



Sichern und Überprüfen Ihrer Datenbanken

SnapManager Oracle

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/de-de/snapmanager-oracle/unix-installation-7mode/concept_snapmanager_backup_overview.html on October 04, 2023. Always check docs.netapp.com for the latest.

Inhalt

- Sichern und Überprüfen Ihrer Datenbanken 1
 - SnapManager Backup – Überblick 1
 - Backup-Strategie definieren 1
 - Erstellen eines Profils für Ihre Datenbank 4
 - Sichern Ihrer Datenbank 7
 - Datenbank-Backups werden überprüft 8
 - Planung wiederkehrender Backups 9

Sichern und Überprüfen Ihrer Datenbanken

Nach der Installation von SnapManager können Sie ein Basis-Backup Ihrer Datenbank erstellen und überprüfen, ob das Backup keine beschädigten Dateien enthält.

Verwandte Informationen

[SnapManager Backup – Überblick](#)

[Backup-Strategie definieren](#)

[Erstellen eines Profils für Ihre Datenbank](#)

[Sichern Ihrer Datenbank](#)

[Datenbank-Backups werden überprüft](#)

[Planung wiederkehrender Backups](#)

SnapManager Backup – Überblick

SnapManager erstellt mithilfe von NetApp Snapshot Technologie die Backups von Datenbanken. Sie können das DBVERIFY-Dienstprogramm verwenden oder SnapManager verwenden, um die Integrität der Backups zu überprüfen.

SnapManager sichert eine Datenbank, indem Snapshot Kopien der Volumes erstellt werden, die Datendateien, Kontrolldateien und Archivprotokolldateien enthalten. Diese Snapshot Kopien bestehen zusammen aus einem Backup-Set, mit dem SnapManager eine Datenbank wiederherstellen kann.

Backup-Strategie definieren

Wenn Sie eine Backup-Strategie vor der Erstellung Ihrer Backups definieren, stellen Sie sicher, dass Ihnen Backups zur erfolgreichen Wiederherstellung Ihrer Datenbanken zur Verfügung stehen. SnapManager bietet einen flexiblen, granularen Backup-Zeitplan, der Ihr Service Level Agreement (SLA) erfüllt.



Informationen zu den Best Practices für SnapManager finden Sie unter *TR 3761*.

Welcher Modus für SnapManager Backups benötigen Sie?

SnapManager unterstützt zwei Backup-Modi:

| Backup-Modus | Beschreibung |
|---------------|--|
| Online-Backup | Erstellt ein Backup der Datenbank, wenn sich die Datenbank im Online-Status befindet. Dieser Backup-Modus wird auch als Hot Backup bezeichnet. |

| Backup-Modus | Beschreibung |
|----------------|---|
| Offline-Backup | Erstellt eine Sicherung der Datenbank, wenn sich die Datenbank entweder im angehängten oder abschaltenden Zustand befindet. Dieser Backup-Modus wird auch als Cold Backup bezeichnet. |

Welche Art von SnapManager-Backup benötigen Sie?

SnapManager unterstützt drei Arten von Backups:

| Backup-Typ | Beschreibung |
|-----------------------------|--|
| Vollständiges Backup | Erstellt ein Backup der gesamten Datenbank, die alle Datendateien, Kontrolldateien und Archivprotokolldateien umfasst. |
| Teilweise Sicherung | Erstellt ein Backup ausgewählter Datendateien, Kontrolldateien, Tablespaces und Archivprotokolldateien |
| Backup nur für Archivierung | Erstellt eine Sicherung nur der Archivprotokolldateien. Sie müssen beim Erstellen des Profils Archivprotokolle separat auswählen. |

Was für ein Datenbankprofil benötigen Sie?

