SnapManager für Oracle verwendet Protection Manager, um ein Datenbank-Backup zu schützen

SnapManager Oracle

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/de-de/snapmanager-oracle/unix-administration/concept_details_of_the_target_database.html on October 04, 2023. Always check docs.netapp.com for the latest.

Inhalt

SnapManager für Oracle verwendet Protection Manager, um ein Datenbank-Backup zu schützen 1
Details der Zieldatenbank 1
Konfiguration und Topologie des primären und sekundären Storage 1
Backup-Zeitplan und Aufbewahrungsstrategie 5
Workflow-Zusammenfassung für lokale und sekundäre Datenbank-Backups 6
Geschützte Backup-Konfiguration und -Ausführung 7
Datenbankwiederherstellung aus Backup 16

SnapManager für Oracle verwendet Protection Manager, um ein Datenbank-Backup zu schützen

Wenn SnapManager für Oracle und Protection Manager auf einem UNIX-Host bzw. auf dem Server installiert sind, geben Sie dem SnapManager Datenbankadministrator (DBA) die Möglichkeit, richtlinienbasierte Oracle-Datenbank-Backups auf Sekundärspeicher zu konfigurieren und durchzuführen, Und zur Wiederherstellung, falls erforderlich, die gesicherten Daten aus dem sekundären- auf dem primären Storage.

Im folgenden Beispiel erstellt ein DBA, der SnapManager nutzt, ein Profil für ein lokales Backup im primären Storage und ein weiteres Profil für ein geschütztes Backup im Sekundärspeicher. Anschließend arbeitet dieser DBA mit seinem Netzwerk-Storage-Administrator, der die Protection Manager-Konsole verwendet, zusammen, um ein richtlinienbasiertes Backup dieser Datenbank vom primären zum sekundären Storage zu konfigurieren.

Details der Zieldatenbank

Dieses Beispiel eines integrierten Datenbankschutzes beschreibt den Schutz einer Gehaltsabrechnungsdatenbank. Im Beispiel werden die folgenden Daten verwendet.

Der Datenbankadministrator (DBA) von TechCo, einem Unternehmen mit 3000 Personen mit Hauptsitz in Atlanta, muss ein konsistentes Backup der Gehaltsabrechnungsdatenbank für die Produktion, PAYDB, erstellen. Zur Sicherungsstrategie für das Backup im primären und sekundären Storage müssen DBA und der Storage-Administrator gemeinsam die Oracle Datenbank sowohl lokal auf dem Primärspeicher als auch Remote auf dem Sekundärspeicher an einem Remote-Standort sichern.

- **Profilinformationen**

  Wenn Sie ein Profil in SnapManager erstellen, benötigen Sie die folgenden Daten:

