Oracle Database-Workloads schützen (Preview)

NetApp Backup and Recovery

NetApp
June 02, 2026

Inhalt

Oracle Database-Workloads schützen (Preview) . . . 1
Übersicht über den Schutz von Oracle Database-Workloads . . . 1
Entdecken Sie Oracle-Datenbank-Workloads in NetApp Backup and Recovery . . . 1
Fügen Sie einen Oracle Database-Host hinzu und entdecken Sie Ressourcen . . . 1
Weiter zum NetApp Backup and Recovery Dashboard . . . 3
Konfigurieren einer Oracle-Datenbank in NetApp Backup und Recovery . . . 3
Konfigurieren einer Oracle-Datenbank . . . 3
Erstellen und Verwalten von Schutzgruppen für Oracle-Datenbank-Workloads mit NetApp Backup und Recovery . . . 4
Erstellen einer Schutzgruppe . . . 4
Löschen einer Schutzgruppe . . . 5
Erstellen und Verwalten von Oracle-Datenbank-Backup-Richtlinien in NetApp Backup und Recovery . . . 5
Richtlinien anzeigen . . . 6
Erstellen einer Richtlinie . . . 6
Bearbeiten einer Richtlinie . . . 12
Löschen einer Richtlinie . . . 12
Sichern Sie Oracle-Datenbank-Workloads mit NetApp Backup und Recovery . . . 13
Sichern Sie Schutzgruppen jetzt mit einem On-Demand-Backup . . . 13
Sichern Sie jetzt eine Datenbank mit einem On-Demand-Backup . . . 14
Oracle-Datenbank-Workloads mithilfe von NetApp Backup and Recovery klonen . . . 14
Erstellen Sie einen Klon einer Oracle-Datenbank . . . 14
Planen Sie das Klonen einer Oracle-Datenbank . . . 15
Einen Klon teilen . . . 16
Löschen eines Klons . . . 16
Stellen Sie Oracle-Datenbanken mit NetApp Backup and Recovery wieder her . . . 17
So funktioniert die Wiederherstellung von Oracle-Datenbanken . . . 17
Wiederherstellen einer Oracle-Datenbank . . . 17
Oracle Database-Wiederherstellungspunkte mit NetApp Backup und Recovery einbinden, aushängen und katalogisieren . . . 19
Einen Oracle-Datenbank-Recovery-Punkt einbinden . . . 19
Einen Wiederherstellungspunkt einer Oracle-Datenbank aushängen . . . 20
Katalogisieren Sie einen Wiederherstellungspunkt einer Oracle-Datenbank . . . 21

Oracle Database-Workloads schützen (Preview)

Übersicht über den Schutz von Oracle Database-Workloads

Schützen Sie Oracle-Datenbanken und -Protokolle mit NetApp Backup und Recovery. Erhalten Sie schnelle, platzsparende, absturzkonsistente und datenbankkonsistente Backups und Wiederherstellungen. Sichern Sie Oracle Database-Workloads in AWS S3, NetApp StorageGRID, Azure Blob Storage oder ONTAP S3. Stellen Sie Backups auf einem lokalen Oracle-Host wieder her.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Schutzstrategie zu implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Speichersystemen sowie 1 Kopie in der Cloud haben. Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Sie können NetApp Backup und Recovery verwenden, um die folgenden Aufgaben im Zusammenhang mit Oracle Database-Workloads durchzuführen:

- "Oracle Database-Workloads entdecken"
- "Erstellen und Verwalten von Schutzgruppen für Oracle Database-Workloads"
- "Oracle-Datenbank-Workloads sichern"
- "Oracle-Datenbank-Workloads wiederherstellen"

Entdecken Sie Oracle-Datenbank-Workloads in NetApp Backup and Recovery

Die Erkennung von Oracle-Datenbanken ermöglicht es NetApp Backup and Recovery, diese durch das Erstellen und Wiederherstellen von Backups und Snapshots zu schützen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Fügen Sie einen Oracle Database-Host hinzu und entdecken Sie Ressourcen

Fügen Sie Oracle-Hostinformationen hinzu und lassen Sie NetApp Backup and Recovery die Workloads erkennen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.

2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Ressourcen entdecken**.
4. Wählen Sie **Oracle** für das Feld **Workload type** aus.
5. Wenn Sie noch keine Anmeldeinformationen für diesen Oracle Database-Host gespeichert haben, wählen Sie **Add credentials**.
   a. Wählen Sie den Konsolenagenten aus, der mit diesem Host verwendet werden soll.
   b. Geben Sie einen Namen für diese Anmeldeinformationen ein.
   c. Geben Sie den Benutzernamen und das Kennwort für das Konto ein.
   d. Wählen Sie **Fertig**.
6. **Hostregistrierung**: Fügen Sie einen neuen Oracle Database Host hinzu. Geben Sie im Feld **Host-FQDN oder IP-Adresse** den FQDN oder die IP-Adresse des Hosts ein – bei Clusterdatenbanken können Sie den FQDN oder die IP-Adresse eines beliebigen Knotens im Cluster eingeben. Geben Sie anschließend die Anmeldeinformationen, den Console Agent und die Portnummer an.
7. (Optional) Wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer auswählen, führen Sie Folgendes aus:
   a. Anweisungen zum Hinzufügen des von Ihnen ausgewählten Nicht-Root-Benutzers zur sudoers-Datei auf dem Oracle Database-Host finden Sie unter **Configure sudoers**.
   b. Folgen Sie den Anweisungen im Dialog, aktivieren Sie das Kontrollkästchen, wenn Sie fertig sind, und wählen Sie **Fertig**.
8. **Erweiterte Einstellungen**: Führen Sie Folgendes aus:
   a. Geben Sie den Port und den Installationspfad für das NetApp Plug-in ein. Das Plug-in ermöglicht die Kommunikation zwischen dem Oracle-Datenbankhost und NetApp Backup and Recovery.
   b. Wählen Sie, ob NetApp Backup und Recovery das Plug-in automatisch auf jedem Host installieren oder die automatische Plug-in-Installation für alle Hosts überspringen soll. Wählen Sie **Anleitung anzeigen**, um Anweisungen zur manuellen Installation zu erhalten.

      Backup und Recovery verbindet sich per SSH mit jedem Host, um das Plug-in automatisch zu installieren. Aktivieren Sie die Option **manuelle Installation verwenden**, wenn einer der folgenden Punkte zutrifft:

      - Auf einem oder mehreren Hosts läuft der SSH-Dienst nicht.
      - Auf jedem Host ist das NetApp Plug-in bereits vorhanden (auch wenn es nur auf einigen Cluster-Mitgliedern vorhanden ist).
      - Sie bevorzugen es, das Plug-in auf jedem Host manuell zu installieren.

   c. Wenn der Datenbankhost in einem Cluster organisiert ist, aktivieren Sie die Option **Alle Hosts im Cluster hinzufügen**, um alle Hosts im Cluster zu ermitteln.
   d. Wählen Sie, ob vor der automatischen Installation des Plug-ins auf jedem Host Vorabprüfungen durchgeführt werden sollen. Schlagen die Prüfungen fehl, wird die automatische Plug-in-Installation gestoppt. Um die Prüfungen zu umgehen und das Plug-in trotzdem zu installieren, aktivieren Sie **Optionale Vorabprüfungen überspringen** (automatisch aktiviert, wenn Sie die manuelle Installation wählen).
9. Wählen Sie **Entdecken**.

