Oracle Datensicherung

Enterprise applications

NetApp
May 09, 2024

Inhalt

Oracle Datensicherung

Oracle Datensicherung mit ONTAP

NetApp weiß, dass die geschäftskritischsten Daten in Datenbanken zu finden sind.

Ein Unternehmen kann nicht ohne Zugriff auf seine Daten arbeiten, und manchmal definieren die Daten das Unternehmen. Diese Daten müssen geschützt werden. Bei der Datensicherung geht es jedoch mehr als nur um das Sicherstellen eines nutzbaren Backups. Es geht darum, die Backups schnell und zuverlässig durchzuführen und diese sicher zu speichern.

Die andere Seite der Datensicherung ist die Datenwiederherstellung. Wenn auf Daten nicht zugegriffen werden kann, ist das Unternehmen betroffen und kann nicht mehr in Betrieb sein, bis die Daten wiederhergestellt werden. Dieser Prozess muss schnell und zuverlässig sein. Schließlich müssen die meisten Datenbanken vor Ausfällen geschützt werden, was bedeutet, dass ein Replikat der Datenbank beibehalten wird. Das Replikat muss ausreichend aktuell sein. Außerdem muss es schnell und einfach sein, das Replikat zu einer voll funktionsfähigen Datenbank zu machen.

Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4591: Oracle Data Protection: Backup, Recovery und Replication.*

Planung

Die richtige Datensicherungsarchitektur hängt von den geschäftlichen Anforderungen für die Datenaufbewahrung, Recovery-Fähigkeit und Ausfalltoleranz bei verschiedenen Ereignissen ab.

Betrachten Sie beispielsweise die Anzahl der im Umfang enthaltenen Applikationen, Datenbanken und wichtigen Datensätze. Die Entwicklung einer Backup-Strategie für einen einzelnen Datensatz gewährleistet, dass die Compliance mit typischen SLAs relativ unkompliziert ist, da nicht viele Objekte zu managen sind. Je mehr Datensätze es gibt, desto komplizierter wird das Monitoring und Administratoren müssen sich zunehmend mit dem Vermeiden von Backup-Fehlern befassen. Wenn eine Umgebung also die Skalierung von Cloud- und Service-Provider-Umgebungen erreicht, braucht es einen ganz anderen Ansatz.

Die Datensatzgröße wirkt sich auch auf die Strategie aus. Es gibt beispielsweise viele Optionen für Backup und Recovery mit einer Datenbank mit 100 GB, da die Datenmenge so klein ist. Das einfache Kopieren der Daten von Backup-Medien mit herkömmlichen Tools bietet normalerweise eine ausreichende RTO für die Recovery. Eine 100-TB-Datenbank benötigt normalerweise eine komplett andere Strategie, es sei denn, das RTO erlaubt einen mehrtägigen Ausfall. In diesem Fall könnte ein herkömmliches Backup und Recovery auf Basis von Kopien akzeptabel sein.

Schließlich gibt es Faktoren, die nicht dem Backup- und Recovery-Prozess selbst unterliegen. Gibt es zum Beispiel Datenbanken, die kritische Produktionsaktivitäten unterstützen, was das Recovery zu einem seltenen Ereignis macht, das nur von erfahrenen DBAs durchgeführt wird? Sind Datenbanken alternativ Teil einer großen Entwicklungsumgebung, in der häufig ein Recovery erfolgt und von einem IT-Team mit Generalisten gemanagt wird?

RTO-, RPO- und SLA-Planung für Oracle Database

Mit ONTAP können Sie in einfacher Weise eine Datensicherungsstrategie für Oracle Database an Ihre Geschäftsanforderungen anpassen.

Zu diesen Anforderungen gehören Faktoren wie die Geschwindigkeit der Recovery, der maximal zulässige Datenverlust und die Anforderungen an die Aufbewahrung von Backups. Der Datensicherungsplan muss zudem verschiedene gesetzliche Vorgaben für die Datenaufbewahrung und -Wiederherstellung berücksichtigen. Schließlich müssen verschiedene Datenwiederherstellungsszenarien in Betracht gezogen werden, von der typischen und vorhersehbaren Wiederherstellung aufgrund von Benutzer- oder Applikationsfehlern bis hin zu Disaster Recovery-Szenarien, die den vollständigen Ausfall eines Standorts beinhalten.

Kleine Änderungen an Richtlinien zur Datensicherung und Wiederherstellung können sich erheblich auf die Gesamtarchitektur von Storage, Backup und Recovery auswirken. Es ist wichtig, Standards zu definieren und zu dokumentieren, bevor mit dem Design begonnen wird, um eine Verkomplizierung einer Datensicherungsarchitektur zu vermeiden. Unnötige Schutzfunktionen oder -Ebenen führen zu unnötigen Kosten und Management-Overhead. Eine zunächst übersehene Anforderung kann ein Projekt in die falsche Richtung führen oder kurzfristig Designänderungen erfordern.

Recovery-Zeitvorgabe

Die Recovery-Zeitvorgabe (Recovery Time Objective, RTO) definiert die maximal zulässige Zeit für die Recovery eines Services. Eine Personaldatenbank könnte beispielsweise eine RTO von 24 Stunden haben, da, obwohl es sehr unpraktisch wäre, den Zugriff auf diese Daten während der Arbeitszeit zu verlieren, das Unternehmen dennoch arbeiten kann. Im Gegensatz dazu würde bei einer Datenbank, die das Hauptbuch einer Bank unterstützt, eine RTO in Minuten oder sogar Sekunden gemessen werden. Ein RTO von null ist nicht möglich, da es eine Möglichkeit geben muss, zwischen einem tatsächlichen Serviceausfall und einem Routineereignis wie einem verlorenen Netzwerkpaket zu unterscheiden. Typische Anforderungen sind jedoch ein RTO von nahezu null.