SnapManager erstellt Backups basierend darauf, ob das Datenbankprofil die Archiv-Log-Backups von den Datendatei-Backups trennt.

| Profiltyp | Beschreibung |
|---|--|
| Ein einzelnes Datenbankprofil für eine kombinierte Sicherung von Datendateien und Archivprotokollen | <p>Ermöglicht Ihnen das Erstellen von:</p> <ul style="list-style-type: none"> • Vollständige Sicherung mit allen Datendateien, Archivprotokolldateien und Kontrolldateien • Partielles Backup mit ausgewählten Datendateien, Tablespaces, Archivprotokolldateien und Kontrolldateien |

| Profiltyp | Beschreibung |
|--|---|
| Separate Datenbankprofile für Backups von Archivierungsprotokolldaten und Datendatei-Backups | <p>Ermöglicht Ihnen das Erstellen von:</p> <ul style="list-style-type: none"> • Kombiniertes Backup mit unterschiedlichen Kennungen für Backup von Datendateien und Backup von Archivierungsprotokolldaten • Datendatei-only-Backup aller Datendateien zusammen mit den Kontrolldateien • Partielles, datenonly Backup von ausgewählten Datendateien oder Tablespace zusammen mit den Control Files • Backup nur bei Archivierung und Protokollen |

Welche Namenskonventionen sollten für Snapshot Kopien verwendet werden?

Von Backups erstellte Snapshot Kopien können einer benutzerdefinierten Namenskonvention folgen. Benutzerdefinierte Text oder integrierte Variablen wie der Profilname, der Datenbankname und die von SnapManager bereitgestellte Datenbank-SID können zur Erstellung der Namenskonvention verwendet werden. Sie können die Namenskonvention erstellen, während Sie die Richtlinie erstellen.



Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

Die Namenskonventionen für Snapshot Kopien können während oder nach der Erstellung eines Profils geändert werden. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Vorhandene Snapshot Kopien behalten das vorherige Muster bei.

Wie lange möchten Sie Backup-Kopien auf dem primären Storage-System und dem sekundären Storage-System aufbewahren?

In einer Backup-Aufbewahrungsrichtlinie wird die Anzahl der erfolgreichen Sicherungskopien festgelegt, die aufbewahrt werden sollen. Sie können die Aufbewahrungsrichtlinie angeben, während Sie die Richtlinie erstellen.

Sie können stündlich, täglich, wöchentlich, monatlich oder unbegrenzt als Aufbewahrungsklasse auswählen. Sie können für jede Aufbewahrungsklasse den Aufbewahrungszähler und die Aufbewahrungsdauer entweder gemeinsam oder einzeln festlegen.

- Die Anzahl der Aufbewahrung bestimmt die Mindestanzahl der Backups einer bestimmten Aufbewahrungsklasse, die beibehalten werden soll.

Wenn beispielsweise der Backup-Zeitplan *Daily* lautet und die Anzahl der Aufbewahrung 10 ist, werden 10 tägliche Backups aufbewahrt.



Die maximale Anzahl von Snapshot Kopien, die Sie mit Data ONTAP aufbewahren können, ist 255. Nach Erreichen des maximalen Limits schlägt die Erstellung neuer Snapshot Kopien standardmäßig fehl. Sie können jedoch die Rotationsrichtlinie in Data ONTAP konfigurieren, um ältere Snapshot-Kopien zu löschen.

- Die Aufbewahrungsdauer legt die Mindestanzahl an Tagen fest, für die das Backup aufbewahrt werden soll.

Wenn beispielsweise der Backup-Zeitplan *täglich* lautet und die Aufbewahrungsdauer *10* beträgt, werden täglich 10 Tage Backups aufbewahrt.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.



Zur langfristigen Aufbewahrung von Backup-Kopien sollten Sie SnapVault verwenden.

Möchten Sie Backup-Kopien mithilfe des Quell-Volume oder eines Ziel-Volume überprüfen?

Wenn Sie SnapMirror oder SnapVault einsetzen, können Sie Backup-Kopien mithilfe der Snapshot-Kopie auf dem SnapMirror oder SnapVault Ziel-Volume überprüfen anstelle der Snapshot-Kopie auf dem primären Storage-System. Die Verwendung eines Ziel-Volumes zur Verifizierung reduziert die Last auf dem primären Storage-System.