Das Hinzufügen von Ressourcen kann einige Minuten dauern. Um den Fortschritt zu sehen, wählen Sie **Fortschritt verfolgen** im Statusdialog unten auf der Inventarseite oder wählen Sie **Überwachung** im Menü auf der linken Seite.

Ergebnis

Die Oracle Database-Workload wird in der Liste der Workloads auf der Inventarseite angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

1. Wählen Sie im NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie eine Workload-Kachel aus (z. B. Microsoft SQL Server).
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Dashboard“ aus.
4. Überprüfen Sie den Zustand des Datenschutzes. Die Anzahl der gefährdeten oder geschützten Workloads steigt basierend auf den neu entdeckten, geschützten und gesicherten Workloads.

Konfigurieren einer Oracle-Datenbank in NetApp Backup und Recovery

Sie können Authentifizierung und Knoteneinstellungen für eine neue eigenständige oder geclusterte Oracle-Datenbank ändern. NetApp Backup und Recovery schützt Datenbanken ohne diese Änderungen. Wenn sich Ihre Umgebung nach der Erkennung ändert, müssen Sie möglicherweise die Datenbankeinstellungen aktualisieren.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Konfigurieren einer Oracle-Datenbank

Ändern Sie die Konfiguration für eine eigenständige oder geclusterte Oracle-Datenbank.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie im Oracle-Inventar das Menü **Datenbanken** aus.
4. Wählen Sie in der Liste der Datenbanken entweder **Datenbank konfigurieren** (eigenständige Datenbank) oder **RAC-Datenbank konfigurieren** (Clusterdatenbank) für die Datenbank aus, die Sie konfigurieren möchten.
5. **Datenbankeinstellungen konfigurieren**: Konfigurieren Sie die Authentifizierungseinstellungen für die eigenständige oder die Cluster-Datenbank.
    - Wählen Sie **OS-Authentifizierung**, um sich nur beim Host-Betriebssystem zu authentifizieren. Backup und Recovery verwendet die Host-Anmeldeinformationen, die Sie während der Erkennung angegeben haben.
    - Wählen Sie **Database authentication**, wenn die Datenbank Anmeldeinformationen erfordert. Wählen Sie anschließend vorhandene Anmeldeinformationen aus oder fügen Sie neue hinzu und wählen Sie den Port für die Verbindung.

6. **RMAN-Katalog konfigurieren**: Wählen Sie aus, wo Metadaten für Backup- und Recovery-Vorgänge für diese Datenbank oder diesen Cluster gespeichert werden, wenn die automatische Katalogisierung in der Datensicherungsstrategie aktiviert ist oder wenn Sie einen Wiederherstellungspunkt manuell katalogisieren:
    - Wählen Sie **Target control file** aus, um Metadaten in der Datenbank-Kontrolldatei zu speichern.
    - Wählen Sie **Katalogdatenbank** aus, um Metadaten im RMAN-Wiederherstellungskatalog zu speichern. Wählen Sie die Anmeldeinformationen und den Transparent Network Substrate (TNS)-Namen aus, um eine Verbindung zum Wiederherstellungskatalog herzustellen.

      Der RMAN-Wiederherstellungskatalog ist ein separates Datenbankschema, das vom RMAN-Dienstprogramm verwendet wird, um Metadaten zu Sicherungs- und Wiederherstellungsvorgängen registrierter Datenbanken zu speichern. Er bietet Redundanz und langfristige Aufbewahrung für den Fall, dass die Kontrolldatei verloren geht oder historische Daten benötigt werden. Aktivieren Sie diese Option, um Datendateien und Archivprotokollkopien im RMAN-Repository zu registrieren, sodass RMAN diese Kopien für Berichterstellung und Wiederherstellung nachverfolgen und verwalten kann.
7. **Knoten konfigurieren** (nur für Clusterdatenbanken): Knoten zum Schutz hinzufügen oder entfernen oder die Knotenpriorität mithilfe der Pfeiltasten ändern.

   Knoten mit höherer Priorität werden zuerst geschützt. Knoten mit niedrigerer Priorität werden nur dann geschützt, wenn Knoten mit höherer Priorität nicht erreichbar oder fehlerhaft sind.
8. Wenn Sie fertig sind, wählen Sie **Fertig**.

Ergebnis

Backup und Recovery stellt mit den neuen Einstellungen eine Verbindung zur Datenbank her.

Erstellen und Verwalten von Schutzgruppen für Oracle-Datenbank-Workloads mit NetApp Backup und Recovery

Erstellen Sie Schutzgruppen, um die Sicherungsvorgänge für eine Reihe von Oracle Database-Ressourcen zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie Datenbanken, die Sie gemeinsam schützen möchten. Sie müssen eine Schutzgruppe erstellen, um Oracle-Datenbanken zu sichern.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe.
- Schutzdetails anzeigen.
- Sichern Sie jetzt eine Schutzgruppe. Siehe "Sichern Sie jetzt Oracle Database Workloads".
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie VMs und Speicherpools, die Sie gemeinsam schützen möchten, in einer Schutzgruppe.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Backupadministratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die VMs oder Speicherpools aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.

   Wenn Sie eine Richtlinie erstellen möchten, wählen Sie **Neue Richtlinie erstellen** und folgen Sie den Anweisungen zum Erstellen einer Richtlinie. Sehen"Erstellen von Richtlinien" für weitere Informationen.

10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Löschen einer Schutzgruppe

Durch das Löschen einer Schutzgruppe werden diese und alle zugehörigen Sicherungszeitpläne entfernt. Möglicherweise möchten Sie eine Schutzgruppe löschen, wenn sie nicht mehr benötigt wird.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie löschen möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Schutz entfernen**.
7. Überprüfen Sie die Bestätigungsmeldung zum Löschen der zugehörigen Sicherungen und bestätigen Sie den Löschvorgang.

Erstellen und Verwalten von Oracle-Datenbank-Backup-Richtlinien in NetApp Backup und Recovery

In NetApp Backup und Recovery können Sie eigene Oracle Database-Backup-Richtlinien erstellen, die die Backup-Häufigkeit, den Zeitpunkt der Backup-Erstellung und die Anzahl der aufzubewahrenden Backup-Dateien regeln.

Einige dieser Optionen und Konfigurationsabschnitte sind nicht für alle Workloads verfügbar.