Recovery-Zeitpunkt

Der Recovery Point Objective (RPO) definiert den maximal tolerierbaren Datenverlust. In vielen Fällen wird der RPO lediglich durch die Häufigkeit von Snapshots oder snapmirror Updates bestimmt.

In manchen Fällen lässt sich der RPO-Wert aggressiver einsetzen, da er bestimmte Daten selektiv häufiger schützt. Im Datenbankkontext ist der RPO in der Regel eine Frage, wie viele Protokolldaten in einer bestimmten Situation verloren gehen können. In einem typischen Recovery-Szenario, bei dem eine Datenbank aufgrund eines Produktfehlers oder eines Benutzerfehlers beschädigt wird, sollte der RPO gleich null sein, d. h. es darf keine Daten verloren gehen. Bei der Wiederherstellung wird eine frühere Kopie der Datenbankdateien wiederhergestellt und anschließend die Protokolldateien wiedergegeben, um den Datenbankstatus auf den gewünschten Zeitpunkt zu bringen. Die für diesen Vorgang erforderlichen Protokolldateien sollten sich bereits am ursprünglichen Speicherort befinden.

In ungewöhnlichen Szenarien können Protokolldaten verloren gehen. Zum Beispiel eine versehentliche oder böswillige `rm -rf *` Der Datenbankdateien können zum Löschen aller Daten führen. Die einzige Option wäre die Wiederherstellung aus dem Backup, einschließlich Protokolldateien, und einige Daten würden unweigerlich verloren gehen. Die einzige Option zur Verbesserung des RPO in einer herkömmlichen Backup-Umgebung besteht in der Durchführung wiederholter Backups der Protokolldaten. Dies hat jedoch Einschränkungen aufgrund der ständigen Datenverschiebung und der Schwierigkeiten, ein Backup-System als ständig laufenden Service zu warten. Einer der Vorteile erweiterter Storage-Systeme besteht in der Möglichkeit, Daten vor versehentlichen oder böswilligen Schäden an Dateien zu schützen und somit ein besseres RPO ohne Datenverschiebung zu ermöglichen.

Disaster Recovery

Disaster Recovery umfasst die IT-Architektur, Richtlinien und Verfahren, die zur Wiederherstellung eines Services bei einem physischen Ausfall erforderlich sind. Dies kann Überschwemmungen, Brände oder

Personen sein, die mit böswilliger oder fahrlässiger Absicht handeln.

Disaster Recovery ist mehr als nur eine Reihe von Recovery-Verfahren. Der gesamte Prozess umfasst die Identifizierung der verschiedenen Risiken, die Definition der Anforderungen an die Datenwiederherstellung und die Servicekontinuität sowie die Bereitstellung der richtigen Architektur mit den zugehörigen Verfahren.

Bei der Festlegung von Datensicherungsanforderungen ist es entscheidend, zwischen den typischen RPO- und RTO-Anforderungen und den für die Disaster Recovery erforderlichen RPO- und RTO-Anforderungen zu unterscheiden. Einige Applikationsumgebungen erfordern einen RPO von null und ein RTO von nahezu null für Datenverluste – von einem relativ normalen Benutzerfehler bis hin zu einem Brand, der ein Datacenter zerstört. Für diese hohen Schutzniveaus gibt es jedoch Kosten- und administrative Konsequenzen.

Im Allgemeinen sollten die Anforderungen an die nicht-Disaster-Recovery aus zwei Gründen strikt erfüllt werden. Zunächst sind Anwendungsfehler und Benutzerfehler, die zu Datenschäden führen, bis zu dem Punkt vorhersehbar, an dem sie fast unvermeidlich sind. Zweitens ist es nicht schwierig, eine Backup-Strategie zu entwickeln, die einen RPO von null und ein RTO von niedrigen Vorgaben liefern kann, solange das Storage-System nicht zerstört wird. Es gibt keinen Grund, ein erhebliches Risiko, das leicht behoben werden kann, nicht anzugehen. Deshalb sollten die RPO- und RTO-Ziele für die lokale Recovery aggressiv sein.

Disaster Recovery-RTO- und RPO-Anforderungen variieren stärker, je nach Wahrscheinlichkeit eines Ausfalls und den Folgen des damit verbundenen Datenverlusts oder der Unterbrechung des Geschäftsbetriebs. RPO- und RTO-Anforderungen sollten auf den tatsächlichen geschäftlichen Anforderungen basieren und nicht auf allgemeinen Prinzipien. Sie müssen mehrere logische und physische Ausfallszenarien berücksichtigen.

Logische Ausfälle

Zu logischen Katastrophen gehören Datenbeschädigungen durch Benutzer, Applikations- oder Betriebssystemfehler und Fehlfunktionen. Zu logischen Katastrophen können auch böswillige Angriffe durch externe Parteien mit Viren oder Würmern gehören oder die Ausnutzung von Schwachstellen von Applikationen. In diesen Fällen wird die physische Infrastruktur unbeschädigt, die zugrunde liegenden Daten sind jedoch nicht mehr gültig.

Eine immer häufiger vorauftretende logische Katastrophe wird als Ransomware bezeichnet. Bei ihr werden Daten mit einem Angriffsvektor verschlüsselt. Die Verschlüsselung schädigt die Daten nicht, macht sie jedoch erst verfügbar, wenn die Zahlung an einen Dritten erfolgt. Immer mehr Unternehmen sind gezielt auf Ransomware-Hacks ausgerichtet. Für diese Bedrohung bietet NetApp manipulationssichere Snapshots, bei denen nicht einmal der Storage-Administrator geschützte Daten vor dem konfigurierten Ablaufdatum ändern kann.