Verwandte Informationen

["Technischer Bericht 3761: SnapManager für Oracle: Best Practices"](#)

Erstellen eines Profils für Ihre Datenbank

Sie müssen ein Profil erstellen, damit Ihre Datenbank alle Vorgänge in dieser Datenbank ausführen kann. Das Profil enthält Informationen über die Datenbank und kann nur auf eine Datenbank verweisen. Eine Datenbank kann jedoch durch mehrere Profile referenziert werden. Ein Backup, das mit einem Profil erstellt wird, kann nicht von einem anderen Profil aus aufgerufen werden, auch wenn beide Profile mit derselben Datenbank verknüpft sind.

Sie müssen sicherstellen, dass die Details der Zieldatenbank in der Datei `/etc/oratab` enthalten sind.

Mit diesen Schritten wird die Erstellung eines Profils für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es bevorzugen.

Informationen zum Erstellen von Profilen mithilfe der CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie in der Repository-Struktur mit der rechten Maustaste auf das Repository oder den Host und wählen Sie **Profil erstellen** aus.
2. Geben Sie auf der Seite Profilkonfigurationsinformationen den benutzerdefinierten Namen und das Kennwort für das Profil ein.
3. Geben Sie auf der Seite Datenbankkonfigurationsinformationen die folgenden Informationen ein:

| In diesem Feld... | Tun Sie das... |
|----------------------|---|
| Datenbankname | Geben Sie den Namen der Datenbank ein, die Sie sichern möchten. |

| In diesem Feld... | Tun Sie das... |
|--|--|
| <ul style="list-style-type: none"> • Datenbank-SID* | Geben Sie die sichere ID (SID) der Datenbank ein. Der Datenbankname und die Datenbank-SID können identisch sein. |
| Gastgeber | Geben Sie die IP-Adresse des Hosts ein, auf dem sich die Zieldatenbank befindet. Sie können auch den Hostnamen angeben, wenn der Hostname im Domain Name System (DNS) angegeben ist. |
| Host-Konto | Geben Sie den Oracle-Benutzernamen der Zieldatenbank ein. der Standardwert für den Benutzer ist oracle. |
| Host-Gruppe | <p>Geben Sie den Namen der Oracle-Benutzergruppe ein. Der Standardwert ist dba.</p> <p>+</p> |

4. Wählen Sie auf der Seite Datenbankverbindungsinformationen eine der folgenden Optionen aus:

| Wählen Sie diese Option... | Ihr Ziel ist |
|---|--|
| O/S-Authentifizierung verwenden | Verwenden Sie die vom Betriebssystem gepflegten Anmeldeinformationen, um Benutzer zu authentifizieren, die auf die Datenbank zugreifen. |
| Datenbankauthentifizierung Verwenden | <p>Erlauben Sie Oracle, einen administrativen Benutzer mithilfe der Authentifizierung von Kennwortdateien zu authentifizieren. Geben Sie die entsprechenden Informationen zur Datenbankverbindung ein.</p> <ul style="list-style-type: none"> • Geben Sie im Feld SYSDBA Privileged User Name den Namen des Datenbankadministrators mit Administratorrechten ein. • Geben Sie im Feld Passwort das Passwort des Datenbankadministrators ein. • Geben Sie im Feld Port die Portnummer ein, die für die Verbindung mit dem Host verwendet wird, auf dem sich die Datenbank befindet. <p>Der Standardwert ist .</p> |

| Wählen Sie diese Option... | Ihr Ziel ist |
|---|--|
| Verwendung der ASM-Instanz-Authentifizierung | <p>Zulassen, dass die ASM-Datenbankinstanz einen administrativen Benutzer authentifiziert. Geben Sie die entsprechenden Authentifizierungsdaten für die ASM-Instanz ein.</p> <ul style="list-style-type: none"> • Geben Sie im Feld SYSDBA/SYSASM Privileged User Name den Benutzernamen des ASM-Instanzadministrators mit Administratorrechten ein. • Geben Sie im Feld Passwort das Passwort des Administrators ein. |

Hinweis: Sie können den ASM-Authentifizierungsmodus nur auswählen, wenn Sie eine ASM-Instanz auf dem Datenbank-Host haben.