Wenn Sie Ressourcen aus SnapCenter importieren, können Sie auf Unterschiede zwischen den in SnapCenter und den in NetApp Backup and Recovery verwendeten Richtlinien stoßen. Sehen"Richtlinienunterschiede

zwischen SnapCenter und NetApp Backup and Recovery" .

Sie können die folgenden Ziele im Zusammenhang mit Richtlinien erreichen:

- Erstellen einer lokalen Snapshot-Richtlinie
- Erstellen einer Richtlinie für die Replikation auf sekundären Speicher
- Erstellen einer Richtlinie für Objektspeichereinstellungen
- Konfigurieren erweiterter Richtlinieneinstellungen
- Richtlinien bearbeiten (nicht verfügbar für VMware workloads)
- Richtlinien löschen

Richtlinien anzeigen

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Überprüfen Sie die Richtliniendetails. Zum Beispiel:
    - **Workload**: Beispiele sind Microsoft SQL Server, ONTAP Volumes, VMware, KVM, Hyper-V, Oracle Database oder Kubernetes.
    - **Sicherungstyp**: Beispiele sind vollständige Sicherung und Protokollsicherung.
    - **Architektur**: Beispiele hierfür sind lokaler Snapshot, Fan-Out, Kaskadierung, Disk-to-Disk und Disk-to-Object-Store.
    - **Geschützte Ressourcen**: Zeigt an, wie viele Ressourcen der Gesamtressourcen dieser Arbeitslast geschützt sind.
    - **Ransomware-Schutz**: Zeigt an, ob die Richtlinie eine Snapshot-Sperre für den lokalen Snapshot, eine Snapshot-Sperre für den sekundären Speicher oder eine DataLock-Sperre für den Objektspeicher umfasst.

Erstellen einer Richtlinie

Sie können Richtlinien erstellen, die Ihre lokalen Snapshots, Replikationen auf sekundären Speicher und Backups auf Objektspeicher regeln. Ein Teil Ihrer 3-2-1-Strategie besteht darin, einen Snapshot der Instanzen, Datenbanken, Anwendungen oder VMs auf dem **primären** Speichersystem zu erstellen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Backupadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Bevor Sie beginnen

Wenn Sie eine Replikation auf einen sekundären Speicher planen und die Snapshot-Sperre auf lokalen Snapshots oder auf einem Remote ONTAP Sekundärspeicher verwenden möchten, müssen Sie zunächst die ONTAP Compliance-Uhr auf Clusterebene initialisieren. Dies ist eine Voraussetzung zum Aktivieren der Snapshot-Sperre in der Richtlinie.

Anweisungen hierzu finden Sie unter "Initialisieren Sie die Compliance-Uhr in ONTAP" .

Allgemeine Informationen zum Sperren von Snapshots finden Sie unter "Snapshot-Sperre in ONTAP" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.

2. Wählen Sie auf der Seite „Richtlinien“ die Option „Neue Richtlinie erstellen“ aus.

   Die Seite „Richtlinien“ wird angezeigt.

3. Geben Sie im Abschnitt **Details** Informationen ein:
   - Arbeitslasttyp: Wählen Sie **Oracle Database**.
   - Geben Sie einen Richtliniennamen ein.
   - Wählen Sie einen Konsolenagenten aus der Liste **Agent** aus.
4. Geben Sie im Abschnitt **Backup-Architektur** Informationen ein. Wählen Sie den Datenfluss für das Backup aus der Liste aus:
   - **3-2-1-Fanout**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) zu Cloud (Objektspeicher). Erstellt mehrere Kopien von Daten auf verschiedenen Speichersystemen, wie ONTAP zu ONTAP und ONTAP zu Objektspeicher-Konfigurationen. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher sein. Am besten geeignet für optimale Datensicherung und Disaster Recovery. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **3-2-1-Kaskade**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) und Primärspeicher (Festplatte) zu Cloud-Speicher (Objektspeicher). Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher wie StorageGRID sein. Dadurch entsteht eine Kette der Datenreplizierung über mehrere Systeme hinweg, um Redundanz und Zuverlässigkeit zu gewährleisten. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **Festplatte zu Festplatte**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte). Die ONTAP zu ONTAP Datensicherungsstrategie repliziert Daten zwischen zwei ONTAP Systemen, um hohe Verfügbarkeit und Disaster Recovery zu gewährleisten. Dies wird typischerweise mithilfe von SnapMirror erreicht, das sowohl synchron als auch asynchrone Replizierung unterstützt. Diese Methode hält Ihre Daten standortübergreifend aktuell und verfügbar für eine starke Datensicherung.
   - **Disk-to-object storage**: Primärspeicher (Festplatte) zu Cloud (Objektspeicher). Dabei werden Daten von einem ONTAP System zu einem Objektspeichersystem repliziert. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher wie StorageGRID sein. Diese Methode ist ideal für die langfristige Datenaufbewahrung und Archivierung. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **Disk-to-Disk-Fanout**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) und Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte). Sie können mehrere sekundäre Einstellungen für die Disk-to-Disk-Fanout-Option konfigurieren.
   - **Lokale Snapshots**: Lokaler Snapshot des ausgewählten Volumes. Dadurch werden schreibgeschützte, zeitpunktgenaue Kopien der Produktionsvolumes erstellt, auf denen Ihre Workloads ausgeführt werden. Sie können lokale Snapshots verwenden, um Datenverlust oder -beschädigung zu beheben sowie um Backups für die Notfallwiederherstellung zu erstellen.
5. Geben Sie Informationen für den Abschnitt **Lokale Snapshot-Einstellungen** an:
   - Wählen Sie die Option **Zeitplan hinzufügen**, um den oder die Snapshot-Zeitpläne auszuwählen. Sie können maximal 5 Zeitpläne haben.
   - **Schnappschusshäufigkeit**: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich. Die jährliche Häufigkeit ist für Kubernetes-Workloads nicht verfügbar.
   - **Aufbewahrung von Snapshots**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
   - **Protokollsicherung aktivieren**: Aktivieren Sie diese Option, um Protokolle zu sichern und die Häufigkeit und Aufbewahrungsdauer der Protokollsicherungen festzulegen. Hierfür müssen Sie bereits eine Protokollsicherung konfiguriert haben. Siehe "Konfigurieren von Protokollverzeichnissen".
     - **Archivprotokolle nach der Sicherung löschen**: Wenn die Sicherung von Protokollen aktiviert ist,

können Sie diese Funktion optional aktivieren, um die Aufbewahrungsdauer der Oracle-Archivprotokolle durch Backup and Recovery zu begrenzen. Sie können die Aufbewahrungsdauer sowie den Ort festlegen, an dem Backup and Recovery die Archivprotokolle löschen soll.