Physische Ausfälle

Zu physischen Ausfällen gehört der Ausfall von Komponenten einer Infrastruktur, die die Redundanzmerkmale übertreffen und zu einem Datenverlust oder erweitertem Service-Verlust führen. Der RAID-Schutz bietet beispielsweise Redundanz für Laufwerke, und die Verwendung von HBAs bietet Redundanz für FC-Port und FC-Kabel. Hardwareausfälle solcher Komponenten sind vorhersehbar und beeinträchtigen nicht die Verfügbarkeit.

In einer Unternehmensumgebung ist es in der Regel möglich, die Infrastruktur eines gesamten Standorts mit redundanten Komponenten so weit zu schützen, dass das einzige vorhersehbare physische Ausfallszenario ein vollständiger Verlust des Standorts ist. Die Planung des Disaster Recovery hängt dann von der Site-to-Site-Replizierung ab.

Synchrone und asynchrone Datensicherung

Im Idealfall würden alle Daten zwischen geografisch verteilten Standorten synchron repliziert werden. Eine solche Replikation ist nicht immer möglich oder sogar aus mehreren Gründen möglich:

- Die synchrone Replikation erhöht zwangsläufig die Schreiblatenz, da alle Änderungen an beiden Standorten repliziert werden müssen, bevor die Applikation/Datenbank mit der Verarbeitung fortfahren kann. Der daraus resultierende Performance-Effekt ist manchmal nicht akzeptabel, sodass die Verwendung von synchroner Spiegelung ausgeschlossen wird.
- Die zunehmende Einführung von 100 % SSD-Storage bedeutet, dass zusätzliche Schreiblatenz mit größerer Wahrscheinlichkeit zu verzeichnen ist, da die Performance-Erwartungen Hunderttausende IOPS und eine Latenz von unter einer Millisekunde umfassen. Um das volle Potenzial von 100 % SSDs auszuschöpfen, kann ein erneuter Besuch der Disaster-Recovery-Strategie erforderlich sein.
- Die Anzahl der Datensätze nimmt weiterhin an Byte zu. Dies stellt Unternehmen vor Herausforderungen, wenn es darum geht, genügend Bandbreite für eine synchrone Replizierung sicherzustellen.
- Die Komplexität der Datensätze nimmt zu und führt zu Herausforderungen beim Management einer umfassenden synchronen Replizierung.
- Cloud-basierte Strategien sind häufig mit höheren Replizierungsentfernungen und Latenz verbunden, wodurch die Nutzung einer synchronen Spiegelung weiterhin ausgeschlossen wird.

NetApp bietet Lösungen, die sowohl synchrone Replikation für höchste Anforderungen an die Datenwiederherstellung als auch asynchrone Lösungen für eine bessere Performance und Flexibilität beinhalten. Darüber hinaus lässt sich die NetApp Technologie nahtlos in viele Replizierungslösungen von Drittanbietern integrieren, wie z. B. Oracle DataGuard

Aufbewahrungszeit

Der letzte Aspekt einer Datensicherungsstrategie ist die Zeit für die Datenaufbewahrung, die sehr unterschiedlich sein kann.

- Eine typische Anforderung sind nächtliche Backups von 14 Tagen auf dem primären Standort und 90 Tage Backups auf einem sekundären Standort.
- Viele Kunden erstellen vierteljährliche eigenständige Archive, die auf unterschiedlichen Medien gespeichert sind.
- Eine ständig aktualisierte Datenbank benötigt möglicherweise keine Verlaufsdaten, und Backups müssen nur für einige Tage aufbewahrt werden.
- Gesetzliche Vorschriften erfordern möglicherweise die Wiederherstellbarkeit bis zu einem beliebigen Zeitpunkt jeder beliebigen Transaktion innerhalb eines Zeitfensters von 365 Tagen.

Verfügbarkeit von Oracle Database mit ONTAP

ONTAP wurde für eine maximale Verfügbarkeit von Oracle-Datenbanken konzipiert. Eine vollständige Beschreibung der Hochverfügbarkeitsfunktionen von ONTAP übersteigt den Rahmen dieses Dokuments. Wie bei der Datensicherheit ist jedoch ein grundlegendes Verständnis dieser Funktionalität bei der Entwicklung einer Datenbankinfrastruktur wichtig.

HA-Paare

Die Basiseinheit der Hochverfügbarkeit ist das HA-Paar. Jedes Paar enthält redundante Links, um die Replikation von Daten in NVRAM zu unterstützen. NVRAM ist kein Schreib-Cache. Der RAM im Controller dient als Schreib-Cache. Der Zweck von NVRAM besteht darin, Daten vorübergehend zu protokollieren, um Schutz vor unerwarteten Systemausfällen zu bieten. In dieser Hinsicht ähnelt es einem Datenbank-Redo-Protokoll.

Sowohl NVRAM als auch ein Datenbank-Wiederherstellungsprotokoll werden verwendet, um Daten schnell zu speichern, sodass Datenänderungen so schnell wie möglich vorgenommen werden können. Die Aktualisierung der persistenten Daten auf Laufwerken (oder Datendateien) findet erst später bei einem Prozess statt, der sowohl auf ONTAP- als auch auf den meisten Datenbankplattformen als Checkpoint bezeichnet wird. Weder NVRAM-Daten noch Datenbank-Wiederherstellungsprotokolle werden im normalen Betrieb gelesen.