5. Wählen Sie auf der Seite RMAN-Konfigurationsinformationen eine der folgenden Optionen aus:

| Wählen Sie diese Option... | Wenn... |
|--|--|
| Verwenden Sie nicht RMAN | Sie verwenden RMAN nicht für das Management von Backup- und Restore-Vorgängen. |
| Verwenden Sie RMAN über die Steuerdatei | Sie verwalten das RMAN-Repository mit Steuerdateien. |
| Verwenden Sie RMAN über den Wiederherstellungskatalog | <p>Sie verwalten das RMAN-Repository mithilfe der Recovery-Katalogdatenbank. Geben Sie den Benutzernamen ein, der Zugriff auf die Datenbank des Wiederherstellungspatalogs, das Kennwort und den Oracle-Nettodiensnamen der Datenbank hat, die die TNS-Verbindung (Transparent Network Substrat) verwaltet.</p> <p>+</p> |

6. Wählen Sie auf der Seite Snapshot Naming Information die Variablen aus, um ein Benennungsformat für die Snapshot Kopie anzugeben.

Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

7. Führen Sie auf der Seite Richtlinieneinstellungen folgende Schritte durch:

- Geben Sie Anzahl und Dauer der Aufbewahrung für jede Aufbewahrungsklasse ein.
- Wählen Sie aus der Dropdown-Liste **Protection Policy** die Protection Manager-Richtlinie aus.
- Wenn Sie Archivprotokolle separat sichern möchten, aktivieren Sie das Kontrollkästchen **Archivprotokolle separat sichern**, legen Sie die Aufbewahrung fest und wählen Sie die Schutzrichtlinie aus.

Sie können eine Richtlinie auswählen, die sich von der für Datendateien verknüpften Richtlinie unterscheidet. Wenn Sie beispielsweise eine der Protection Manager-Richtlinie für Datendateien ausgewählt haben, können Sie eine andere Protection Manager-Richtlinie für Archivprotokolle auswählen.

8. Geben Sie auf der Seite Benachrichtigungseinstellungen konfigurieren die Einstellungen für E-Mail-Benachrichtigungen an.
9. Wählen Sie auf der Seite Verlaufsdaten-Konfigurationsinformationen eine der Optionen aus, um den Verlauf der SnapManager-Vorgänge beizubehalten.
10. Überprüfen Sie auf der Seite Vorgang „Profil erstellen“ die Informationen und klicken Sie auf **Erstellen**.
11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

["SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"](#)

Sichern Ihrer Datenbank

Nachdem Sie ein Profil erstellt haben, müssen Sie Ihre Datenbank sichern. Sie können wiederkehrende Backups nach der erstmaligen Sicherung und Überprüfung planen.

In diesen Schritten wird gezeigt, wie Sie mithilfe der SnapManager-Benutzeroberfläche ein Backup Ihrer Datenbank erstellen. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden.

Informationen zur Erstellung von Backups mit CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die zu sichernde Datenbank enthält, und wählen Sie **Backup** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherheitsbezeichnung.

Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die `override.default.backup.pattern` und `new.default.backup.pattern` Konfigurationsvariablen bearbeiten, um Ihr eigenes Standard-Backup-Label-Muster zu erstellen.

3. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

4. Führen Sie auf der Seite Datenbank, Tablespaces oder Datendateien zur Datensicherung die folgenden Schritte aus:
 - a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte

Datendateien oder ausgewählte Tabellen zu sichern.

- b. Wählen Sie **Backup Archivelogs** aus, um die Archiv-Log-Dateien separat zu sichern.
- c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.



Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

- d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

- e. Wählen Sie **Jetzt schützen** aus, wenn Sie die Sicherung sofort auf dem sekundären Speicher schützen möchten, der den Schutzzeitplan des Protection Manager überschreibt.
- f. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

Wenn Sie Auto auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

- g. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
 - h. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.
5. Geben Sie auf der Seite Task Enabling an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.
 6. Überprüfen Sie auf der Seite Backup-Vorgang durchführen die Informationen und klicken Sie auf **Backup**.
 7. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Datenbank-Backups werden überprüft

Sie können die Sicherung Ihrer Datenbank überprüfen, um sicherzustellen, dass die gesicherten Dateien nicht beschädigt sind.

