Grundlagen von Backup und Recovery

Enterprise applications

NetApp
February 10, 2026

Inhalt

Grundlagen von Backup und Recovery . . . 1
- Snapshot basierte Backups . . . 1
  - Ist ein Snapshot eine Sicherung? . . . 1
  - Snapshot basierte Backups . . . 2
  - Konsistenzgruppen . . . 2
  - Snapshots von Konsistenzgruppen . . . 3
  - Strategien . . . 4
  - Snapshot-basierte Recovery . . . 5
  - Snapshot Reserve . . . 5
  - Snapshots von ONTAP und Drittanbietern . . . 6
- SnapRestore . . . 6
  - Volume SnapRestore . . . 7
  - File SnapRestore . . . 7
- Online-Backups . . . 8
  - Datenlayout . . . 8
  - Verfahren zur lokalen Wiederherstellung – NFS . . . 9
  - Verfahren zur lokalen Wiederherstellung – SAN . . . 9
- Storage Snapshot optimierte Backups . . . 10
  - Datenlayout . . . 11
  - Verfahren zur lokalen Wiederherstellung – NFS . . . 11
  - Verfahren zur lokalen Wiederherstellung – SAN . . . 11
  - Beispiel für eine vollständige Wiederherstellung . . . 12
  - Beispiel für eine zeitpunktgenaue Recovery . . . 12
- Tools für Datenbankmanagement und Automatisierung . . . 14
  - SnapCenter . . . 14
  - RUHE . . . 15

Grundlagen von Backup und Recovery

Snapshot basierte Backups

Die Grundlage der Datensicherung für Oracle-Datenbanken auf ONTAP ist die NetApp Snapshot Technologie.

Die wichtigsten Werte sind:

- **Einfachheit.** Ein Snapshot ist eine schreibgeschützte Kopie des Inhalts eines Datencontainers zu einem bestimmten Zeitpunkt.
- **Effizienz.** Snapshots benötigen zum Zeitpunkt der Erstellung keinen Platz. Der Speicherplatz wird nur dann verbraucht, wenn Daten geändert werden.
- **Verwaltbarkeit.** Eine auf Snapshots basierende Backup-Strategie lässt sich einfach konfigurieren und verwalten, da Snapshots ein nativer Teil des Storage-Betriebssystems sind. Wenn das Speichersystem eingeschaltet ist, kann es Backups erstellen.
- **Skalierbarkeit.** bis zu 1024 Backups eines einzigen Dateicontainers und LUNs können beibehalten werden. Bei komplexen Datensätzen können diverse Daten-Container durch einen einzelnen, konsistenten Satz von Snapshots gesichert werden.
- Die Performance bleibt davon unberührt, ob ein Volume 1024 Snapshots enthält oder keine.

Viele Storage-Anbieter liefern zwar Snapshot-Technologie, doch ist die Snapshot Technologie bei ONTAP einzigartig und bietet in Enterprise-Applikations- und Datenbankumgebungen deutliche Vorteile:

- Snapshot Kopien sind Teil des zugrunde liegenden Write-Anywhere-Dateilayouts (WAFL). Es handelt sich nicht um ein Add-on oder eine externe Technologie. Dies vereinfacht das Management, da das Storage-System das Backup-System ist.
- Snapshot-Kopien beeinträchtigen die Performance nicht. Ausnahmen bilden Edge-Fälle, in denen so viele Daten in Snapshots gespeichert werden, dass sich das zugrunde liegende Storage-System füllt.
- Der Begriff „Konsistenzgruppe“ wird häufig verwendet, um eine Gruppierung von Storage-Objekten zu referenzieren, die als konsistente Sammlung von Daten gemanagt werden. Ein Snapshot eines bestimmten ONTAP Volumes stellt ein Konsistenzgruppenbackup dar.

ONTAP Snapshots lassen sich auch besser skalieren als bei Technologien von Mitbewerbern. Kunden können ohne Beeinträchtigung der Performance 5, 50 oder 500 Snapshots speichern. Derzeit sind in einem Volume maximal 1024 Snapshots zulässig. Wenn eine zusätzliche Snapshot-Aufbewahrung erforderlich ist, gibt es Optionen, die Snapshots an zusätzliche Volumes zu übergeben.

Daher ist die Sicherung eines auf ONTAP gehosteten Datensatzes einfach und hochskalierbar. Backups erfordern keine Verschiebung von Daten. Daher kann eine Backup-Strategie auf die Bedürfnisse des Unternehmens zugeschnitten werden und nicht auf die Beschränkungen der Netzwerkübertragungsraten, der großen Anzahl von Bandlaufwerken oder der Bereiche, in denen Festplatten bereitgestellt werden.

Ist ein Snapshot eine Sicherung?

Eine häufig gestellte Frage zur Verwendung von Snapshots als Datensicherungsstrategie ist die Tatsache, dass sich die „echten“ Daten und Snapshot-Daten auf denselben Laufwerken befinden. Der Verlust dieser Laufwerke würde sowohl zum Verlust der Primärdaten als auch des Backups führen.

Das ist ein berechtigte Anliegen. Lokale Snapshots werden für tägliche Backup- und Recovery-Anforderungen

verwendet, in dieser Hinsicht ist der Snapshot ein Backup. Beinahe 99 % aller Recovery-Szenarien in NetApp Umgebungen basieren auf Snapshots, um selbst die anspruchsvollsten RTO-Anforderungen zu erfüllen.

Lokale Snapshots sollten jedoch nie die einzige Backup-Strategie sein. Deshalb bietet NetApp Technologien wie SnapMirror und SnapVault-Replizierung, um Snapshots schnell und effizient auf einen unabhängigen Laufwerkssatz zu replizieren. In einer richtig konzipierten Lösung mit Snapshots und Snapshot-Replikation kann die Verwendung von Tapes auf ein vierteljährliches Archiv minimiert oder ganz eliminiert werden.

Snapshot basierte Backups

Für die Sicherung Ihrer Daten gibt es viele Optionen für den Einsatz von ONTAP Snapshots. Snapshots bilden die Basis vieler anderer ONTAP Funktionen wie Replizierung, Disaster Recovery und Klonen. Eine vollständige Beschreibung der Snapshot-Technologie geht über den Umfang dieses Dokuments hinaus. Die folgenden Abschnitte bieten jedoch einen allgemeinen Überblick.