Wenn ein Controller abrupt ausfällt, sind in NVRAM wahrscheinlich noch nicht gespeicherte Änderungen zu erwarten, die noch nicht auf die Laufwerke geschrieben wurden. Der Partner-Controller erkennt den Ausfall, übernimmt die Kontrolle über die Laufwerke und wendet die erforderlichen Änderungen an, die im NVRAM gespeichert wurden.

Takeover und Giveback

Takeover und Giveback beziehen sich auf den Prozess, bei dem die Verantwortung für Storage-Ressourcen zwischen Nodes in einem HA-Paar übertragen wird. Takeover und Giveback sind zweierlei Aspekte:

- Verwaltung der Netzwerkverbindung, die den Zugriff auf die Laufwerke ermöglicht
- Verwaltung der Antriebe selbst.

Die Netzwerkschnittstellen, die CIFS- und NFS-Datenverkehr unterstützen, werden sowohl mit dem Home-Standort als auch mit dem Failover-Standort konfiguriert. Eine Übernahme umfasst das Verschieben der Netzwerkschnittstellen zu ihrem temporären Home-Standort auf einer physischen Schnittstelle, die sich in denselben Subnetzen befindet wie der ursprüngliche Standort. Bei einem Giveback werden die Netzwerkschnittstellen zurück an ihre ursprünglichen Standorte verschoben. Das genaue Verhalten kann nach Bedarf angepasst werden.

Netzwerkschnittstellen, die SAN-Blockprotokolle wie iSCSI und FC unterstützen, werden während des Takeover und Giveback nicht verlagert. Stattdessen sollten LUNs mit Pfaden bereitgestellt werden, die ein vollständiges HA-Paar enthalten, was zu einem primären Pfad und einem sekundären Pfad führt.

Zusätzliche Pfade zu zusätzlichen Controllern können auch konfiguriert werden, um das Verschieben von Daten zwischen Nodes in einem größeren Cluster zu unterstützen. Dies ist jedoch nicht Teil des HA-Prozesses.

Der zweite Aspekt von Takeover und Giveback ist die Übertragung der Eigentumsrechte an den Festplatten. Der genaue Prozess hängt von mehreren Faktoren ab, einschließlich dem Grund für das Takeover/Giveback und den ausgegebenen Befehlszeilenoptionen. Das Ziel ist es, die Operation so effizient wie möglich durchzuführen. Obwohl der Gesamtprozess möglicherweise mehrere Minuten in Anspruch nimmt, kann der tatsächliche Zeitpunkt, in dem die Eigentumsrechte an dem Laufwerk von einem Node auf einen Node übertragen werden, in der Regel in Sekunden gemessen werden.

Takeover-Zeit

Host I/O durchläuft zwar eine kurze I/O-Pause bei Takeover- und Giveback-Vorgängen, jedoch sollte in einer korrekt konfigurierten Umgebung keine Applikationsunterbrechung auftreten. Der eigentliche

Transitionsprozess, bei dem I/O verzögert wird, wird in der Regel in Sekunden gemessen. Der Host benötigt jedoch möglicherweise zusätzliche Zeit, um die Änderung der Datenpfade zu erkennen und die I/O-Vorgänge erneut auszuführen.

Die Art der Störung hängt vom Protokoll ab:

- Eine Netzwerkschnittstelle, die NFS- und CIFS-Datenverkehr unterstützt, stellt nach dem Übergang zu einem neuen physischen Standort eine ARP-Anforderung (Address Resolution Protocol) an das Netzwerk aus. Dies führt dazu, dass die Netzwerk-Switches ihre MAC-Adresstabellen (Media Access Control) aktualisieren und die I/O-Verarbeitung fortsetzen Im Falle von geplanten Takeover und Giveback werden Störungen in der Regel in Sekunden gemessen und oftmals nicht feststellbar. Einige Netzwerke sind möglicherweise langsamer, um die Änderung des Netzwerkpfads vollständig zu erkennen, und einige Betriebssysteme können in sehr kurzer Zeit viele I/O-Vorgänge in Warteschlange stellen, die erneut versucht werden müssen. Dadurch kann die für die I/O-Wiederaufnahme erforderliche Zeit verlängert werden
- Eine Netzwerkschnittstelle, die SAN-Protokolle unterstützt, kann nicht an einen neuen Speicherort verschoben werden. Ein Host-Betriebssystem muss den oder die verwendeten Pfade ändern. Die vom Host beobachtete I/O-Pause hängt von mehreren Faktoren ab. Aus Sicht des Storage-Systems beträgt der Zeitraum, in dem I/O nicht mehr ausgeführt werden kann, nur wenige Sekunden. Verschiedene Host-Betriebssysteme erfordern jedoch möglicherweise eine zusätzliche Zeit, damit eine I/O-Dauer vor einem erneuten Versuch wieder aberkannt wird. Neuere Betriebssysteme können eine Pfadänderung viel schneller erkennen, aber ältere Betriebssysteme benötigen in der Regel bis zu 30 Sekunden, um eine Änderung zu erkennen.

Die zu erwartenden Übernahmezeiten, während denen das Storage-System keine Daten für eine Applikationsumgebung bereitstellen kann, sind in der folgenden Tabelle aufgeführt. Es sollte keine Fehler in einer Applikationsumgebung geben, das Takeover sollte stattdessen als kurze Pause bei der I/O-Verarbeitung erscheinen.

	NFS	AFF	ASA
Geplante Übernahme	15 Sek.	6-10 Sek.	2-3 Sek.
Ungeplante Übernahme	30 Sek.	6-10 Sek.	2-3 Sek.