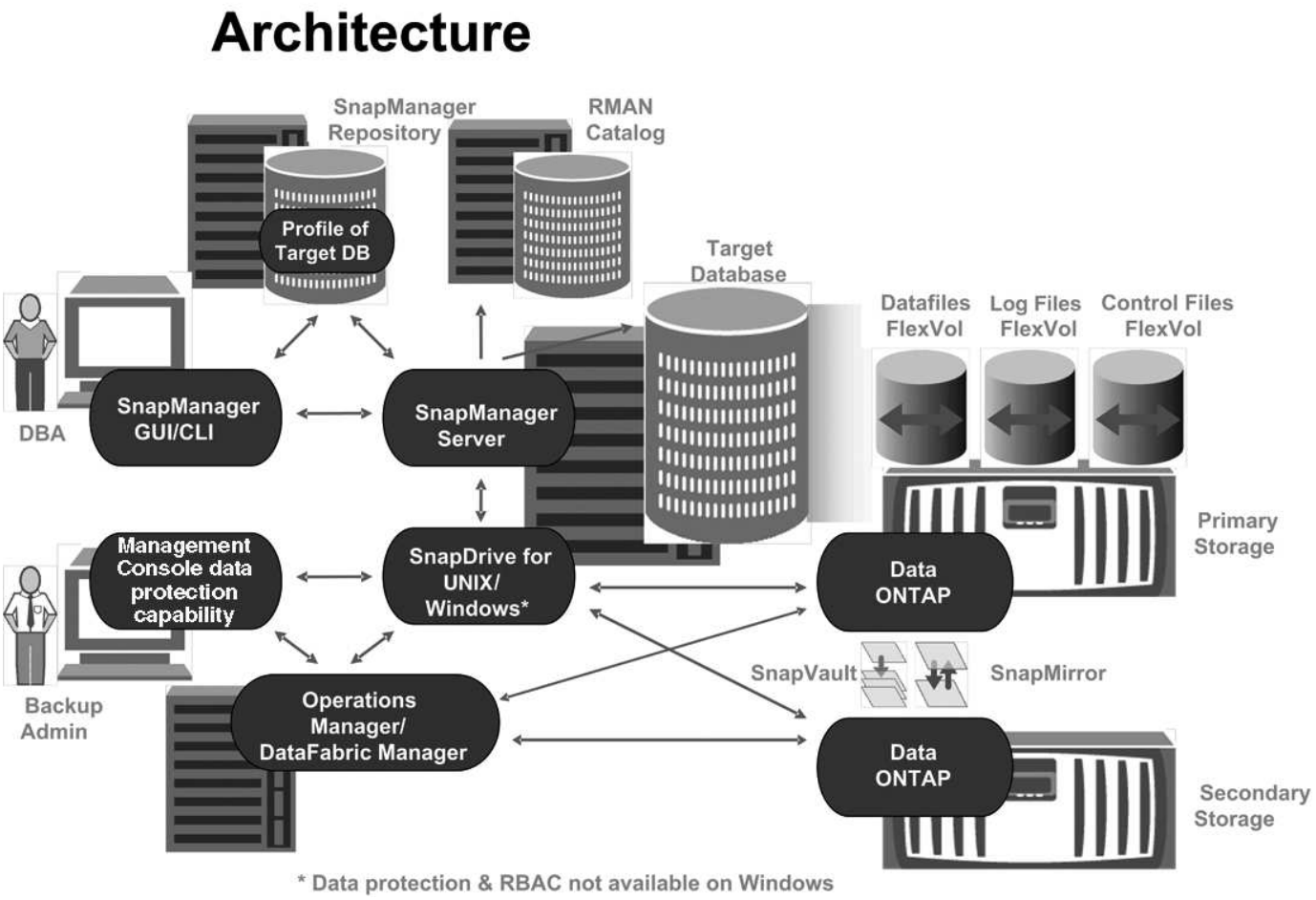
  - Datenbankname: PAYDB
  - Host-Name: payroll.techco.com
  - Datenbank-ID: Payrolldb
  - Profilname: Gehaltsabrechnung_Prod
  - Verbindungsmodus: Datenbankauthentifizierung
  - Snapshot Benennungsschema: smo_Hostname_dbsid_smoprofile_scope_Mode_smid (übersetzt in „smo_payroll.xyz.com_payrolldb_payroll_prod_f_h_x")

Konfiguration und Topologie des primären und sekundären Storage

In diesem Beispiel betreibt die TechCo-Corporation ihre Gehaltsabrechnungsdatenbank auf einem Datenbankserver, der auch ein SnapManager für Oracle-Host ist und seine Gehaltsabrechnungsdaten und Konfigurationsdateien auf Primär-Storage-Systemen an der Unternehmenszentrale speichert. Die unternehmenseigene Anforderung besteht darin, die Datenbank mit täglichen und wöchentlichen Backups auf dem lokalen Storage sowie Backups auf den Storage-Systemen an einem rund 50 Kilometer entfernten

sekundären Storage-Standort zu sichern.