Es gibt zwei primäre Ansätze zum Erstellen eines Snapshots eines Datensatzes:

- Absturzkonsistente Backups
- Applikationskonsistente Backups

Ein absturzkonsistentes Backup eines Datensatzes bezieht sich auf die Erfassung der gesamten Datensatzstruktur zu einem bestimmten Zeitpunkt. Wenn der Datensatz in einem einzigen Volume gespeichert wird, ist der Vorgang einfach. Ein Snapshot kann jederzeit erstellt werden. Wenn ein Datensatz in mehreren Volumes gespeichert ist, muss ein Snapshot einer Konsistenzgruppe (CG) erstellt werden. Für das Erstellen von Snapshots von Konsistenzgruppen stehen verschiedene Optionen zur Verfügung, darunter NetApp SnapCenter-Software, native Funktionen von ONTAP-Konsistenzgruppen und vom Benutzer verwaltete Skripts.

Absturzkonsistente Backups kommen vor allem dann zum Einsatz, wenn die Recovery am Point-of-the-Backup ausreichend ist. Wenn ein granulareres Recovery erforderlich ist, sind in der Regel applikationskonsistente Backups erforderlich.

Das Wort „konsistent“ in „anwendungskonsistent“ ist oft eine Fehlbezeichnung. Das Platzieren einer Oracle-Datenbank in den Backup-Modus wird beispielsweise als applikationskonsistentes Backup bezeichnet, die Daten werden jedoch in keiner Weise konsistent oder stillgelegt. Die Daten ändern sich während des Backups weiterhin. Im Gegensatz dazu machen die meisten MySQL und Microsoft SQL Server Backups die Daten tatsächlich stillgelegt, bevor sie das Backup ausführen. VMware kann bestimmte Dateien konsistent machen oder auch nicht.

Konsistenzgruppen

Der Begriff „Konsistenzgruppe“ bezieht sich auf die Fähigkeit eines Speicherarrays, mehrere Speicherressourcen als ein einziges Image zu verwalten. Beispielsweise kann eine Datenbank aus 10 LUNs bestehen. Das Array muss in der Lage sein, diese 10 LUNs konsistent zu sichern, wiederherzustellen und zu replizieren. Eine Wiederherstellung ist nicht möglich, wenn die Images der LUNs zum Zeitpunkt des Backups nicht konsistent waren. Die Replikation dieser 10 LUNs erfordert, dass alle Replikate perfekt miteinander synchronisiert sind.

Der Begriff „Konsistenzgruppe“ wird nicht oft verwendet, wenn es um ONTAP geht, da Konsistenz immer eine Grundfunktion der Volume- und Aggregat-Architektur in ONTAP war. Viele andere Storage Arrays managen LUNs oder File-Systeme als einzelne Einheiten. Sie könnten aus Datenschutzgründen optional als „Konsistenzgruppe“ konfiguriert werden, dies ist jedoch ein zusätzlicher Schritt in der Konfiguration.

ONTAP war schon immer in der Lage, konsistente lokale und replizierte Images von Daten zu erfassen. Auch

wenn die verschiedenen Volumes auf einem ONTAP-System normalerweise nicht formal als Konsistenzgruppe beschrieben werden, so sind sie doch das. Ein Snapshot dieses Volumes ist ein Konsistenzgruppenabbild, die Wiederherstellung dieses Snapshots ist eine Wiederherstellung der Konsistenzgruppe, und sowohl SnapMirror als auch SnapVault bieten Konsistenzgruppenreplikation.

Snapshots von Konsistenzgruppen

Konsistenzgruppen-Snapshots (cg-Snapshots) sind eine Erweiterung der grundlegenden ONTAP-Snapshot-Technologie. Bei einem standardmäßigen Snapshot-Vorgang wird ein konsistentes Image aller Daten innerhalb eines einzelnen Volumes erstellt. In manchen Fällen ist es jedoch erforderlich, einen konsistenten Satz von Snapshots über mehrere Volumes und sogar über mehrere Storage-Systeme hinweg zu erstellen. Das Ergebnis ist ein Satz von Snapshots, die auf die gleiche Weise wie ein Snapshot von nur einem einzelnen Volume verwendet werden können. Sie können für die lokale Datenwiederherstellung verwendet, für Disaster Recovery-Zwecke repliziert oder als einheitliche konsistente Einheit geklont werden.

Die größte Verwendung von cg-Snapshots ist eine Datenbankumgebung mit einer Größe von ca. 1 PB und 12 Controllern. Die cg-Snapshots, die auf diesem System erstellt wurden, werden für Backups, Wiederherstellungen und Klonvorgänge verwendet.

Wenn ein Datensatz über mehrere Volumes verteilt und die Schreibreihenfolge beibehalten werden muss, wird meist automatisch ein cg-Snapshot von der ausgewählten Managementsoftware verwendet. Es besteht in solchen Fällen nicht die Notwendigkeit, die technischen Details von cg-Snapshots zu verstehen. Allerdings gibt es Situationen, in denen komplizierte Datensicherungsanforderungen eine detaillierte Kontrolle über den Datenschutz- und Replizierungsprozess erfordern. Einige Optionen sind Automatisierungs-Workflows oder der Einsatz benutzerdefinierter Skripte, um cg-Snapshot-APIs aufzurufen. Das Verständnis der besten Option und der Rolle von cg-Snapshot erfordert eine detailliertere Erläuterung der Technologie.

Die Erstellung eines Satzes von cg-Snapshots erfolgt in zwei Schritten:

1. Erstellung von Write Fencing auf allen Ziel-Volumes
2. Erstellen Sie Snapshots dieser Volumes im abgetrennten Zustand.

Schreibzaun wird seriell hergestellt. Das bedeutet, dass bei der Einrichtung des Fencing-Prozesses über mehrere Volumes hinweg die I/O-Schreibvorgänge auf dem ersten Volume in der Sequenz eingefroren werden, da sie weiterhin auf Volumes übertragen werden, die später angezeigt werden. Dies mag anfänglich möglicherweise gegen die Vorgabe verstoßen, die Schreibreihenfolge zu erhalten, gilt aber nur für I/O-Vorgänge, die asynchron auf dem Host ausgegeben werden und nicht von anderen Schreibvorgängen abhängen.

Beispielsweise kann eine Datenbank eine Vielzahl asynchroner Datendatei-Updates ausgeben und dem Betriebssystem ermöglichen, die I/O-Vorgänge neu zu ordnen und sie gemäß seiner eigenen Scheduler-Konfiguration abzuschließen. Die Reihenfolge dieser E/A-Typen kann nicht garantiert werden, da die Anwendung und das Betriebssystem bereits die Anforderung zur Wahrung der Schreibreihenfolge freigegeben haben.