Prüfsummen und Oracle-Datenbankintegrität

ONTAP und die unterstützten Protokolle umfassen mehrere Funktionen zum Schutz der Integrität der Oracle-Datenbank, darunter sowohl Daten im Ruhezustand als auch Daten, die über das Netzwerk übertragen werden.

Die logische Datensicherung innerhalb von ONTAP setzt sich aus drei Kernanforderungen zusammen:

- Daten müssen vor Datenbeschädigung geschützt werden.
- Die Daten müssen vor Laufwerksausfällen geschützt werden.
- Änderungen an Daten müssen vor Verlust geschützt werden.

Diese drei Anforderungen werden in den folgenden Abschnitten erläutert.

Netzwerkkorruption: Prüfsummen

Die grundlegendste Stufe des Datenschutzes ist die Prüfsumme, die einen speziellen Fehler erkennenden

Code ist, der neben den Daten gespeichert wird. Eine Beschädigung der Daten bei der Netzwerkübertragung wird mit Hilfe einer Prüfsumme und in einigen Fällen mehreren Prüfsummen erkannt.

Ein FC-Frame enthält beispielsweise eine Form der Prüfsumme, die als zyklische Redundanzprüfung (CRC, Cyclic Redundancy Check) bezeichnet wird, um sicherzustellen, dass die Nutzlast während der Übertragung nicht beschädigt ist. Der Sender sendet sowohl die Daten als auch den CRC der Daten. Der Empfänger eines FC-Frames berechnet den CRC der empfangenen Daten neu, um sicherzustellen, dass er mit dem übertragenen CRC übereinstimmt. Wenn der neu berechnete CRC nicht mit dem CRC übereinstimmt, der dem Frame zugeordnet ist, sind die Daten beschädigt und der FC-Frame wird verworfen oder abgelehnt. Eine iSCSI-I/O-Operation umfasst Prüfsummen auf TCP/IP- und Ethernet-Ebenen und kann für zusätzlichen Schutz optional auch den CRC-Schutz auf der SCSI-Schicht beinhalten. Jede Bit-Beschädigung auf dem Kabel wird von der TCP-Schicht oder IP-Schicht erkannt, was zu einer erneuten Übertragung des Pakets führt. Wie bei FC führen Fehler im SCSI CRC zu einem Verwerfen oder Zurückweisen des Vorgangs.

Laufwerkbeschädigungen: Prüfsummen

Mit Prüfsummen wird auch die Integrität der auf Laufwerken gespeicherten Daten überprüft. Auf Laufwerke geschriebene Datenblöcke werden mit einer Prüfsummenfunktion gespeichert, die eine unvorhersehbare Anzahl ergibt, die mit den Originaldaten verknüpft ist. Wenn Daten vom Laufwerk gelesen werden, wird die Prüfsumme neu berechnet und mit der gespeicherten Prüfsumme verglichen. Wenn sie nicht übereinstimmt, sind die Daten beschädigt und müssen von der RAID-Schicht wiederhergestellt werden.

Datenbeschädigung: Verlorene Schreibvorgänge

Eine der schwierigsten Arten von Korruption ist ein verlorenes oder falsch geschaltenes Schreiben. Wenn ein Schreibvorgang bestätigt wird, muss er an der richtigen Stelle auf das Medium geschrieben werden. Datenbeschädigungen lassen sich mithilfe einer einfachen Prüfsumme, die mit den Daten gespeichert wurde, relativ einfach erkennen. Wenn der Schreibvorgang jedoch einfach verloren geht, dann könnte die vorherige Version der Daten noch existieren und die Prüfsumme wäre korrekt. Wenn der Schreibvorgang an einem falschen physischen Speicherort platziert wird, ist die zugehörige Prüfsumme erneut für die gespeicherten Daten gültig, auch wenn der Schreibvorgang andere Daten zerstört hat.

Die Lösung für diese Herausforderung ist wie folgt:

- Ein Schreibvorgang muss Metadaten enthalten, die den Speicherort angeben, an dem der Schreibvorgang erwartungsgemäß gefunden werden soll.
- Ein Schreibvorgang muss eine Art Versionskennung enthalten.

Wenn ONTAP einen Block schreibt, schließt er Daten ein, zu denen der Block gehört. Wenn ein nachfolgender Lesezugriff einen Block identifiziert, der jedoch aufgrund der Metadaten zu Standort 123 gehört, als er an Position 456 gefunden wurde, wurde der Schreibvorgang fehlgestellt.

Es ist schwieriger, einen vollständig verlorenen Schreibvorgang zu erkennen. Die Erklärung ist sehr kompliziert, aber im Wesentlichen speichert ONTAP Metadaten so, dass ein Schreibvorgang zu Updates an zwei verschiedenen Orten auf den Laufwerken führt. Wenn ein Schreibvorgang verloren geht, werden bei einem nachfolgenden Lesen der Daten und der zugehörigen Metadaten zwei unterschiedliche Versionsidentitäten angezeigt. Dies zeigt an, dass der Schreibvorgang vom Laufwerk nicht abgeschlossen wurde.

Verloren gegangene und falsch verlegte Schreibvorgänge sind äußerst selten, doch steigt mit zunehmendem Laufwerksanzahl und steigenden Datenmengen der Datensätze das Risiko. Jedes Storage-System, das Datenbank-Workloads unterstützt, sollte die verlorener Schreibschutz enthalten.

Laufwerksausfälle: RAID, RAID DP und RAID-TEC

Wenn ein Datenblock auf einem Laufwerk erkannt wird, dass er beschädigt ist oder das gesamte Laufwerk ausfällt und nicht verfügbar ist, müssen die Daten wiederhergestellt werden. Dies wird in ONTAP mithilfe von Paritätslaufwerken durchgeführt. Die Daten werden auf mehreren Datenlaufwerken verteilt und anschließend Paritätsdaten generiert. Diese wird getrennt von den Originaldaten gespeichert.