Die folgende Abbildung zeigt die SnapManager für Oracle und die Datensicherungskomponenten der NetApp Management Console, die zur Unterstützung des lokalen und sekundären Backup-Schutzes erforderlich sind.



Für das Management der Gehaltsabrechnungsdatenbank und für Unterstützung des lokalen und sekundären Backup-Schutzes, wie in der vorherigen Grafik dargestellt, wird die folgende Implementierung verwendet.

- **SnapManager-Host**

  Der SnapManager Host, payroll.techco.com, befindet sich in der Unternehmenszentrale und wird auf einem UNIX Server ausgeführt, auf dem auch das Datenbankprogramm ausgeführt wird, das die Gehaltsabrechnungsdatenbank generiert und verwaltet.

  - **Verbindungen**

    Zur Unterstützung von lokalem Backup und sekundärem Backup-Schutz verfügt der SnapManager-Host über Netzwerkverbindungen mit den folgenden Komponenten:

    - SnapManager für Oracle Client
    - SnapManager-Repository für das Datenbankprogramm, SnapDrive für UNIX und SnapManager
    - Primärspeicher
    - Sekundäre Storage-Systeme
    - DataFabric Manager Server

- **Installierte Produkte**

  Der SnapManager Host wird für dieses Beispiel mit den folgenden Produkten installiert:

  - SnapManager Server
  - SnapDrive für UNIX
  - Host Utilities

- **TechCo Primärspeichersysteme**

  Die Gehaltsabrechnungsdatenbank, einschließlich zugehöriger Datendateien, Log-Dateien und Kontrolldateien, befindet sich in den primären Storage-Systemen. Diese befinden sich am Hauptsitz des Unternehmens TechCo sowie am SnapManager Host und am Netzwerk, das primären Storage mit dem SnapManager Host verbindet. Die neuesten Transaktionen und Updates der Gehaltsabrechnung von Datenbanken werden auf die primären Storage-Systeme geschrieben. Snapshot-Kopien, die einen lokalen Backup-Schutz der Gehaltsabrechnungsdatenbank bieten, befinden sich auch auf dem primären Storage-System.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügen die primären Speichersysteme über Netzwerkverbindungen mit den folgenden Komponenten:

    - Auf dem SnapManager Host wird das Datenbankprogramm, SnapDrive für UNIX und SnapManager ausgeführt
    - Sekundäre Storage-Systeme
    - DataFabric Manager Server

  - **Installierte Produkte**

    Für dieses Beispiel müssen die folgenden Lizenzen auf diesen Systemen aktiviert sein:

    - Data ONTAP 7.3.1 oder höher
    - SnapVault ONTAP Primärspeicher
    - FlexVol (erforderlich für NFS)
    - SnapRestore
    - NFS-Protokoll

- **TechCo Sekundärspeichersysteme**

  Die sekundären Storage-Systeme an einem über das Netzwerk verbundenen sekundären Storage-Standort, sind 50 Meilen entfernt, und speichern sekundäre Backups der Gehaltsabrechnungsdatenbank.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügen die sekundären Speichersysteme über Netzwerkverbindungen mit den folgenden Komponenten:

    - Primärspeicher
    - DataFabric Manager Server

  - **Installierte Produkte**

In diesem Beispiel müssen die folgenden Lizenzen auf den sekundären Speichersystemen aktiviert sein:

  - Data ONTAP
  - SnapVault ONTAP Sekundärspeicher
  - SnapRestore
  - FlexVol (erforderlich für NFS)
  - NFS-Protokoll

- **DataFabric Manager Server**

  Der DataFabric Manager Server, techco_dfm, befindet sich an der Unternehmenszentrale an einem Standort, auf den der Storage-Administrator zugreifen kann. DataFabric Manager Server koordiniert unter anderem die Backup-Aufgaben zwischen dem primären und dem sekundären Storage.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes unterhält der DataFabric Manager Server Netzwerkverbindungen mit den folgenden Komponenten:

    - NetApp Management Console
    - Primärspeicher
    - Sekundäre Storage-Systeme

  - **Installierte Produkte**

    Der DataFabric Manager-Server ist für die folgenden Serverprodukte für dieses Beispiel lizenziert:

    - DataFabric Manager

- **SnapManager-Repository**

  Das SnapManager-Repository auf einem dedizierten Server speichert Daten zu den von SnapManager ausgeführten Vorgängen, beispielsweise zum Zeitpunkt von Backups, Tabellen und Datendateien, die gesichert wurden, von verwendeten Storage-Systemen, erstellten Klonen und von Snapshot Kopien. Wenn ein DBA eine vollständige oder teilweise Wiederherstellung versucht, fragt SnapManager das Repository ab, um von SnapManager für Oracle zur Wiederherstellung erstellte Backups zu identifizieren.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügen die sekundären Speichersysteme über Netzwerkverbindungen mit den folgenden Komponenten:

    - SnapManager Host
    - SnapManager für Oracle Client

- **NetApp Management Console**

  Die NetApp Management Console ist die grafische Benutzeroberfläche, über die der Storage-Administrator Zeitpläne, Richtlinien, Datensätze und Ressourcen-Pool-Zuweisungen konfiguriert, um Backups in sekundären Storage-Systemen zu ermöglichen, auf die der Storage-Administrator zugreifen kann.

  - **Verbindungen**

Zur Unterstützung des sekundären Backup-Schutzes verfügt die NetApp Management Console über Netzwerkverbindungen mit den folgenden Komponenten:

  - Primärspeicher
  - Sekundäre Storage-Systeme
  - DataFabric Manager Server

- **SnapManager für Oracle-Client**

  Der SnapManager für Oracle Client ist die grafische Benutzeroberfläche und Befehlszeilenkonsole, die von dem DBA für die Gehaltsabrechnungsdatenbank in diesem Beispiel für die Konfiguration und das Durchführen eines lokalen Backups und Backups im Sekundärspeicher verwendet wird.

  - **Verbindungen**

    Zur Unterstützung von lokalem Backup und sekundärem Backup-Schutz verfügt SnapManager für den Oracle Client über Netzwerkverbindungen mit den folgenden Komponenten:

    - SnapManager Host
    - SnapManager-Repository für Datenbanken, SnapDrive für UNIX und SnapManager
    - Datenbank-Host (wenn getrennt von dem Host, auf dem SnapManager ausgeführt wird)
    - DataFabric Manager Server

  - **Installierte Produkte**

    Zur Unterstützung von lokalem Backup und sekundärem Backup-Schutz muss die SnapManager für Oracle Client-Software auf dieser Komponente installiert sein.

Backup-Zeitplan und Aufbewahrungsstrategie

Der DBA möchte sicherstellen, dass Backups im Falle eines Datenverlusts, im Fall eines Notfalls und aus gesetzlichen Gründen verfügbar sind. Dies erfordert eine sorgfältig durchdachte Aufbewahrungsrichtlinie für die verschiedenen Datenbanken.

Bei der Gehaltsabrechnungsdatenbank für die Produktion hält sich der DBA an die folgende TechCo-Aufbewahrungsstrategie:

Sicherungshäufigkeit	Aufbewahrungsdauer	Backup-Zeit	Art des Storage
Einmal täglich	10 Tage	7 Uhr	Primär (lokal)
Einmal täglich	10 Tage	7 Uhr	Sekundär (Archiv)
Einmal pro Woche	52 Wochen	Samstags 1 Uhr	Sekundär (Archiv)

- **Vorteile der lokalen Sicherung**

  Die täglichen lokalen Backups bieten sofortige Datenbanksicherung, belegt keine Netzwerkbandbreite, benötigt minimalen zusätzlichen Speicherplatz, ermöglicht die sofortige Wiederherstellung und bietet fein abgestimmte Backup- und Restore-Funktionen.