Als Zählerbeispiel sind die meisten Datenbankprotokollierungsaktivitäten synchron. Die Datenbank fährt erst mit weiteren Protokollschreibvorgängen fort, nachdem der I/O-Vorgang bestätigt wurde und die Reihenfolge dieser Schreibvorgänge erhalten bleiben muss. Wenn ein Protokoll-I/O auf einem Volume mit Fencing ankommt, wird dies nicht bestätigt, und die Applikation blockiert weitere Schreibvorgänge. Ebenso ist der I/O der Filesystem-Metadaten in der Regel synchron. Beispielsweise darf ein Dateilösch nicht verloren gehen. Wenn ein Betriebssystem mit einem xfs-Dateisystem eine Datei und den I/O gelöscht hat, der die xfs-Dateisystemmetadaten aktualisiert hat, um den Verweis auf diese Datei zu entfernen, der auf einem umzäunten Volume gelandet ist, wird die Dateisystemaktivität angehalten. Dies garantiert die Integrität des Dateisystems während cg-Snapshot-Vorgängen.

Nach der Einrichtung von Write Fencing über die Ziel-Volumes hinweg sind sie für die Snapshot-Erstellung bereit. Die Snapshots müssen nicht genau zur gleichen Zeit erstellt werden, da der Zustand der Volumes aus einer abhängigen Schreibweise eingefroren wird. Um sich vor einem Fehler in der Anwendung zu schützen, die cg-Snapshots erstellt, enthält das anfängliche Write Fencing ein konfigurierbares Timeout, bei dem ONTAP die Fencing automatisch freigibt und die Schreibverarbeitung nach einer definierten Anzahl von Sekunden wieder aufnimmt. Wenn alle Snapshots erstellt werden, bevor die Zeitüberschreitung abgelaufen ist, dann ist der resultierende Snapshot-Satz eine gültige Konsistenzgruppe.

Abhängige Schreibreihenfolge

Aus technischer Sicht ist der Schlüssel zu einer Konsistenzgruppe die Aufrechterhaltung der Schreibreihenfolge und insbesondere der abhängigen Schreibreihenfolge. Beispielsweise wird eine Datenbank, die in 10 LUNs schreibt, gleichzeitig auf alle geschrieben. Viele Schreibvorgänge werden asynchron ausgegeben. Dies bedeutet, dass die Reihenfolge ihrer Fertigstellung unwichtig ist und die Reihenfolge ihrer Fertigstellung je nach Betriebssystem und Netzwerkverhalten variiert.

Einige Schreibvorgänge müssen auf der Festplatte vorhanden sein, bevor die Datenbank mit zusätzlichen Schreibvorgängen fortfahren kann. Diese kritischen Schreibvorgänge werden als abhängige Schreibvorgänge bezeichnet. Nachfolgende Schreib-I/O hängt davon ab, ob diese Schreibvorgänge auf der Festplatte vorhanden sind. Jeder Snapshot, jede Wiederherstellung oder Replikation dieser 10 LUNs muss sicherstellen, dass die abhängige Schreibreihenfolge gewährleistet ist. Dateisystemaktualisierungen sind ein weiteres Beispiel für Schreibvorgänge in Schreibreihenfolge. Die Reihenfolge, in der Dateisystemänderungen vorgenommen werden, muss beibehalten werden, oder das gesamte Dateisystem kann beschädigt werden.

Strategien

Es gibt zwei primäre Ansätze bei Snapshot-basierten Backups:

- Absturzkonsistente Backups
- Snapshot geschützte Hot-Backups

Ein absturzkonsistentes Backup einer Datenbank bezieht sich auf die Erfassung der gesamten Datenbankstruktur, einschließlich Datendateien, Wiederherstellungsprotokolle und Kontrolldateien zu einem bestimmten Zeitpunkt. Wenn die Datenbank in einem einzigen Volume gespeichert wird, ist der Vorgang einfach. Ein Snapshot kann jederzeit erstellt werden. Wenn eine Datenbank in mehreren Volumes gespeichert ist, muss ein Snapshot einer Konsistenzgruppe (CG) erstellt werden. Für das Erstellen von Snapshots von Konsistenzgruppen stehen verschiedene Optionen zur Verfügung, darunter NetApp SnapCenter-Software, native Funktionen von ONTAP-Konsistenzgruppen und vom Benutzer verwaltete Skripts.

Absturzkonsistente Snapshot Backups werden in erster Linie verwendet, wenn die Recovery eines bestimmten Backup ausreichend ist. Archivprotokolle können unter bestimmten Umständen eingesetzt werden. Wenn jedoch eine granularere zeitpunktgenaue Recovery erforderlich ist, ist ein Online-Backup vorzuziehen.

Das grundlegende Verfahren für ein Snapshot-basiertes Online-Backup ist wie folgt:

1. Platzieren Sie die Datenbank in `backup` Modus.
2. Erstellen Sie einen Snapshot aller Volumes, die Datendateien hosten.
3. Beenden `backup` Modus.
4. Führen Sie den Befehl aus `alter system archive log current` So erzwingen Sie die Protokollarchivierung.
5. Erstellen Sie Snapshots aller Volumes, die die Archivprotokolle hosten.

Dieses Verfahren ergibt einen Satz von Snapshots, die Datendateien im Backup-Modus enthalten, und die kritischen Archivprotokolle, die im Backup-Modus generiert wurden. Dies sind die beiden Anforderungen für das Recovery einer Datenbank. Dateien wie Kontrolldateien sollten ebenfalls aus Gründen der Bequemlichkeit geschützt werden, aber die einzige absolute Anforderung ist die Sicherung von Datendateien und Archivprotokollen.

Auch wenn unterschiedliche Kunden möglicherweise sehr unterschiedliche Strategien verfolgen, basieren fast alle diese Strategien letztendlich auf den unten erläuterten Prinzipien.

Snapshot-basierte Recovery

Beim Entwurf von Volume-Layouts für Oracle-Datenbanken ist die erste Entscheidung, ob die Volume-basierte VBSR-Technologie (NetApp SnapRestore) verwendet wird.