ONTAP verwendete ursprünglich RAID 4, das für jede Gruppe von Datenlaufwerken ein Single-Parity-Laufwerk verwendet. Das Ergebnis war, dass ein Laufwerk in der Gruppe ausfallen konnte, ohne dass es zu Datenverlust kam. Bei einem Ausfall des Paritätslaufwerks wurden keine Daten beschädigt und ein neues Paritätslaufwerk erstellt. Wenn ein einzelnes Datenlaufwerk ausfällt, können die verbleibenden Laufwerke zusammen mit dem Paritätslaufwerk verwendet werden, um die fehlenden Daten neu zu generieren.

Bei geringen Laufwerksanzahl war die statistische Wahrscheinlichkeit, dass zwei Laufwerke gleichzeitig ausfallen, vernachlässigbar. Mit wachsenden Laufwerkskapazitäten hat sich auch die Zeit entwickelt, die für die Wiederherstellung von Daten nach einem Laufwerksausfall benötigt wird. Dadurch erhöht sich das Zeitfenster, in dem ein zweiter Laufwerksausfall zum Datenverlust führen würde. Darüber hinaus erzeugt der Neuerstellungsvorgang eine Menge zusätzlicher I/O auf den verbleibenden Laufwerken. Mit zunehmendem Festplattenalter steigt auch das Risiko, dass die zusätzliche Last zu einem zweiten Laufwerksausfall führt. Selbst wenn das Risiko eines Datenverlusts mit der fortgesetzten Nutzung von RAID 4 nicht Anstieg, würden die Folgen eines Datenverlusts schwerwiegender. Je mehr Daten im Falle eines Ausfalls einer RAID-Gruppe verloren gehen würden, desto länger würde die Wiederherstellung der Daten dauern, wodurch die Unterbrechung des Geschäftsbetriebs käme.

Aus diesen Problemen entwickelte NetApp die NetApp RAID DP-Technologie, eine Variante von RAID 6. Diese Lösung umfasst zwei Paritätslaufwerke, d. h., zwei beliebige Laufwerke einer RAID-Gruppe können ohne Datenverlust ausfallen. Die Größe der Laufwerke wurde weiter vergrößert, wodurch NetApp schließlich die NetApp RAID-TEC-Technologie entwickelt hat, wodurch ein drittes Paritätslaufwerk eingeführt wird.

Einige bewährte Verfahren für historische Datenbanken empfehlen die Verwendung von RAID-10, auch als Striped Mirroring bekannt. Dies bietet weniger Datensicherheit als RAID DP, da mehrere zwei-Festplatten-Fehlerszenarien auftreten, während es in RAID DP keine gibt.

Es gibt auch einige historische Best Practices für Datenbanken, die darauf hinweisen, dass RAID-10 aufgrund von Performance-Bedenken den Optionen RAID-4/5/6 vorzuziehen ist. Diese Empfehlungen beziehen sich manchmal auf einen RAID-Abzug. Obwohl diese Empfehlungen in der Regel richtig sind, gelten sie nicht für die Implementierungen von RAID innerhalb von ONTAP. Die Leistungsbedenken beziehen sich auf die Paritäts-Regeneration. Bei herkömmlichen RAID-Implementierungen müssen bei der Verarbeitung der routinemäßigen, zufälligen Schreibvorgänge durch eine Datenbank mehrere Lesezugriffe auf die Festplatte durchgeführt werden, um die Paritätsdaten neu zu generieren und den Schreibvorgang abzuschließen. Der Abzug wird definiert als die zusätzlichen Lese-IOPS, die zum Ausführen von Schreibvorgängen erforderlich sind.

Bei ONTAP kommt es nicht zu RAID-Einbußen, da Schreibvorgänge in den Speicher ausgelagert werden, wo Parität erzeugt wird und dann als einzelner RAID-Stripe auf die Festplatte geschrieben wird. Zum Abschließen des Schreibvorgangs sind keine Lesevorgänge erforderlich.

Zusammengefasst bieten RAID DP und RAID-TEC im Vergleich zu RAID 10 viel mehr nutzbare Kapazität, besseren Schutz vor Festplattenausfällen und keine Performance-Einbußen.

Schutz vor Hardware-Ausfällen: NVRAM

Jedes Storage-Array für Datenbank-Workloads muss Schreibvorgänge so schnell wie möglich durchführen. Darüber hinaus muss ein Schreibvorgang vor einem Verlust durch unerwartete Ereignisse, wie z. B. einen Stromausfall, geschützt werden. Das bedeutet, dass jeder Schreibvorgang sicher an mindestens zwei Orten

gespeichert werden muss.

AFF und FAS Systeme vertrauen zur Erfüllung dieser Anforderungen auf NVRAM. Der Schreibvorgang funktioniert wie folgt:

1. Die eingehenden Schreibdaten werden im RAM gespeichert.
2. Die Änderungen, die an Daten auf Festplatte vorgenommen werden müssen, werden sowohl auf dem lokalen Node als auch auf dem Partner-Node in NVRAM eingetragen. NVRAM ist kein Schreib-Cache, sondern ein Journal, das einem Datenbank-Wiederherstellungsprotokoll ähnelt. Unter normalen Bedingungen wird sie nicht gelesen. Sie wird nur für die Wiederherstellung verwendet, z. B. nach einem Stromausfall während der I/O-Verarbeitung.
3. Der Schreibvorgang wird dann dem Host bestätigt.

