlich**, und klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite Datenbank, Tablespaces oder Datafiles to Backup die Option **Full Backup** aus, und klicken Sie auf **Next**.
10. Um die Sicherung auf einem sekundären Speicher zu schützen, überprüfen Sie **Sichern Sie das Backup** und klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite Vorgang durchführen die von Ihnen bereitgestellten Informationen und klicken Sie auf **Sicherung**.
12. Zeigen Sie auf der Seite „Fortschritt“ den Fortschritt und die Ergebnisse der Backup-Erstellung an.
13. Um die Details der Operation anzuzeigen, klicken Sie auf **Betriebsdetails**.

Bestätigen Sie den Backup-Schutz mit SnapManager für Oracle

Mit SnapManager für Oracle können Sie eine Liste der mit einem Profil verknüpften Backups anzeigen, bestimmen, ob die Backups für den Schutz aktiviert wurden, und die Aufbewahrungsklasse (in diesem Beispiel täglich oder wöchentlich) anzeigen.

Zunächst wird das neue Backup in diesem Beispiel als geplant für den Schutz angezeigt, aber noch nicht geschützt (in der grafischen Benutzeroberfläche des SnapManager und in der Ausgabe des Backup show-Befehls). Nachdem der Storage-Administrator sicherstellt, dass das Backup in den sekundären Storage kopiert wurde, ändert SnapManager den Backup-Sicherungsstatus sowohl in der grafischen Benutzeroberfläche als auch mit dem Befehl der Backup-Liste von „nicht geschützt“ in „geschützt“.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Erweitern Sie in der Struktur des SnapManager-Repository das Profil, um seine Backups anzuzeigen.
3. Klicken Sie auf die Registerkarte **Backups/Klone**.
4. Wählen Sie im Fensterbereich Berichte die Option **Backup Details** aus.
5. Überprüfen Sie in der Spalte Schutz, und stellen Sie sicher, dass der Status „geschützt“ lautet.