Mit Volume-basierten SnapRestore kann ein Volume fast sofort auf einen früheren Zeitpunkt zurückgesetzt werden. Da alle Daten auf dem Volume zurückgesetzt werden, ist VBSR möglicherweise nicht für alle Anwendungsfälle geeignet. Wenn beispielsweise eine gesamte Datenbank, einschließlich Datendateien, Wiederherstellungs- und Archivprotokolle, auf einem einzelnen Volume gespeichert ist und dieses Volume mit VBSR wiederhergestellt wird, gehen Daten verloren, da das neuere Archivprotokoll und die Wiederherstellungsdaten verworfen werden.

VBSR ist für die Wiederherstellung nicht erforderlich. Viele Datenbanken können mithilfe von dateibasiertem Single-File SnapRestore (SFSR) oder einfach durch Kopieren von Dateien aus dem Snapshot zurück in das aktive Dateisystem wiederhergestellt werden.

VBSR wird bevorzugt, wenn eine Datenbank sehr groß ist oder wenn sie so schnell wie möglich wiederhergestellt werden muss, und die Verwendung von VBSR erfordert die Isolierung der Datendateien. In einer NFS-Umgebung müssen die Datendateien einer bestimmten Datenbank in dedizierten Volumes gespeichert werden, die nicht durch andere Dateitypen kontaminiert sind. In einer SAN-Umgebung müssen Datendateien in dedizierten LUNs auf dedizierten Volumes gespeichert werden. Wenn ein Volume-Manager verwendet wird (einschließlich Oracle Automatic Storage Management [ASM]), muss die Festplattengruppe auch für Datendateien reserviert sein.

Werden Datendateien auf diese Weise isoliert, können sie in einen früheren Zustand zurückgesetzt werden, ohne andere Filesysteme zu beschädigen.

Snapshot Reserve

Für jedes Volume mit Oracle-Daten in einer SAN-Umgebung die `percent-snapshot-space` Sollte auf null gesetzt werden, da das Reservieren von Speicherplatz für einen Snapshot in einer LUN-Umgebung nicht nützlich ist. Wenn die fraktionale Reserve auf 100 eingestellt ist, benötigt ein Snapshot eines Volumes mit LUNs genug freien Platz im Volumen, ausgenommen die Snapshot-Reserve, um 100% Umsatz aller Daten aufzunehmen. Wenn die fraktionale Reserve auf einen niedrigeren Wert eingestellt ist, dann ist entsprechend weniger freier Speicherplatz erforderlich, schließt jedoch immer die Snapshot Reserve aus. Das bedeutet, dass der Speicherplatz der Snapshot-Reserve in einer LUN-Umgebung verschwendet wird.

In einer NFS-Umgebung gibt es zwei Optionen:

- Stellen Sie die ein `percent-snapshot-space` Basiert auf dem erwarteten Snapshot-Speicherplatzverbrauch.
- Stellen Sie die ein `percent-snapshot-space` Zur gemeinsamen Nutzung von Speicherplatz und Snapshots sowie zur Vermeidung und zum Management dieser Kapazitäten.

Mit der ersten Option `percent-snapshot-space` Wird auf einen Wert ungleich Null gesetzt, normalerweise

etwa 20 %. Dieser Raum wird dann vor dem Benutzer ausgeblendet. Dieser Wert schafft jedoch keine Begrenzung der Auslastung. Wenn bei einer Datenbank mit einer Reservierung von 20 % 30 % anfällt, kann der Snapshot-Platz über die Grenze der 20-prozentigen Reserve hinauswachsen und nicht reservierten Speicherplatz belegen.

Der Hauptvorteil, wenn Sie eine Reserve auf einen Wert wie 20% setzen, besteht darin zu überprüfen, ob etwas Speicherplatz für Snapshots immer verfügbar ist. Bei einem 1-TB-Volume mit einer Reserve von 20 % wäre es beispielsweise nur einem Datenbankadministrator (DBA) möglich, 800 GB an Daten zu speichern. Diese Konfiguration garantiert mindestens 200 GB Speicherplatz für den Snapshot-Verbrauch.

Wenn `percent-snapshot-space` Ist auf null festgelegt, sodass der gesamte Speicherplatz im Volume für den Endbenutzer verfügbar ist, sodass bessere Sichtbarkeit gewährleistet wird. Ein DBA muss verstehen, dass ein 1-TB-Volume, das Snapshots nutzt, 1 TB Speicherplatz zwischen aktiven Daten und dem Snapshot-Umsatz gemeinsam genutzt wird.

Es gibt keine klare Präferenz zwischen Option 1 und Option 2 unter den Endbenutzern.

Snapshots von ONTAP und Drittanbietern

Oracle Doc ID 604683.1 erläutert die Anforderungen für die Snapshot-Unterstützung von Drittanbietern und die verschiedenen verfügbaren Optionen für Backup- und Wiederherstellungsvorgänge.

Der Drittanbieter muss sicherstellen, dass die Snapshots des Unternehmens den folgenden Anforderungen entsprechen:

- Snapshots müssen sich in die von Oracle empfohlenen Restore- und Recovery-Vorgänge integrieren.
- Snapshots müssen zum Zeitpunkt des Snapshots auch beim Absturz einer Datenbank konsistent sein.
- Die Schreibreihenfolge wird für jede Datei in einem Snapshot beibehalten.

Die Oracle Managementprodukte von ONTAP und NetApp erfüllen diese Anforderungen.

SnapRestore

Die schnelle Datenwiederherstellung in ONTAP anhand eines Snapshots wird durch die NetApp SnapRestore Technologie ermöglicht.

Wenn ein kritischer Datensatz nicht verfügbar ist, laufen die geschäftskritischen Prozesse ab. Tapes können beschädigt werden und selbst Restores aus festplattenbasierten Backups können die Übertragung über das Netzwerk verlangsamen. SnapRestore vermeidet diese Probleme durch eine nahezu sofortige Wiederherstellung der Datensätze. Selbst Datenbanken im Petabyte-Bereich lassen sich in wenigen Minuten vollständig wiederherstellen.

Es gibt zwei Arten von SnapRestore: Datei-/LUN-basiert und Volume-basiert.

- Einzelne Dateien oder LUNs lassen sich innerhalb von Sekunden wiederherstellen, egal ob es sich um eine 2-TB-LUN oder eine 4-KB-Datei handelt.
- Der Container von Dateien oder LUNs kann innerhalb von Sekunden wiederhergestellt werden, egal ob es sich um 10 GB oder 100 TB an Daten handelt.