Der Schreibvorgang in dieser Phase ist aus Sicht der Applikation abgeschlossen, und die Daten sind vor Verlust geschützt, da sie an zwei verschiedenen Standorten gespeichert werden. Schließlich werden die Änderungen auf die Festplatte geschrieben, doch dieser Prozess ist aus Sicht der Applikation bandextern, da er nach dem Quittieren des Schreibvorgangs auftritt und sich somit nicht auf die Latenz auswirkt. Dieser Prozess ist wieder ähnlich wie die Datenbankprotokollierung. Eine Änderung an der Datenbank wird so schnell wie möglich in den Wiederherstellungsprotokollen aufgezeichnet und die Änderung wird dann als festgeschrieben bestätigt. Die Updates der Datendateien erfolgen viel später und haben keinen direkten Einfluss auf die Geschwindigkeit der Verarbeitung.

Bei einem Controller-Ausfall übernimmt der Partner-Controller die erforderlichen Festplatten und gibt die protokollierten Daten im NVRAM wieder, um I/O-Vorgänge, die beim Ausfall gerade ausgeführt wurden, wiederherzustellen.

Schutz vor Hardware-Ausfällen: NVFAIL

Wie zuvor bereits erläutert, wird ein Schreibvorgang erst bestätigt, wenn er in lokalem NVRAM und NVRAM auf mindestens einem anderen Controller angemeldet wurde. Dieser Ansatz stellt sicher, dass ein Hardware-Ausfall oder ein Stromausfall nicht zum Verlust der aktiven I/O führen Wenn der lokale NVRAM ausfällt oder die Verbindung zum HA-Partner ausfällt, werden diese aktiven Daten nicht mehr gespiegelt.

Wenn der lokale NVRAM einen Fehler meldet, wird der Node heruntergefahren. Dieses Herunterfahren führt zu einem Failover auf einen HA-Partner-Controller. Es gehen keine Daten verloren, da der Controller den Schreibvorgang nicht bestätigt hat.

ONTAP lässt kein Failover zu, wenn die Daten nicht synchron sind, es sei denn, das Failover wird erzwungen. Durch das Erzwingen einer solchen Änderung der Bedingungen wird bestätigt, dass Daten im ursprünglichen Controller zurückgelassen werden können und dass ein Datenverlust akzeptabel ist.

Datenbanken sind besonders anfällig für Beschädigungen, wenn ein Failover erzwungen wird, da Datenbanken große interne Daten-Caches auf der Festplatte aufbewahren. Wenn ein erzwungenes Failover auftritt, werden zuvor bestätigte Änderungen effektiv verworfen. Der Inhalt des Storage Arrays springt effektiv zurück in die Zeit, und der Zustand des Datenbank-Cache entspricht nicht mehr dem Status der Daten auf der Festplatte.

Um Daten aus dieser Situation zu schützen, können mit ONTAP Volumes für speziellen Schutz vor NVRAM-Ausfällen konfiguriert werden. Wenn dieser Schutzmechanismus ausgelöst wird, gelangt ein Volume in den Status „NVFAIL“. Dieser Status führt zu I/O-Fehlern, die dazu führen, dass Applikationen heruntergefahren werden, sodass keine veralteten Daten verwendet werden. Daten sollten nicht verloren gehen, da alle bestätigten Schreibvorgänge auf dem Speicher-Array vorhanden sein sollten.

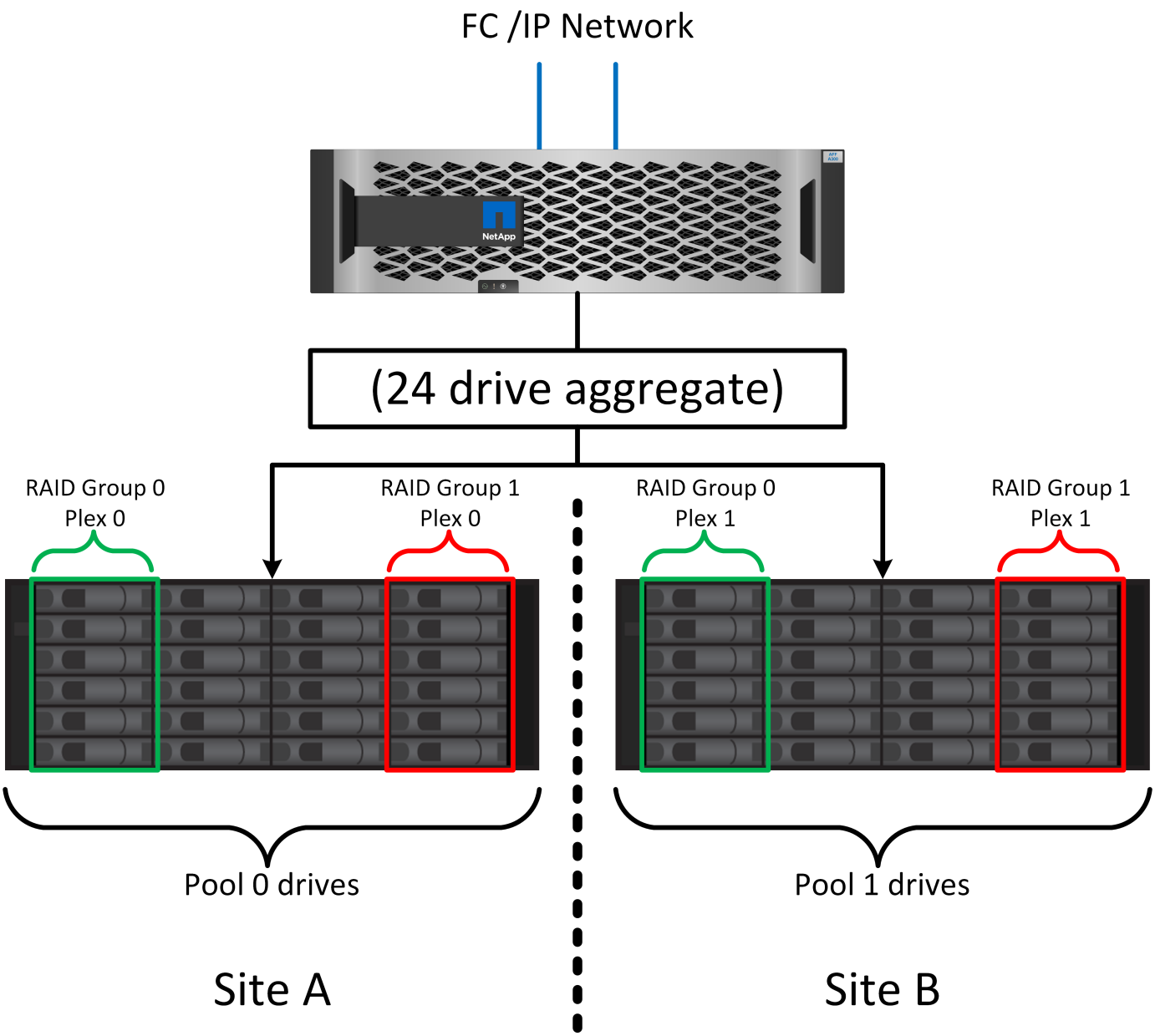
Als Nächstes muss ein Administrator die Hosts vollständig herunterfahren, bevor die LUNs und Volumes