Wenn Sie beim Erstellen eines Backups nicht das Kontrollkästchen **Backup überprüfen mit dem Dienstprogramm Oracle DBVERIFY** aktiviert haben, müssen Sie diese Schritte manuell durchführen, um die Sicherung zu überprüfen. Wenn Sie das Kontrollkästchen aktiviert haben, überprüft SnapManager das Backup automatisch.

1. Wählen Sie aus der Struktur **Repositories** das Profil aus.
2. Klicken Sie mit der rechten Maustaste auf das Backup, das Sie überprüfen möchten, und wählen Sie **Überprüfen**.
3. Klicken Sie Auf **Fertig Stellen**.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Klicken Sie im Baum **Repository** mit der rechten Maustaste auf das Backup und klicken Sie dann auf **Eigenschaften**, um die Ergebnisse des Verifizierungsvorgangs anzuzeigen.

Sie können gesicherte Dateien verwenden, um Wiederherstellungsvorgänge durchzuführen. Informationen zur Durchführung von Wiederherstellungsvorgängen über die SnapManager-Benutzeroberfläche (UI) finden Sie in der *Online-Hilfe*. Wenn Sie die Befehlszeilenschnittstelle (CLI) zum Durchführen von Wiederherstellungsvorgängen verwenden möchten, finden Sie im *SnapManager für Oracle – Administratorhandbuch für UNIX*.

Verwandte Informationen

["SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"](#)

Planung wiederkehrender Backups

Sie können Backup-Vorgänge so planen, dass die Backups automatisch in regelmäßigen Abständen initiiert werden. SnapManager ermöglicht die Planung von Backups auf Stundenbasis, täglich, wöchentlich, monatlich oder einmalig.

Sie können mehrere Backup-Zeitpläne für eine einzige Datenbank zuweisen. Wenn Sie jedoch mehrere Backups für dieselbe Datenbank planen, müssen Sie sicherstellen, dass die Backups nicht gleichzeitig geplant sind.

Mit diesen Schritten wird das Erstellen eines Backup-Zeitplans für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche (UI) erläutert. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden. Informationen zum Planen von Backups mithilfe der CLI finden Sie im Administratorhandbuch „*SnapManager für Oracle Administration Guide for UNIX*“.

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die Datenbank enthält, für die Sie einen Backup-Zeitplan erstellen möchten, und wählen Sie **Backup planen** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die Variablen `override.default.backup.pattern` und `new.default.backup.patternconfiguration` bearbeiten, um Ihr eigenes Standard-Backup-Label-Muster zu erstellen.

3. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

4. Führen Sie auf der Seite Datenbank, Tablespaces oder Datendateien zur Datensicherung die folgenden Schritte aus:
 - a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
 - b. Wählen Sie **Backup Archivlogs** aus, um die Archiv-Log-Dateien separat zu sichern.

- c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.



Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

- d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

- e. Wählen Sie **Jetzt schützen** aus, wenn Sie die Sicherung sofort auf dem sekundären Speicher schützen möchten, der den Schutzzeitplan des Protection Manager überschreibt.
- f. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

Wenn Sie Auto auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

- g. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
- h. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.

5. Geben Sie im Feld **Terminplanname** einen benutzerdefinierten Namen des Zeitplans ein.

Sie dürfen keine Leerzeichen in den Namen einfügen.

6. Führen Sie auf der Seite Backup Schedule konfigurieren die folgenden Schritte aus:

- a. Wählen Sie aus der Dropdown-Liste **Durchführung dieser Operation** die Häufigkeit des Backup-Zeitplans aus.
- b. Geben Sie im Feld **Startdatum** das Datum an, an dem Sie den Backup-Zeitplan starten möchten.
- c. Geben Sie im Feld **Startzeit** den Zeitpunkt an, zu dem der Backup-Zeitplan gestartet werden soll.
- d. Geben Sie das Intervall an, in dem Backups erstellt werden sollen.

Wenn Sie beispielsweise die Frequenz als stündlich ausgewählt haben und das Intervall als 2 angeben, werden die Backups alle 2 Stunden geplant.

7. Geben Sie auf der Seite Task Enabling an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.
8. Überprüfen Sie auf der Seite Backup Schedule Operation durchführen die Informationen und klicken Sie auf **Zeitplan**.
9. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

["SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"](#)

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 IRGEND EINER 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.