Ein „Container mit Dateien oder LUNs“ würde sich normalerweise auf ein FlexVol Volume beziehen. Beispielsweise können Sie 10 LUNs aufweisen, aus denen sich eine LVM-Festplattengruppe in einem einzelnen Volume befindet. Alternativ kann ein Volume die NFS-Home-Verzeichnisse von 1000 Benutzern

speichern. Anstatt für jede einzelne Datei oder jedes LUN einen Wiederherstellungsvorgang auszuführen, können Sie das gesamte Volume als einzelnen Vorgang wiederherstellen. Der Prozess funktioniert auch mit horizontal skalierbaren Containern, die mehrere Volumes enthalten, wie z. B. eine FlexGroup oder eine ONTAP-Konsistenzgruppe.

Der Grund, warum SnapRestore so schnell und effizient arbeitet, liegt in der Natur eines Snapshots, der im Wesentlichen eine parallele schreibgeschützte Ansicht der Inhalte eines Volumes zu einem bestimmten Zeitpunkt ist. Aktive Blöcke sind die realen Blöcke, die geändert werden können, während der Snapshot eine schreibgeschützte Ansicht des Status der Blöcke ist, die die Dateien und LUNs zum Zeitpunkt der Snapshot-Erstellung ausmachen.

ONTAP erlaubt nur schreibgeschützten Zugriff auf Snapshot-Daten, die Daten können jedoch mit SnapRestore reaktiviert werden. Der Snapshot wird als Lese-/Schreibansicht der Daten wieder aktiviert und gibt die Daten in ihren vorherigen Zustand zurück. SnapRestore kann auf Volume- oder Dateiebene betrieben werden. Die Technologie ist im Wesentlichen die gleiche mit ein paar geringfügigen Unterschiede im Verhalten.

Volume SnapRestore

Volume-basierte SnapRestore stellt das gesamte Datenvolumen in einen früheren Zustand zurück. Dieser Vorgang erfordert keine Datenverschiebung, d. h., der Wiederherstellungsprozess erfolgt im Wesentlichen unmittelbar, obwohl die Verarbeitung der API- oder CLI-Vorgänge einige Sekunden dauern kann. Die Wiederherstellung von 1 GB Daten ist nicht komplizierter und zeitaufwändiger als die Wiederherstellung von 1 PB Daten. Diese Funktion ist der Hauptgrund dafür, dass viele Enterprise-Kunden zu ONTAP Storage-Systemen migrieren. Die RTO wird in Sekunden für selbst größte Datensätze gemessen.

Ein Nachteil von Volume-basierten SnapRestore ist die Tatsache, dass Änderungen innerhalb eines Volumes im Laufe der Zeit kumuliert werden. Daher sind jeder Snapshot und die Daten der aktiven Datei von den bis zu diesem Zeitpunkt vorgenommenen Änderungen abhängig. Das Zurücksetzen eines Volumes in einen früheren Zustand bedeutet, dass alle nachfolgenden Änderungen, die an den Daten vorgenommen wurden, verworfen werden. Weniger offensichtlich ist jedoch, dass dies nachträglich erstellte Snapshots einschließt. Das ist nicht immer wünschenswert.

Beispielsweise kann in einem SLA für die Datenaufbewahrung eine nächtliche Sicherung von 30 Tagen festgelegt werden. Wenn ein Datensatz auf einen vor fünf Tagen mit Datenträger SnapRestore erstellten Snapshot wiederhergestellt wird, werden alle in den letzten fünf Tagen erstellten Snapshots verworfen und dies verstößt gegen den SLA.

Es gibt eine Reihe von Optionen, um diese Einschränkung zu beheben:

1. Daten können von einem früheren Snapshot kopiert werden, anstatt eine SnapRestore des gesamten Volumes durchzuführen. Diese Methode eignet sich am besten für kleinere Datensätze.
2. Ein Snapshot kann geklont und nicht wiederhergestellt werden. Die Einschränkung dieses Ansatzes besteht darin, dass der Quell-Snapshot eine Abhängigkeit des Klons ist. Daher kann sie nur gelöscht oder in ein unabhängiges Volume aufgesplittet werden.
3. Verwendung von dateibasiertem SnapRestore.

File SnapRestore

Bei File-basierten SnapRestore handelt es sich um einen granulareren Snapshot-basierten Wiederherstellungsprozess. Anstatt den Status eines gesamten Volume zurückzusetzen, wird der Status einer einzelnen Datei oder LUN zurückgesetzt. Es müssen keine Snapshots gelöscht werden. Durch diesen Vorgang wird auch keine Abhängigkeit von einem vorherigen Snapshot erzeugt. Die Datei oder LUN ist im aktiven Volume sofort verfügbar.

Bei einem SnapRestore Restore einer Datei oder eines LUN sind keine Datenverschiebungen erforderlich. Einige interne Metadaten-Updates sind jedoch erforderlich, um abzubilden, dass die zugrunde liegenden Blöcke in einer Datei oder einem LUN jetzt sowohl in einem Snapshot als auch in dem aktiven Volume vorhanden sind. Die Performance sollte sich nicht auswirken, doch bei diesem Prozess wird die Erstellung von Snapshots blockiert, bis dieser abgeschlossen ist. Die Verarbeitungsrate beträgt ca. 5 Gbit/s (18 TB/Stunde), basierend auf der Gesamtgröße der wiederhergestellten Dateien.

Online-Backups

Zwei Datensätze sind erforderlich, um eine Oracle Datenbank im Backup-Modus zu schützen und wiederherzustellen. Beachten Sie, dass dies nicht die einzige Oracle-Backup-Option ist, aber es ist die häufigste.

- Ein Snapshot der Datendateien im Backup-Modus
- Die Archivprotokolle, die erstellt wurden, während sich die Datendateien im Backup-Modus befanden

Wenn eine vollständige Recovery einschließlich aller festgeschriebenen Transaktionen notwendig ist, ist ein dritter Artikel erforderlich:

- Ein Satz aktueller Wiederherstellungsprotokolle

Es gibt eine Reihe von Möglichkeiten, die Recovery eines Online-Backups zu fördern. Viele Kunden stellen Snapshots mithilfe der ONTAP CLI wieder her und verwenden dann Oracle RMAN oder sqlplus, um die Recovery abzuschließen. Dies ist besonders bei großen Produktionsumgebungen der Fall, in denen die Wahrscheinlichkeit und Häufigkeit der Wiederherstellung von Datenbanken äußerst gering ist und alle Wiederherstellungsverfahren von einem erfahrenen DBA durchgeführt werden. Für die vollständige Automatisierung verfügen Lösungen wie NetApp SnapCenter über ein Oracle Plug-in mit Befehlszeile und grafischer Benutzeroberfläche.