6. Geben Sie Informationen für den Abschnitt **Sekundäre Einstellungen** (Replikation auf Sekundärspeicher) an:
   - **Sicherung**: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich.
   - **Sicherungsziel**: Wählen Sie das Zielsystem auf dem Sekundärspeicher für die Sicherung aus.
   - **Aufbewahrung**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
   - **Snapshot-Sperre aktivieren**: Wählen Sie aus, ob Sie manipulationssichere Snapshots aktivieren möchten.
   - **Sperrzeitraum für Snapshots**: Geben Sie die Anzahl der Tage, Monate oder Jahre ein, für die Sie den Snapshot sperren möchten.
   - **Wechsel zur weiterführenden Schule**:
     - Die Option * ONTAP Übertragungsplan – Inline* ist standardmäßig ausgewählt und gibt an, dass Snapshots sofort auf das sekundäre Speichersystem übertragen werden. Sie müssen die Sicherung nicht planen.
     - Weitere Optionen: Wenn Sie eine aufgeschobene Überweisung wählen, erfolgen die Überweisungen nicht sofort und Sie können einen Zeitplan festlegen.
   - * Sekundäre Beziehung zwischen SnapMirror und SnapVault SMAS*: Verwenden Sie sekundäre Beziehungen zwischen SnapMirror und SnapVault SMAS für SQL Server-Workloads.
7. Geben Sie Informationen für den Abschnitt **Objektspeichereinstellungen** (Sicherung im Objektspeicher) an:

   Die angezeigten Felder unterscheiden sich je nach ausgewähltem Anbieter und Architektur.

   - **Anbieter**: Wählen Sie den Anbieter für Ihren Objektspeicher und geben Sie die Anmeldeinformationen in die entsprechenden Felder ein (die Felder für die Anmeldeinformationen unterscheiden sich je nach Anbieter).
   - **Sicherungsziel**: Wählen Sie ein registriertes Objektspeicherziel aus. Stellen Sie sicher, dass das Ziel in Ihrer Sicherungsumgebung zugänglich ist.
   - **IPspace**: Wählen Sie den IPspace aus, der für die Sicherungsvorgänge verwendet werden soll. Dies ist nützlich, wenn Sie über mehrere IP-Bereiche verfügen und steuern möchten, welcher für Sicherungen verwendet wird.
   - **Zeitplaneinstellungen**: Wählen Sie den Zeitplan aus, der für die lokalen Snapshots festgelegt wurde. Sie können einen Zeitplan entfernen, aber keinen hinzufügen, da die Zeitpläne entsprechend den lokalen Snapshot-Zeitplänen festgelegt werden.
   - **Aufbewahrungskopien**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
   - **Ausführen um**: Wählen Sie den ONTAP Übertragungszeitplan zum Sichern von Daten im Objektspeicher.
   - **Stufen Sie Ihre Backups vom Objektspeicher in den Archivspeicher auf**: Wenn Sie Backups in den Archivspeicher (z. B. AWS Glacier) aufstufen möchten, wählen Sie die Stufenoption und die Anzahl der Tage für die Archivierung aus.
   - **Integritätsprüfung aktivieren**: Wählen Sie aus, ob Sie Integritätsprüfungen (Snapshot-Sperrung) für den Objektspeicher aktivieren möchten. Dadurch wird sichergestellt, dass Ihre Backups gültig und wiederherstellbar sind. Die Integritätsprüfung erfolgt standardmäßig alle 7 Tage. Um Ihre Backups vor Änderungen oder Löschung zu schützen, wählen Sie die Option **Integritätsprüfung**. Die Prüfung wird

nur für den neuesten Snapshot durchgeführt. Sie können Integritätsprüfungen für den neuesten Snapshot aktivieren oder deaktivieren.

Konfigurieren Sie erweiterte Einstellungen in der Richtlinie

Sie können optional erweiterte Einstellungen in der Richtlinie konfigurieren. Diese Optionen stehen Ihnen für alle Backup-Architekturen und Speicherziele zur Verfügung. Die verfügbaren erweiterten Optionen hängen von der oben auf der Seite ausgewählten Arbeitslast ab, daher treffen einige der hier beschriebenen Optionen möglicherweise nicht auf alle Arbeitslasten zu.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Wählen Sie auf der Seite „Richtlinien“ die Option „Neue Richtlinie erstellen“ aus.
3. Wählen Sie im Abschnitt „Richtlinie > Erweitert*-Einstellungen“ das Menü „Erweiterte Aktion auswählen*, um aus einer Liste erweiterter Einstellungen auszuwählen.
4. Aktivieren Sie alle Einstellungen, die Sie anzeigen oder ändern möchten, und wählen Sie dann **Akzeptieren**.
5. Geben Sie die folgenden Informationen an:
   - **RMAN-Katalogeinstellungen**: Aktivieren Sie die Option **Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren**, um Metadaten für Oracle Datenbank-Backup und Recovery-Vorgänge automatisch zu katalogisieren. Die Metadaten werden gemäß den von Ihnen gewählten **RMAN-Katalog konfigurieren**-Einstellungen für die Datenbank gespeichert (standardmäßig in der Ziel-Kontrolldatei). Siehe "Konfigurieren einer Oracle-Datenbank" zum Ändern dieser Einstellungen für eine Datenbank.
   - **Backup-Überprüfung**: Wählen Sie aus, ob Sie die Backup-Überprüfung aktivieren und ob diese sofort oder später erfolgen soll. Diese Funktion stellt sicher, dass die Backups gültig sind und erfolgreich wiederhergestellt werden können. Wir empfehlen, diese Option zu aktivieren, um die Integrität Ihrer Backups zu gewährleisten. Standardmäßig wird die Backup-Überprüfung vom Sekundärspeicher ausgeführt, sofern der Sekundärspeicher konfiguriert ist. Wenn kein Sekundärspeicher konfiguriert ist, wird die Backup-Überprüfung vom Primärspeicher ausgeführt.

     Konfigurieren Sie zusätzlich die folgenden Optionen:

     - Wählen Sie den Zeitpunkt für die Backup-Überprüfung aus:
       - **Sofort**: Führt die Überprüfung als letzten Schritt jedes Sicherungsauftrags durch. Verwenden Sie diese Option, um jede Sicherung direkt nach ihrer Erstellung zu validieren. Beachten Sie, dass dies den Zeit- und Ressourcenverbrauch des Sicherungsfensters erhöht.
       - **Später**: Führt die Überprüfung nach einem von Ihnen festgelegten Zeitplan unabhängig vom Sicherungsauftrag durch. Verwenden Sie dies, um Sicherungsfenster kurz zu halten, indem Sie die Überprüfungen außerhalb der Geschäftszeiten ausführen, oder um nur bestimmte Ebenen zu überprüfen (zum Beispiel wöchentlich und monatlich, aber nicht täglich).
     - **Überprüfung auf sekundärem Speicher**: Aktivieren Sie diese Option, um die sekundäre (replizierte) Kopie des Backups anstelle der primären Kopie zu überprüfen. Dies ist hilfreich, wenn Sie bestätigen möchten, dass die Offsite-Kopie wiederherstellbar ist oder die I/O-Last auf dem primären Storage reduzieren möchten.