Da die letzten wöchentlichen Backups der Gehaltsabrechnungsdatenbank für mindestens 52 Wochen an einem sekundären Standort aufbewahrt werden, müssen die täglichen Backups nicht mehr als 10 Tage aufbewahrt werden.

- **Geschützte Backup-Vorteile**

  Tägliche und wöchentliche Backups auf dem Sekundärspeicher an einem Remote-Standort gewährleisten, dass die Zieldatenbank weiterhin gesichert ist und aus dem Sekundärspeicher wiederhergestellt werden kann, wenn die Daten am primären Storage-Standort beschädigt sind.

  Die täglichen Backups auf dem Sekundärspeicher werden durchgeführt, um das System vor Schäden am primären Speichersystem zu schützen. Da die letzten wöchentlichen Backups der Gehaltsabrechnungsdatenbank für mindestens 52 Wochen aufbewahrt werden, muss die tägliche Sicherung nicht mehr als 10 Tage aufbewahrt werden.

Workflow-Zusammenfassung für lokale und sekundäre Datenbank-Backups

In diesem Beispiel koordinieren der DBA (mittels SnapManager) und der Storage-Administrator (mithilfe der Datensicherheitsfunktion der NetApp Management Console) Aktionen zur Konfiguration von lokalem Backup und sekundärem Backup (auch als geschütztes Backup bezeichnet) der Zieldatenbank.

Die Reihenfolge der durchgeführten Maßnahmen ist wie folgt zusammengefasst:

- **Konfiguration des sekundären Ressourcen-Pools**

  Der Storage-Administrator konfiguriert mithilfe der Datensicherheitsfunktion der NetApp Management Console einen Ressourcen-Pool aus Storage-Systemen am sekundären Standort, der zum Speichern des Gehaltsabrechnungs-Backups verwendet werden kann.

- **Sekundärsicherungsplan**

  Der Storage-Administrator konfiguriert mithilfe der Datensicherheitsfunktion der NetApp Management Console sekundäre Backup-Zeitpläne.

- **Konfiguration der Schutzrichtlinien**

  Der Storage-Administrator konfiguriert mithilfe der Datensicherungsfunktionen der NetApp Management Console eine sekundäre Backup-Sicherungsrichtlinie für die Zieldatenbank. Die Sicherungsrichtlinie umfasst die Zeitpläne und legt den Basistyp für die Implementierung von Backup-Sicherung (Backup, Spiegelung oder Kombination aus beidem) fest sowie Richtlinien zur Aufbewahrung von Primärdaten, sekundären und manchmal tertiären Storage Nodes.

- **Zuweisung von Datenbankprofilen und Schutzrichtlinien**

  Der DBA erstellt und bearbeitet mit SnapManager ein Profil der Zieldatenbank, die das sekundäre Backup unterstützt. Beim Konfigurieren des Profils verfügt der DBA über:

  - Ermöglicht Backup-Sicherung auf sekundärem Storage.
  - Weist diesem Profil die neue Sicherungsrichtlinie zu, die in erstellt wurde und von der Datensicherungsfunktion der NetApp Management Console abgerufen wurde.

Das Zuweisen der Sicherungsrichtlinie schließt die Zieldatenbank automatisch in einem teilweise bereitgestellten, nicht jedoch den Datensatz mit der Datensicherungsfunktion der NetApp Management Console ein. Wenn die Datensatzkonfiguration vollständig bereitgestellt ist, kann das Backup der Zieldatenbank auf dem sekundären Storage aktiviert werden.

Der Datensatz-Name verwendet diese Syntax: smo_hostname_databaseame, was sich in „smo_payroll.techco.com_paydb"“ übersetzt.

- **Sekundäre und tertiäre Speicherbereitstellung**

  Der Storage-Administrator nutzt die NetApp Management Console Datensicherungsfunktionen, um Ressourcen-Pools zuzuweisen, um sekundäre und manchmal tertiäre Storage Nodes bereitzustellen (wenn in der zugewiesenen Sicherungsrichtlinie tertiäre Storage Nodes angegeben sind).