Einige große Kunden haben einen einfacheren Ansatz verfolgt, indem sie einfache Skripte auf den Hosts konfigurieren, um die Datenbanken zu einem bestimmten Zeitpunkt in den Backup-Modus zu versetzen, um einen geplanten Snapshot vorzubereiten. Planen Sie beispielsweise den Befehl `alter database begin backup` Um 23:58 `alter database end backup` Um 00:02 Uhr, und planen Sie dann Snapshots direkt auf dem Speichersystem um Mitternacht. Das Ergebnis ist eine einfache, hochgradig skalierbare Backup-Strategie, für die keine externe Software oder Lizenzen erforderlich sind.

Datenlayout

Am einfachsten ist es, Datendateien in einem oder mehreren dedizierten Volumes zu isolieren. Sie müssen durch einen anderen Dateityp nicht kontaminiert sein. Dadurch soll sichergestellt werden, dass die Datendatei-Volumes über einen SnapRestore-Vorgang schnell wiederhergestellt werden können, ohne dass ein wichtiges Wiederherstellungsprotokoll, eine Steuerdatei oder ein Archivprotokoll zerstört werden.

SAN hat ähnliche Anforderungen für die Isolation von Datendateien in dedizierten Volumes. Bei einem Betriebssystem wie Microsoft Windows kann ein einzelnes Volume mehrere Datendatei-LUNs mit jeweils einem NTFS-Filesystem enthalten. Bei anderen Betriebssystemen gibt es in der Regel einen logischen Volume Manager. Mit Oracle ASM wäre es beispielsweise am einfachsten, die LUNs einer ASM-Laufwerksgruppe auf ein einzelnes Volume zu beschränken, das als Einheit gesichert und wiederhergestellt werden kann. Wenn aus Gründen der Performance oder des Kapazitätsmanagements zusätzliche Volumes erforderlich sind, vereinfacht sich das Management durch die Erstellung einer zusätzlichen Festplattengruppe auf dem neuen Volume.

Wenn diese Richtlinien befolgt werden, können Snapshots direkt auf dem Speichersystem geplant werden,

ohne dass ein Snapshot einer Konsistenzgruppe erforderlich ist. Der Grund hierfür liegt darin, dass für Oracle-Backups keine Datendateien gleichzeitig gesichert werden müssen. Das Online-Backup-Verfahren wurde entwickelt, damit Datendateien weiterhin aktualisiert werden können, da sie im Laufe der Stunden langsam auf Tape gestreamt werden.

Eine Komplikation entsteht in Situationen wie der Verwendung einer ASM-Datenträgergruppe, die auf Volumes verteilt ist. In diesen Fällen muss ein cg-Snapshot ausgeführt werden, um sicherzustellen, dass die ASM-Metadaten über alle zusammengehörigen Volumes hinweg konsistent sind.

Achtung: Überprüfen Sie, dass der ASM `spfile` Und `passwd` Die Dateien befinden sich nicht in der Festplattengruppe, in der die Datendateien gehostet werden. Dies beeinträchtigt die Fähigkeit, Datendateien und nur Datendateien selektiv wiederherzustellen.

Verfahren zur lokalen Wiederherstellung – NFS

Dieses Verfahren kann manuell oder über eine Anwendung wie SnapCenter gesteuert werden. Das Grundverfahren ist wie folgt:

1. Fahren Sie die Datenbank herunter.
2. Stellen Sie die Datendatei-Volumes unmittelbar vor dem gewünschten Wiederherstellungspunkt auf den Snapshot wieder her.
3. Geben Sie Archivprotokolle bis zum gewünschten Punkt wieder.
4. Wiederholen Sie die aktuellen Wiederherstellungsprotokolle, wenn eine vollständige Wiederherstellung gewünscht wird.

Bei diesem Verfahren wird davon ausgegangen, dass die gewünschten Archivprotokolle noch im aktiven Dateisystem vorhanden sind. Ist dies nicht der Fall, müssen die Archivprotokolle wiederhergestellt werden oder rman/sqlplus kann zu den Daten im Snapshot-Verzeichnis geleitet werden.

Außerdem können Datendateien bei kleineren Datenbanken von einem Endbenutzer direkt aus wiederhergestellt werden `.snapshot` Verzeichnis ohne die Unterstützung von Automatisierungs-Tools oder Storage-Administratoren, ein auszuführen `snaprestore` Befehl.

Verfahren zur lokalen Wiederherstellung – SAN

Dieses Verfahren kann manuell oder über eine Anwendung wie SnapCenter gesteuert werden. Das Grundverfahren ist wie folgt:

1. Fahren Sie die Datenbank herunter.
2. Legen Sie die Festplattengruppe(n), die die Datendateien hosten, still. Die Vorgehensweise hängt vom gewählten Logical Volume Manager ab. Bei ASM muss die Datenträgergruppe demontieren. Bei Linux müssen die Dateisysteme demontiert und die logischen Volumes und Volume-Gruppen deaktiviert werden. Ziel ist es, alle Aktualisierungen auf der Zieldatentengruppe zu stoppen, die wiederhergestellt werden sollen.
3. Stellen Sie die Datendatei-Datenträgergruppen auf dem Snapshot unmittelbar vor dem gewünschten Wiederherstellungspunkt wieder her.
4. Reaktivieren Sie die neu wiederhergestellten Datenträgergruppen.
5. Geben Sie Archivprotokolle bis zum gewünschten Punkt wieder.
6. Wiederholen Sie alle Wiederherstellungsprotokolle, wenn eine vollständige Wiederherstellung gewünscht wird.

Bei diesem Verfahren wird davon ausgegangen, dass die gewünschten Archivprotokolle noch im aktiven Dateisystem vorhanden sind. Wenn dies nicht der Fall ist, müssen die Archivprotokolle wiederhergestellt werden, indem die Archivprotokoll-LUNs offline geschaltet und eine Wiederherstellung durchgeführt wird. Dies ist ebenfalls ein Beispiel, bei dem sich Archivprotokolle in dedizierte Volumes aufteilen lassen. Wenn die Archivprotokolle eine Volume-Gruppe mit Wiederherstellungsprotokollen gemeinsam nutzen, müssen die Wiederherstellungsprotokolle vor der Wiederherstellung des gesamten LUN-Satzes an eine andere Stelle kopiert werden. Dieser Schritt verhindert den Verlust dieser letzten aufgezeichneten Transaktionen.