       Diese Option wird automatisch deaktiviert, wenn diese Richtlinie **Lokale Snapshots** oder **Disk to object storage** verwendet, da keine dieser Backup-Architekturen über eine sekundäre Ebene verfügt.

     - **Backup-Bezeichnungen**: Wählen Sie in Ihrer Richtlinie eine Backup-Ebene aus, deren Backups überprüft werden sollen. Abhängig von Ihrer Einstellung **Überprüfung auf**

sekundärem Server stammt die Ebenenliste entweder aus Ihrem primären oder sekundären Zeitplan. Stündliche und Protokoll-Backups werden nicht angezeigt, da sie nicht für die Überprüfung in Frage kommen.

- **Überprüfungszeitpläne**: Wenn Sie **Später** als Backup-Überprüfung gewählt haben, wählen Sie für jede von Ihnen gewählte Backup-Bezeichnung (Ebene) die Häufigkeit der Backup-Überprüfung aus.

- **Verifizierungsserver**: Optional können Sie einen oder mehrere registrierte Oracle-Hosts aus der Liste als externe Verifizierungsserver auswählen. Wenn kein Server ausgewählt ist, wird die Verifizierung direkt auf dem Quell-Datenbank-Host ausgeführt. Andernfalls bindet Backup and Recovery den Snapshot-Klon auf einem der ausgewählten Hosts ein und verifiziert das Backup dort, wodurch die Verifizierungs-I/O vom Produktionsdatenbank-Server isoliert wird. Ein Verifizierungsserver muss:
  - Haben Sie das NetApp Plug-in installiert
  - Die Oracle-Datenbank-Binärdateien müssen installiert sein.
  - Verwenden Sie dieselbe Oracle-Datenbankversion wie die Quelldatenbank
  - Netzwerkzugriff auf den Speicher mit dem Snapshot haben (primär oder sekundär)
  - Sie müssen in der Lage sein, das geklonte Volume einzubinden und das Oracle Database DBVERIFY-Dienstprogramm auszuführen.

◦ **SnapMirror Volume- und Snapshot-Format**: Wählen Sie aus den folgenden Optionen:

- **Benutzerdefiniertes Namensformat für Snapshot-Kopien verwenden**: Wählen Sie ein Namensschema für Snapshots. Wenn Sie dieses Feld leer lassen, wird jedem Snapshot-Namen ein Zeitstempel hinzugefügt.
- **SnapMirror-Volume-Format angeben**: Geben Sie ein Präfix, ein Suffix oder beides an, um den Standard-SnapMirror-Volume-Namen zu ändern. Standardmäßig übernimmt ein SnapMirror-Volume den Namen des Quell-Volumes.

◦ **Maximale Transferrate**: Aktivieren Sie die Option **Maximale Transferrate aktivieren**, um eine maximale Transferrate für ausgewählte Hosts festzulegen. Um kein Limit für die Bandbreitennutzung festzulegen, wählen Sie **Unbegrenzt**. Wenn Sie die Transferrate begrenzen möchten, wählen Sie **Begrenzt** und wählen Sie die Netzwerkbandbreite zwischen 1 und 1.000 Mbps, die für das Hochladen von Backups in den Objektspeicher zugewiesen wird. Standardmäßig kann ONTAP eine unbegrenzte Menge an Bandbreite verwenden, um die Backup-Daten von Volumes im System in den Objektspeicher zu übertragen. Wenn der Backup-Datenverkehr die Workloads beeinträchtigt, reduzieren Sie die Netzwerkbandbreite für Übertragungen.

◦ **Wiederholungsversuche für Backups**: Um den Auftrag im Fehlerfall oder bei einer Unterbrechung zu wiederholen, wählen Sie **Wiederholungsversuche bei Fehlern aktivieren**. Geben Sie die maximale Anzahl an Wiederholungsversuchen für Snapshot- und Backup-Aufträge sowie das Wiederholungsintervall ein. Die Anzahl der Wiederholungsversuche muss weniger als 10 betragen.

Wenn die Snapshot-Frequenz auf 1 Stunde eingestellt ist, sollte die maximale Verzögerung zusammen mit der Anzahl der Wiederholungsversuche 45 Minuten nicht überschreiten.

◦ **Ransomware-Scan**: Wählen Sie, ob Sie den Ransomware-Scan für jeden Bucket aktivieren möchten. Dies erfordert DataLock-Sperrung auf dem Objektspeicher. Geben Sie die Scanfrequenz in Tagen an. Diese Option gilt für AWS- und Microsoft Azure-Objektspeicher und kann je nach Cloud-Anbieter zusätzliche Kosten verursachen.

- **Benachrichtigung**: Wählen Sie aus, ob E-Mail-Benachrichtigungen für Backup-Vorgänge aktiviert werden sollen. Sie können auswählen, welche Ereignisse eine Benachrichtigung auslösen – zum Beispiel, wenn ein Backup erfolgreich ist, fehlschlägt oder mit Warnungen abgeschlossen wird.

Bearbeiten einer Richtlinie

Sie können die Backup-Architektur, die Backup-Frequenz, die Aufbewahrungsrichtlinie und weitere Einstellungen einer Richtlinie bearbeiten. Für Kubernetes-Workload-Richtlinien können Sie nur die Zeitplan- und Aufbewahrungseinstellungen bearbeiten.

Sie können beim Bearbeiten einer Richtlinie eine weitere Schutzebene hinzufügen, aber keine Schutzebene entfernen. Wenn die Richtlinie beispielsweise nur lokale Snapshots schützt, können Sie die Replikation zum sekundären Speicher oder die Backups zum Objektspeicher hinzufügen. Wenn Sie über lokale Snapshots und Replikation verfügen, können Sie Objektspeicher hinzufügen. Wenn Sie jedoch über lokale Snapshots, Replikation und Objektspeicher verfügen, können Sie keine dieser Ebenen entfernen.

Wenn Sie eine Richtlinie bearbeiten, die eine Sicherung im Objektspeicher vornimmt, können Sie die Archivierung aktivieren.

Wenn Sie Ressourcen aus SnapCenter importiert haben, stoßen Sie möglicherweise auf einige Unterschiede zwischen den in SnapCenter und NetApp Backup and Recovery verwendeten Richtlinien. Sehen"Richtlinienunterschiede zwischen SnapCenter und NetApp Backup and Recovery" .

Erforderliche NetApp Console

Superadministrator für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Gehen Sie in der NetApp Console zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Option **Richtlinien**.
3. Wählen Sie die Richtlinie aus, die Sie bearbeiten möchten.
4. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Bearbeiten**.

Löschen einer Richtlinie

Sie können eine Richtlinie löschen, wenn Sie sie nicht mehr benötigen.