- **Backup auf lokalem Speicher**

  Der DBA öffnet das Profil mit aktiviertem Schutz in SnapManager und erstellt eine vollständige Sicherung zum lokalen Speicher. Das neue Backup wird in SnapManager als geplant für die Sicherung angezeigt, aber noch nicht geschützt.

- **Sekundäre Backup-Bestätigung**

  Da das Backup auf einem schutzfähigen Profil basiert, wird das Backup gemäß dem Zeitplan der Sicherungsrichtlinie auf einen zweiten übertragen. Der DBA bestätigt die Übertragung des Backups auf den sekundären Storage mithilfe von SnapManager. Nachdem das Backup in den sekundären Storage kopiert wurde, ändert SnapManager den Sicherungsstatus von „nicht geschützt“ in „geschützt“.

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.

Datenbankwiederherstellung aus Backup

Wenn der aktive Inhalt der Gehaltsabrechnungsdatenbank versehentlich verloren geht oder zerstört wird, unterstützen SnapManager und die Datensicherheitsfunktion der NetApp Management Console die Wiederherstellung dieser Daten entweder aus einem lokalen Backup oder einem sekundären Storage.

Einsatz von SnapManager für Oracle zur Wiederherstellung eines lokalen Backups im Primärspeicher

Sie können lokale Backups, die sich im Primärspeicher befinden, wiederherstellen. Der gesamte Prozess wird mit SnapManager für Oracle durchgeführt.

Sie können auch eine Vorschau der Informationen zu einem Backup-Wiederherstellungsprozess anzeigen. Möglicherweise möchten Sie dies tun, um Informationen über die Berechtigung zur Wiederherstellung eines Backups anzuzeigen. SnapManager analysiert die Daten für ein Backup, um zu ermitteln, ob der Wiederherstellungsprozess mithilfe der Volume-basierten Wiederherstellung oder der dateibasierten Restore-Methode abgeschlossen werden kann.

In der Vorschau der Wiederherstellung werden die folgenden Informationen angezeigt:

- Welcher Wiederherstellungsmechanismus (schnelle Wiederherstellung, Filesystem-Wiederherstellung auf Storage-Seite, Dateiwiederherstellung auf Storage-Seite oder Wiederherstellung von Host-seitigen Dateikopien) wird zum Wiederherstellen jeder Datei verwendet.
- Warum effizientere Mechanismen nicht verwendet wurden, um jede Datei wiederherzustellen.

In der Vorschau des Wiederherstellungsplans, SnapManager nichts wiederherstellt. In der Vorschau werden Informationen von bis zu 20 Dateien angezeigt.

Wenn Sie eine Vorschau einer Wiederherstellung von Datendateien, aber die Datenbank ist nicht gemountet, dann SnapManager mountet die Datenbank. Wenn die Datenbank nicht gemountet werden kann, schlägt der Vorgang fehl und SnapManager gibt die Datenbank in ihren ursprünglichen Zustand zurück.

1. Klicken Sie in der Repository-Struktur mit der rechten Maustaste auf das Backup, das Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen** aus.
2. Klicken Sie auf der Startseite des Wiederherstellungs- und Wiederherstellungsassistenten auf **Weiter**.
3. Wählen Sie auf der Seite Konfigurationsinformationen wiederherstellen die Option **vollständige Datei/Tablespace Wiederherstellung mit Steuerdateien** aus.
4. Klicken Sie auf **Herunterfahren der Datenbank zulassen, falls erforderlich**.

Falls erforderlich ändert SnapManager den Datenbankstatus. Wenn beispielsweise die Datenbank offline ist und sie online sein muss, erzwingt SnapManager sie online.

5. Klicken Sie auf der Seite Wiederherstellungskonfigurationsinformationen auf **Alle Protokolle**.

   SnapManager stellt die Datenbank für die letzte Transaktion wieder her und wendet alle erforderlichen Protokolle an.