Storage Snapshot optimierte Backups

Snapshot-basiertes Backup und Recovery wurden vor der Veröffentlichung von Oracle 12c noch einfacher, da eine Datenbank nicht im Hot-Backup-Modus platziert werden muss. Daraus ergibt sich die Möglichkeit, Snapshot basierte Backups direkt auf einem Storage-System zu planen und dennoch eine vollständige oder zeitpunktgenaue Recovery durchzuführen.

Obwohl DBAs mit der Hot-Backup-Wiederherstellung vertrauter sind, ist es seit langem möglich, Snapshots zu verwenden, die nicht erstellt wurden, während sich die Datenbank im Hot-Backup-Modus befand. Für Oracle 10g und 11g waren während der Recovery zusätzliche manuelle Schritte erforderlich, um die Datenbankkonsistenz zu gewährleisten. Mit Oracle 12c, `sqlplus` Und `rman` Enthalten die zusätzliche Logik zur Wiedergabe von Archivprotokollen für Datendatei-Backups, die sich nicht im Hot-Backup-Modus befanden.

Wie bereits erwähnt, erfordert die Wiederherstellung eines Snapshot-basierten Hot-Backups zwei Datensätze:

- Ein Snapshot der Datendateien, der im Backup-Modus erstellt wurde
- Die Archivprotokolle, die generiert wurden, während sich die Datendateien im Hot-Backup-Modus befanden

Während der Recovery liest die Datenbank Metadaten aus den Datendateien, um die erforderlichen Archivprotokolle für die Recovery auszuwählen.

Storage Snapshot optimierte Recovery erfordert geringfügig unterschiedliche Datensätze, um die gleichen Ergebnisse zu erzielen:

- Ein Snapshot der Datendateien und eine Methode zur Identifizierung des Zeits, zu dem der Snapshot erstellt wurde
- Archivieren Sie Protokolle vom Zeitpunkt des letzten Datendatei-Kontrollpunkts bis zum genauen Zeitpunkt des Snapshots

Während der Recovery liest die Datenbank Metadaten aus den Datendateien, um das früheste erforderliche Archivprotokoll zu identifizieren. Eine vollständige oder zeitpunktgenaue Recovery kann durchgeführt werden. Bei einer zeitpunktgenauen Recovery ist es wichtig, die Zeit des Snapshots der Datendateien zu kennen. Der angegebene Wiederherstellungspunkt muss nach der Erstellungszeit der Snapshots liegen. NetApp empfiehlt, die Snapshot-Zeit um mindestens einige Minuten zu erweitern, um Uhrschwankungen zu berücksichtigen.

Ausführliche Informationen finden Sie in der Oracle-Dokumentation zum Thema „Recovery Using Storage Snapshot Optimization“, die in verschiedenen Versionen der Oracle 12c-Dokumentation verfügbar ist. Weitere Informationen zur Snapshot-Unterstützung von Drittanbietern finden Sie unter Oracle Document ID Doc ID 604683.1.

Datenlayout

Am einfachsten ist es, die Datendateien in einem oder mehreren dedizierten Volumes zu isolieren. Sie müssen durch einen anderen Dateityp nicht kontaminiert sein. Dadurch soll sichergestellt werden, dass die Datendatei-Volumes mit einem SnapRestore-Vorgang schnell wiederhergestellt werden können, ohne dass ein wichtiges Wiederherstellungsprotokoll, eine Steuerdatei oder ein Archivprotokoll zerstört werden.

SAN hat ähnliche Anforderungen für die Isolation von Datendateien in dedizierten Volumes. Bei einem Betriebssystem wie Microsoft Windows kann ein einzelnes Volume mehrere Datendatei-LUNs mit jeweils einem NTFS-Filesystem enthalten. Bei anderen Betriebssystemen gibt es in der Regel auch einen logischen Volume Manager. Mit Oracle ASM wäre es beispielsweise am einfachsten, Laufwerksgruppen auf ein einzelnes Volume zu beschränken, das als Einheit gesichert und wiederhergestellt werden kann. Wenn aus Gründen der Performance oder des Kapazitätsmanagements zusätzliche Volumes erforderlich sind, erleichtert die Erstellung einer zusätzlichen Laufwerksgruppe auf dem neuen Volume das Management.

Wenn diese Richtlinien befolgt werden, können Snapshots direkt auf ONTAP geplant werden, ohne dass ein Snapshot einer Konsistenzgruppe erforderlich ist. Der Grund hierfür liegt darin, dass Snapshot-optimierte Backups keine gleichzeitige Sicherung von Datendateien erfordern.

Eine Komplikation entsteht in Situationen wie einer ASM-Datenträgergruppe, die auf Volumes verteilt ist. In diesen Fällen muss ein cg-Snapshot ausgeführt werden, um sicherzustellen, dass die ASM-Metadaten über alle zusammengehörigen Volumes hinweg konsistent sind.

[Hinweis]Vergewissern Sie sich, dass sich die ASM-Spfile- und Passwd-Dateien nicht in der Festplattengruppe befinden, die die Datendateien hostet. Dies beeinträchtigt die Fähigkeit, Datendateien und nur Datendateien selektiv wiederherzustellen.

Verfahren zur lokalen Wiederherstellung – NFS

Dieses Verfahren kann manuell oder über eine Anwendung wie SnapCenter gesteuert werden. Das Grundverfahren ist wie folgt:

1. Fahren Sie die Datenbank herunter.
2. Stellen Sie die Datendatei-Volumes unmittelbar vor dem gewünschten Wiederherstellungspunkt auf den Snapshot wieder her.
3. Geben Sie Archivprotokolle bis zum gewünschten Punkt wieder.

Bei diesem Verfahren wird davon ausgegangen, dass die gewünschten Archivprotokolle noch im aktiven Dateisystem vorhanden sind. Wenn dies nicht der Fall ist, müssen die Archivprotokolle wiederhergestellt werden, oder `rman` Oder `sqlplus` Kann auf die Daten im weitergeleitet werden `.snapshot` Verzeichnis.

Außerdem können Datendateien bei kleineren Datenbanken von einem Endbenutzer direkt aus wiederhergestellt werden `.snapshot` Directory ohne Unterstützung durch Automatisierungs-Tools oder einen Storage-Administrator, um einen SnapRestore-Befehl auszuführen.