Sie können keine Richtlinie löschen, die einer Arbeitslast zugeordnet ist.

Schritte

1. Gehen Sie in der Konsole zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Option **Richtlinien**.
3. Wählen Sie die Richtlinie aus, die Sie löschen möchten.
4. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Löschen**.
5. Bestätigen Sie die Aktion und wählen Sie **Löschen**.

Sichern Sie Oracle-Datenbank-Workloads mit NetApp Backup und Recovery

Verwenden Sie NetApp Backup and Recovery , um Oracle Database-Schutzgruppen oder Datenbanken von lokalen ONTAP -Systemen in Cloud-Speicher zu sichern, einschließlich Amazon S3, NetApp StorageGRID, Microsoft Azure Blob Storage oder ONTAP S3. NetApp Backup and Recovery sichert Datenbanken und Protokolldaten in jeder Schutzgruppe.

Um Schutzgruppen oder einzelne Datenbanken nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die Sicherungs- und Wiederherstellungsvorgänge verwalten. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.

- Erstellen Sie Schutzgruppen, um die Backup- und Recovery-Vorgänge für eine Gruppe von Ressourcen zu verwalten. Siehe "Erstellen und Verwalten von Schutzgruppen für Oracle-Datenbank-Workloads mit NetApp Backup und Recovery" für weitere Informationen.
- Sichern Sie jetzt eine Schutzgruppe (erstellen Sie jetzt ein On-Demand-Backup).
- Sichern Sie jetzt eine Datenbank.

Sichern Sie Schutzgruppen jetzt mit einem On-Demand-Backup

Führen Sie vor Systemänderungen eine On-Demand-Sicherung durch, um sicherzustellen, dass Ihre Daten geschützt sind.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Backupadministratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Inventar**.
4. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
5. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
6. Wählen Sie die Registerkarte **Schutzgruppen**, **Datenspeicher** oder **Virtuelle Maschinen**.
7. Wählen Sie die Schutzgruppe aus, die Sie sichern möchten.
8. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

   NetApp Backup and Recovery verwendet für die Sicherungs- und die Schutzgruppe dieselbe Richtlinie.

9. Wählen Sie die Zeitplanstufe aus.
10. Wählen Sie **Sichern**.

Sichern Sie jetzt eine Datenbank mit einem On-Demand-Backup

Sie können bei Bedarf eine Sicherung einer einzelnen Datenbank ausführen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Backupadministratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Inventar**.
4. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
5. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
6. Wählen Sie die Registerkarte **Datenbanken**.
7. Wählen Sie die Datenbank aus, die Sie sichern möchten.
8. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.
9. Wählen Sie die Zeitplanstufe aus.
10. Wählen Sie **Sichern**.

Oracle-Datenbank-Workloads mithilfe von NetApp Backup and Recovery klonen

Verwenden Sie NetApp Backup and Recovery, um beschreibbare Klone von Oracle-Datenbanken von lokalen ONTAP-Systemen auf primären oder sekundären Speicher zu erstellen. Verwalten Sie den Lebenszyklus der Klone, sodass sie regelmäßig gemäß einem Zeitplan aktualisiert werden.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Backupadministratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Erstellen Sie einen Klon einer Oracle-Datenbank

Erstellen Sie sofort einen Klon aus einem vorhandenen Snapshot. Verwenden Sie diese Methode, um einen einmaligen Klon zu erstellen, der nicht kontinuierlich aus einem Snapshot aktualisiert wird.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Clone** aus.
4. Wählen Sie **Neuen Klon erstellen**.
5. Wählen Sie im Abschnitt **Datenbankquelle** den Quellhost und die Datenbank aus den Listen aus.
6. Im Abschnitt **Zieldatenbank** wählen Sie den Zielhost und die Datenbank aus den Listen aus. Der Zielhost und die Datenbank können sich vom Quellhost unterscheiden.

7. Wählen Sie **Weiter**.
8. Im Abschnitt **Klonen von** auf der Seite **Wiederherstellungspunkt auswählen** wählen Sie **Vorhandene Snapshots**.
9. Wählen Sie einen vorhandenen Snapshot (Wiederherstellungspunkt) aus der Liste aus, um ihn als Basis für den Klon zu verwenden, und wählen Sie **Weiter**.

   Die Option **Speicherort für Snapshots auswählen** erscheint, wenn der Snapshot an mehr als einem Speicherort gespeichert ist.
10. Wählen Sie den Snapshot-Speicherort aus und wählen Sie **Weiter**.
11. Führen Sie auf der Seite **Erweiterte Optionen** Folgendes aus:
    a. Wenn Sie zuvor eine Spezifikationsdatei gespeichert haben, können Sie diese hochladen, um die Einstellungen der geklonten Datenbank anzupassen. Sie können auch die Standardspezifikationsdatei für den Datenbank-Snapshot herunterladen.
    b. Im Abschnitt **Wiederherstellungsbereich** wählen Sie aus, wie die wiederherzustellenden Daten für die Klonerstellung eingeschränkt werden sollen, und geben Sie die erforderlichen Informationen für die von Ihnen gewählte Option ein. Die Auswahl von **Keine** stellt alle Daten wieder her.
    c. Im Abschnitt **Vor- und Nachskripte** können Sie eine oder beide der Optionen **Vorskript** und **Nachskript** aktivieren, um ein Skript auszuführen, bevor der Klonvorgang beginnt oder nachdem er abgeschlossen ist. Geben Sie für jede Option den vollständigen Skriptpfad und alle erforderlichen Argumente ein.
12. Wählen Sie **Clone** aus.

Planen Sie das Klonen einer Oracle-Datenbank

Planen Sie die Erstellung eines sofortigen Klons und die kontinuierliche Aktualisierung des Klons. Dadurch wird der aktuellstmögliche Klon der Datenbank erstellt. Verwenden Sie diese Methode, wenn Sie den Klon kontinuierlich nach einem von Ihnen gewählten Zeitplan aus dem neuesten Stand der Datenbank aktualisieren möchten.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Clone** aus.
4. Wählen Sie **Neuen Klon erstellen**.
5. Wählen Sie im Abschnitt **Datenbankquelle** den Quellhost und die Datenbank aus den Listen aus.
6. Im Abschnitt **Zieldatenbank** wählen Sie den Zielhost und die Datenbank aus den Listen aus. Der Zielhost und die Datenbank können sich vom Quellhost unterscheiden.
7. Wählen Sie **Weiter**.
8. Im Abschnitt **Klonen von** auf der Seite **Wiederherstellungspunkt auswählen** wählen Sie **Instant snapshot and clone**.
9. Wählen Sie einen Speicherort für den Snapshot, wenn er erstellt wird.
10. Wählen Sie **Weiter**.
11. Führen Sie auf der Seite **Erweiterte Optionen** Folgendes aus:
    a. Um die Einstellungen der geklonten Datenbank anzupassen, aktivieren Sie die Option **Zieldatenbankparameter anpassen**. Wenn Sie zuvor eine Spezifikationsdatei gespeichert haben,

können Sie diese mit dieser Option hochladen, um die Einstellungen der geklonten Datenbank anzupassen. Sie können auch die Standardspezifikationsdatei für die Datenbank herunterladen, die deren aktuelle Einstellungen widerspiegelt.