6. Zeigen Sie auf der Seite Konfiguration des Quellenstandorts wiederherstellen die Informationen zum Backup auf dem primären Speicherort an, und klicken Sie auf **Weiter**.

   Wenn das Backup nur auf dem Primärspeicher besteht, stellt SnapManager das Backup aus dem Primärspeicher wieder her.

7. Wählen Sie auf der Seite mit den Informationen zur Volume-Wiederherstellung die Option **Versuch einer Volume-Wiederherstellung** aus, um die Methode zur Volume-Wiederherstellung zu versuchen.
8. Klicken Sie auf **Fallback to file-based restore**.

   Dadurch kann SnapManager die dateibasierte Wiederherstellungsmethode verwenden, wenn die Wiederherstellungsmethode des Volumes nicht verwendet werden kann.

9. Klicken Sie auf **Vorschau**, um die Eignungsprüfungen für schnelle Wiederherstellung und Informationen zu obligatorischen und überfrierbaren Prüfungen anzuzeigen.
10. Überprüfen Sie auf der Seite Vorgang durchführen die eingegebenen Informationen und klicken Sie auf **Wiederherstellen**.
11. Um Details zum Prozess anzuzeigen, klicken Sie auf **Betriebsdetails**.

Verwendung von SnapManager für Oracle zur Wiederherstellung von Backups aus dem sekundären Storage

Administratoren können geschützte Backups von sekundärem Storage wiederherstellen und wählen, wie die Daten zurück auf den primären Storage kopiert werden sollen.

Bevor Sie versuchen, das Backup wiederherzustellen, prüfen Sie die Backup-Eigenschaften und stellen Sie sicher, dass das Backup im primären Speichersystem freigegeben und auf dem Sekundärspeicher gesichert wird.

1. Klicken Sie in der Repository-Struktur SnapManager für Oracle mit der rechten Maustaste auf das Backup, das Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen** aus.
2. Klicken Sie auf der Startseite des Assistenten für Wiederherstellung und Wiederherstellung auf **Weiter**.
3. Klicken Sie auf der Seite Konfigurationsinformationen wiederherstellen auf **Datei/Tablespace Restore with Control Files**.
4. Klicken Sie auf **Herunterfahren der Datenbank zulassen, falls erforderlich**, und klicken Sie dann auf **Weiter**.

   Falls erforderlich ändert SnapManager den Datenbankstatus. Wenn beispielsweise die Datenbank offline ist und sie online sein muss, erzwingt SnapManager sie online.

5. Klicken Sie auf der Seite Wiederherstellungskonfigurationsinformationen auf **Alle Protokolle**. Klicken Sie anschließend auf **Weiter**.

   SnapManager stellt die Datenbank für die letzte Transaktion wieder her und wendet alle erforderlichen

Protokolle an.

6. Wählen Sie auf der Seite Konfiguration des Quellenstandorts wiederherstellen die ID der geschützten Sicherungsquelle aus, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite „Konfigurationsinformationen zur Volume-Wiederherstellung“ auf **Versuch, die Volume-Wiederherstellung** zu starten, um die Volume-Wiederherstellung zu versuchen.
8. Klicken Sie auf **Fallback to file-based restore**.

   Dadurch kann SnapManager die dateibasierte Wiederherstellungsmethode verwenden, wenn die Wiederherstellungsmethode des Volumes nicht abgeschlossen werden kann.

9. Klicken Sie auf **Vorschau**, um die Eignungsprüfungen für schnelle Wiederherstellung und Informationen zu obligatorischen und überridbaren Prüfungen anzuzeigen.
10. Überprüfen Sie auf der Seite „Vorgang durchführen“ die von Ihnen bereitgestellten Informationen und klicken Sie auf **Wiederherstellen**.
11. Um Details zum Prozess anzuzeigen, klicken Sie auf **Betriebsdetails**.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.