Verfahren zur lokalen Wiederherstellung – SAN

Dieses Verfahren kann manuell oder über eine Anwendung wie SnapCenter gesteuert werden. Das Grundverfahren ist wie folgt:

1. Fahren Sie die Datenbank herunter.
2. Legen Sie die Festplattengruppe(n), die die Datendateien hosten, still. Die Vorgehensweise hängt vom gewählten Logical Volume Manager ab. Bei ASM muss die Datenträgergruppe demontieren. Bei Linux

müssen die Dateisysteme getrennt und die logischen Volumes und Volume-Gruppen deaktiviert werden. Ziel ist es, alle Aktualisierungen auf der Zieldatentengruppe zu stoppen, die wiederhergestellt werden sollen.

3. Stellen Sie die Datendatei-Datenträgergruppen auf dem Snapshot unmittelbar vor dem gewünschten Wiederherstellungspunkt wieder her.
4. Reaktivieren Sie die neu wiederhergestellten Datenträgergruppen.
5. Geben Sie Archivprotokolle bis zum gewünschten Punkt wieder.

Bei diesem Verfahren wird davon ausgegangen, dass die gewünschten Archivprotokolle noch im aktiven Dateisystem vorhanden sind. Wenn dies nicht der Fall ist, müssen die Archivprotokolle wiederhergestellt werden, indem die Archivprotokoll-LUNs offline geschaltet und eine Wiederherstellung durchgeführt wird. Dies ist ebenfalls ein Beispiel, bei dem sich Archivprotokolle in dedizierte Volumes aufteilen lassen. Wenn die Archivprotokolle eine Volume-Gruppe mit Wiederherstellungsprotokollen gemeinsam nutzen, müssen die Wiederherstellungsprotokolle vor der Wiederherstellung des gesamten LUN-Satzes an eine andere Stelle kopiert werden, damit die letzten aufgezeichneten Transaktionen nicht verloren gehen.

Beispiel für eine vollständige Wiederherstellung

Angenommen, die Datendateien wurden beschädigt oder zerstört, und eine vollständige Recovery ist erforderlich. Das Verfahren ist wie folgt:

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover automatic;
Media recovery complete.
SQL> alter database open;
Database altered.
SQL>
```

Beispiel für eine zeitpunktgenaue Recovery

Der gesamte Wiederherstellungsvorgang erfolgt über einen einzigen Befehl: `recover automatic`.

Wenn eine Point-in-Time-Recovery erforderlich ist, muss der Zeitstempel der Snapshots bekannt sein und kann wie folgt identifiziert werden:

```
Cluster01::> snapshot show -vserver vserver1 -volume NTAP_oradata -fields
create-time
vserver   volume        snapshot   create-time
--------  ------------  ---------  ------------------------
vserver1  NTAP_oradata  my-backup  Thu Mar 09 10:10:06 2017
```

Die Erstellungszeit für Snapshots wird als 9. März und 10:10:06 aufgeführt. Um sicher zu sein, wird der Snapshot-Zeit eine Minute hinzugefügt:

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover database until time '09-MAR-2017 10:44:15' snapshot time '09-
MAR-2017 10:11:00';
```

Die Wiederherstellung ist nun gestartet. Es gab eine Snapshot-Zeit von 10:11:00, eine Minute nach der aufgezeichneten Zeit, um mögliche Taktabweichungen zu berücksichtigen, und eine Ziel-Recovery-Zeit von 10:44 an. Als Nächstes fordert sqlplus die Archivprotokolle an, die benötigt werden, um die gewünschte Wiederherstellungszeit von 10:44 zu erreichen.

```
ORA-00279: change 551760 generated at 03/09/2017 05:06:07 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_31_930813377.dbf
ORA-00280: change 551760 for thread 1 is in sequence #31
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 552566 generated at 03/09/2017 05:08:09 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_32_930813377.dbf
ORA-00280: change 552566 for thread 1 is in sequence #32
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 553045 generated at 03/09/2017 05:10:12 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_33_930813377.dbf
ORA-00280: change 553045 for thread 1 is in sequence #33
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 753229 generated at 03/09/2017 05:15:58 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_34_930813377.dbf
ORA-00280: change 753229 for thread 1 is in sequence #34
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Log applied.
Media recovery complete.
SQL> alter database open resetlogs;
Database altered.
SQL>
```

Führen Sie die Wiederherstellung einer Datenbank mithilfe von Snapshots mit dem durch `recover automatic` Für Befehl ist keine spezifische Lizenzierung erforderlich, aber die zeitpunktgenaue Recovery mit `snapshot time` Erfordert die Oracle Advanced Compression-Lizenz.

Tools für Datenbankmanagement und Automatisierung

Der Hauptnutzen von ONTAP in einer Oracle Datenbankumgebung ergibt sich aus den zentralen ONTAP Technologien wie sofortige Snapshot Kopien, einfache SnapMirror Replizierung und die effiziente Erstellung von FlexClone Volumes.

In manchen Fällen erfüllt eine einfache Konfiguration dieser Kernfunktionen direkt in ONTAP die Anforderungen, für kompliziertere Anforderungen ist jedoch eine Orchestrierungsschicht erforderlich.

SnapCenter

SnapCenter ist das Vorzeigeprodukt für die Datensicherung von NetApp. Sie ähnelt im Hinblick auf die Durchführung von Datenbank-Backups den SnapManager Produkten. Sie wurde jedoch von Grund auf entwickelt, um bei NetApp Storage-Systemen eine zentrale Konsole für das Management der Daten zu bieten.

SnapCenter umfasst Grundfunktionen wie Snapshot-basierte Backups und Restores, SnapMirror und SnapVault Replizierung sowie weitere Funktionen, die für den skalierten Betrieb von Großunternehmen erforderlich sind. Zu diesen erweiterten Funktionen gehören eine erweiterte Funktion zur rollenbasierten Zugriffssteuerung (RBAC), RESTful APIs zur Integration in Orchestrierungsprodukte von Drittanbietern, unterbrechungsfreies, zentrales Management von SnapCenter Plug-ins auf Datenbank-Hosts und eine Benutzeroberfläche für Cloud-skalierbare Umgebungen.

RUHE

ONTAP enthält außerdem einen umfangreichen RESTful API-Satz. Drittanbieter sind so in der Lage, Datensicherungs- und Management-Applikationen mit enger Integration in ONTAP zu erstellen. Darüber hinaus kann die RESTful API von Kunden genutzt werden, die ihre eigenen Automatisierungs-Workflows und Dienstprogramme erstellen möchten.