b. Im Abschnitt **Aktualisierungszeitplan für den Klon** können Sie festlegen, wann und wie oft der Klon aktualisiert werden soll. Das Aktualisieren des Klons erstellt den sofortigen Snapshot neu und überschreibt den bestehenden Klon mit einem neuen Klon.

c. Im Abschnitt **Vor- und Nachskripte** können Sie eine oder beide der Optionen **Vorskript** und **Nachskript** aktivieren, um ein Skript auszuführen, bevor der Klonvorgang beginnt oder nachdem er abgeschlossen ist. Geben Sie für jede Option den vollständigen Skriptpfad und alle erforderlichen Argumente ein.

12. Wählen Sie **Clone** aus.

Einen Klon teilen

Sie können einen Klon Ihrer Oracle Database-Workloads aufteilen. Das Aufteilen eines Klons erstellt eine neue Sicherung aus dem Klon. Sie können die neue Sicherung verwenden, um Datenbanken wiederherzustellen.

Sie können einen Klon in unabhängige oder langfristige Klone aufteilen. Ein Assistent zeigt die Liste der Aggregate an, die Teil der SVM sind, ihre Größen und wo sich das geklonte Volume befindet. NetApp Backup and Recovery zeigt außerdem an, ob genügend Speicherplatz zum Aufteilen des Klons vorhanden ist. Nachdem der Klon aufgeteilt wurde, wird er zum Schutz zu einer unabhängigen Datenbank.

Der Klon-Job wird nicht entfernt und kann für andere Klone erneut verwendet werden.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie einen Klon aus.
3. Wählen Sie das Symbol Aktionen ••• > **Geteilter Klon**.
4. Überprüfen Sie die Details zum geteilten Klon und wählen Sie **Teilen**.
5. Wenn der geteilte Klon erstellt ist, können Sie ihn auf der Seite **Inventar** anzeigen.

Löschen eines Klons

Sie können einen Klon Ihrer Oracle Database-Workloads löschen. Wenn Sie einen Klon löschen, wird er aus dem Objektspeicher entfernt, wodurch Speicherplatz freigegeben wird.

Wenn eine Richtlinie den Klon schützt, werden sowohl der Klon als auch sein Job gelöscht.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie einen Klon aus.
3. Wählen Sie das Symbol Aktionen ••• > **Klon löschen**.
4. Überprüfen Sie im Bestätigungsdialogfeld zum Löschen des Klons die Löschdetails.
   a. Um die geklonten Ressourcen aus SnapCenter zu löschen, auch wenn auf die Klone oder ihren Speicher nicht zugegriffen werden kann, wählen Sie **Löschen erzwingen**.
   b. Wählen Sie **Löschen**.
5. Wenn der Klon gelöscht wird, wird er von der Seite **Inventar** entfernt.

Stellen Sie Oracle-Datenbanken mit NetApp Backup and Recovery wieder her

Stellen Sie Oracle-Datenbanken aus Snapshots, aus einem auf Sekundärspeicher replizierten Backup oder aus in Objektspeichern gespeicherten Backups mithilfe von NetApp Backup and Recovery wieder her.

Von diesen Speicherorten wiederherstellen

Sie können Datenbanken von verschiedenen Startorten wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten am ursprünglichen Speicherort wiederherstellen. Die Wiederherstellung an einem anderen Speicherort ist in dieser privaten Vorschauversion nicht verfügbar.

- Am ursprünglichen Speicherort wiederherstellen

So funktioniert die Wiederherstellung von Oracle-Datenbanken

Wenn Sie Oracle-Datenbanken wiederherstellen, geschieht Folgendes:

- Wenn Sie eine Datenbank aus einem lokalen Snapshot wiederherstellen, erstellt NetApp Backup and Recovery eine *neue* Ressource mithilfe der Daten aus dem Backup.
- Wenn Sie aus einem replizierten Speicher wiederherstellen, können Sie es am ursprünglichen Speicherort wiederherstellen.
- Wenn Sie ein Backup aus dem Objektspeicher wiederherstellen, können Sie die Daten im Quellspeicher oder auf einem lokalen ONTAP -System wiederherstellen und die Datenbank von dort wiederherstellen.

Auf der Seite „Wiederherstellen“ (auch als „Suchen und Wiederherstellen“ bezeichnet) können Sie eine Datenbank wiederherstellen, auch wenn Sie sich nicht an den genauen Namen, den Speicherort oder das Datum erinnern, an dem sie zuletzt in gutem Zustand war. Sie können mithilfe von Filtern nach der Datenbank suchen.

Wiederherstellen einer Oracle-Datenbank

Stellen Sie je nach Bedarf eine Oracle-Datenbank zu einem bestimmten Zeitpunkt, zu einer bestimmten Systemänderungsnummer (SCN) oder zum letzten fehlerfreien Zustand wieder her. Sie können die Datenbank auch einfach aus Snapshots wiederherstellen und den automatisierten Wiederherstellungsprozess überspringen. Wenn Sie die Wiederherstellung manuell durchführen möchten, können Sie den automatisierten Wiederherstellungsprozess überspringen. Sie können die Datenbank anhand ihres Namens oder mit bestimmten Filtern suchen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
3. Wählen Sie aus der Dropdown-Liste rechts neben dem Namenssuchfeld **Oracle** aus.
4. Geben Sie den Namen der Datenbank ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem Datenbankhost, auf dem sich die wiederherzustellende Datenbank befindet.

   Es wird eine Liste mit Snapshots angezeigt, die Ihren Suchkriterien entsprechen.
5. Wählen Sie die Schaltfläche **Wiederherstellen** für die Datenbank, die Sie wiederherstellen möchten.
6. Wählen Sie eine Wiederherstellungsoption:

   Wiederherstellung zu einem bestimmten Zeitpunkt

   a. Wählen Sie **Zu einem bestimmten Zeitpunkt wiederherstellen**.
   b. Wählen Sie **Weiter**.
   c. Wählen Sie ein Datum aus der Dropdown-Liste und wählen Sie **Suchen**.

      Es wird eine Liste mit passenden Schnappschüssen zum angegebenen Datum angezeigt.

   Wiederherstellen auf eine bestimmte Systemänderungsnummer (SCN)

   a. Wählen Sie **Auf eine bestimmte Systemänderungsnummer (SCN) wiederherstellen**.
   b. Wählen Sie **Weiter**.
   c. Geben Sie die SCN ein, die als Wiederherstellungspunkt verwendet werden soll, und wählen Sie **Suchen**.

      Es wird eine Liste mit passenden Snapshots für die angegebene SCN angezeigt.

   Wiederherstellen auf die letzte Sicherung (letzter guter Zustand)

   a. Wählen Sie **Auf die neueste Sicherung wiederherstellen**.
   b. Wählen Sie **Weiter**.

      Es werden die neuesten Voll- und Protokollsicherungen angezeigt.

   Wiederherstellen aus Snapshots ohne Wiederherstellung

   a. Wählen Sie **Aus Snapshots ohne Wiederherstellung wiederherstellen**.
   b. Wählen Sie **Weiter**.

      Die passenden Schnappschüsse werden angezeigt.
7. Wählen Sie einen Quellspeicherort für den Snapshot aus.
8. Wählen Sie **Weiter**, um fortzufahren.
9. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

1. **Zieleinstellungen**:
   - Wählen Sie, ob die gesamte Datenbank oder nur die Tablespaces für die Datenbank wiederhergestellt werden sollen.
   - **Steuerdateien**: Aktivieren Sie diese Option optional, um auch die Datenbank-Steuerdateien wiederherzustellen.
2. **Optionen vor der Wiederherstellung**:
   - Aktivieren Sie diese Option optional und geben Sie den vollständigen Pfad für ein Skript ein, das vor dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.
   - Wählen Sie einen Timeout-Wert für das Skript. Wenn die Ausführung des Skripts innerhalb dieses Zeitraums fehlschlägt, wird die Wiederherstellung trotzdem fortgesetzt.
3. **Optionen nach der Wiederherstellung**:
   - **Postscript**: Aktivieren Sie diese Option optional und geben Sie den vollständigen Pfad für ein Skript ein, das nach dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.
   - **Öffnen Sie die Datenbank oder Containerdatenbank nach der Wiederherstellung im LESE-/SCHREIB-Modus**: Nachdem der Wiederherstellungsvorgang abgeschlossen ist, aktiviert Backup and Recovery den LESE-/SCHREIB-Modus für die Datenbank.
4. Abschnitt **Benachrichtigung**:
   - **E-Mail-Benachrichtigungen aktivieren**: Wählen Sie diese Option aus, um E-Mail-Benachrichtigungen über den Wiederherstellungsvorgang zu erhalten, und geben Sie an, welche Art von Benachrichtigungen Sie erhalten möchten.
5. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Nicht verfügbar für Oracle Database-Workloads Preview.

Oracle Database-Wiederherstellungspunkte mit NetApp Backup und Recovery einbinden, aushängen und katalogisieren

Sie sollten einen Oracle Database-Wiederherstellungspunkt einbinden, wenn Sie auf die Datenbank in einem kontrollierten Zustand zugreifen müssen, um Wiederherstellungsvorgänge durchzuführen. Katalogisieren Sie den Wiederherstellungspunkt manuell, wenn Sie die Backup und Recovery Metadaten der Sicherungs- und Wiederherstellungsvorgänge im RMAN-Wiederherstellungskatalog speichern müssen und die Option zur automatischen Katalogisierung der Metadaten nicht aktiviert ist.

Einen Oracle-Datenbank-Recovery-Punkt einbinden

Wenn Sie die Schutzrichtlinie für eine Datenbank so konfigurieren, dass Archivprotokolle aufbewahrt werden,

können Sie Wiederherstellungspunkte bereitstellen, um den Änderungsverlauf der Datenbank anzuzeigen.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Oracle-Kachel aus.
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
4. Wählen Sie für die Oracle-Datenbank-Workload in der Liste **Anzeigen** aus.
5. Wählen Sie das Menü **Datenbanken**.
6. Wählen Sie eine Datenbank aus der Liste und wählen Sie das Symbol Aktionen ••• > **Schutzdetails anzeigen**.

   Es wird eine Liste mit Wiederherstellungspunkten für diese Datenbank angezeigt.
7. Wählen Sie einen Wiederherstellungspunkt aus der Liste und wählen Sie das Symbol Aktionen ••• > **Mount**.
8. Führen Sie im angezeigten Dialogfeld die folgenden Schritte aus:
   a. Wählen Sie aus der Liste den Host aus, der den Wiederherstellungspunkt mounten soll.
   b. Wählen Sie den Speicherort aus, den Backup and Recovery zum Bereitstellen des Wiederherstellungspunkts verwenden soll. Für die Vorabversion wird das Mounten aus dem Objektspeicher nicht unterstützt.

      Der Mount-Pfad, den Backup und Recovery verwenden soll, wird angezeigt.
9. Wählen Sie **Mount**.

   Der Wiederherstellungspunkt wird auf dem Oracle-Host bereitgestellt.

Einen Wiederherstellungspunkt einer Oracle-Datenbank aushängen

Heben Sie die Bereitstellung des Wiederherstellungspunkts auf, wenn Sie die an dieser Datenbank vorgenommenen Änderungen nicht mehr anzeigen müssen.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Oracle-Kachel aus.
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
4. Wählen Sie für die Oracle-Workload in der Liste **Anzeigen** aus.
5. Wählen Sie das Menü **Datenbanken**.
6. Wählen Sie eine Datenbank aus der Liste und wählen Sie das Symbol Aktionen ••• > **Schutzdetails anzeigen**.

   Es wird eine Liste mit Wiederherstellungspunkten für diese Datenbank angezeigt.
7. Wählen Sie einen Wiederherstellungspunkt aus der Liste und wählen Sie das Symbol Aktionen ••• > **Aushängen**.
8. Bestätigen Sie die Aktion, indem Sie **Unmount** auswählen.

Katalogisieren Sie einen Wiederherstellungspunkt einer Oracle-Datenbank

Katalogisieren Sie einen Wiederherstellungspunkt manuell, wenn Sie dessen Backup und Recovery-Betriebsmetadaten erhalten müssen. Die Metadaten werden gemäß den von Ihnen für die Datenbank gewählten Einstellungen für **Configure RMAN catalog** gespeichert (standardmäßig in der Ziel-Kontrolldatei). Sie müssen nur manuell katalogisieren, wenn die automatische Katalogisierung in der zugehörigen Datensicherungsstrategie deaktiviert ist.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Oracle-Kachel aus.
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
4. Wählen Sie für die Oracle-Workload in der Liste **Anzeigen** aus.
5. Wählen Sie das Menü **Datenbanken**.
6. Wählen Sie eine Datenbank aus der Liste und wählen Sie das Symbol Aktionen ••• > **Schutzdetails anzeigen**.

   Es wird eine Liste mit Wiederherstellungspunkten für diese Datenbank angezeigt.
7. Wählen Sie einen Wiederherstellungspunkt aus der Liste und klicken Sie auf das Symbol Aktionen ••• > **Katalog**.
8. Bestätigen Sie die Aktion durch Auswahl von **Katalog**.