manuell wieder online geschaltet werden. Obwohl diese Schritte etwas Arbeit erfordern können, ist dieser Ansatz der sicherste Weg, um die Datenintegrität zu gewährleisten. Nicht alle Daten erfordern diesen Schutz. Daher kann ein NVFAIL-Verhalten auf Volume-Basis konfiguriert werden.

Schutz vor Standort- und Shelf-Ausfällen: SyncMirror und Plexe

SyncMirror ist eine Spiegelungstechnologie, die RAID DP oder RAID-TEC verbessert, aber nicht ersetzt. Es spiegelt den Inhalt von zwei unabhängigen RAID-Gruppen. Die logische Konfiguration ist wie folgt:

- Laufwerke werden je nach Standort in zwei Pools konfiguriert. Ein Pool besteht aus allen Laufwerken an Standort A und der zweite Pool besteht aus allen Laufwerken an Standort B
- Ein gemeinsamer Storage Pool, auch bekannt als Aggregat, wird dann auf der Basis gespiegelter Gruppen von RAID-Gruppen erstellt. Von jedem Standort wird eine gleiche Anzahl von Laufwerken gezogen. Ein SyncMirror Aggregat für 20 Laufwerke würde beispielsweise aus 10 Laufwerken an Standort A und 10 Laufwerken an Standort B bestehen
- Jeder Laufwerkssatz an einem bestimmten Standort wird automatisch als eine oder mehrere vollständig redundante RAID-DP- oder RAID-TEC-Gruppen konfiguriert, und zwar unabhängig vom Einsatz der Spiegelung. So wird eine kontinuierliche Datensicherung auch nach dem Verlust eines Standorts gewährleistet.



Die Abbildung oben zeigt eine Beispiel-SyncMirror-Konfiguration. Es wurde ein Aggregat mit 24 Laufwerken auf dem Controller mit 12 Laufwerken aus einem an Standort A zugewiesenen Shelf und 12 Laufwerken aus einem an Standort B zugewiesenen Shelf erstellt Die Laufwerke wurden in zwei gespiegelte RAID-Gruppen gruppiert. RAID-Gruppe 0 enthält einen Plex mit 6 Laufwerken an Standort A, der auf einen Plex mit 6 Laufwerken an Standort B gespiegelt wird Ebenso enthält RAID-Gruppe 1 einen Plex mit 6 Laufwerken an Standort A, der auf einen Plex mit 6 Laufwerken an Standort B gespiegelt wird

Normalerweise wird SyncMirror für die Remote-Spiegelung bei MetroCluster Systemen verwendet, wobei eine Kopie der Daten an jedem Standort vorhanden ist. Gelegentlich wurde es verwendet, um eine zusätzliche Redundanz in einem einzigen System bereitzustellen. Insbesondere bietet sie Redundanz auf Shelf-Ebene. Ein Festplatten-Shelf enthält bereits duale Netzteile und Controller und ist im Großen und Ganzen etwas mehr als Bleche, doch in einigen Fällen ist möglicherweise der zusätzliche Schutz gewährleistet. Ein NetApp Kunde beispielsweise hat SyncMirror für eine mobile Echtzeitanalyse-Plattform für Automobiltests implementiert. Das System wurde in zwei physische Racks getrennt, die von unabhängigen USV-Systemen mit Strom versorgt wurden.

==Prüfsummen

Das Thema Prüfsummen ist von besonderem Interesse für DBAs, die es gewohnt sind, Oracle RMAN Streaming Backups zu Snapshot-basierten Backups zu verwenden. Eine Funktion von RMAN besteht darin, dass es während der Backups Integritätsprüfungen durchführt. Auch wenn dieses Feature einen gewissen Wert bietet, ist der Hauptvorteil für eine Datenbank, die nicht in einem modernen Storage-Array verwendet wird. Wenn physische Laufwerke für eine Oracle-Datenbank verwendet werden, ist es fast sicher, dass eine Beschädigung irgendwann auftritt, wenn die Laufwerke altern, ein Problem, das durch Array-basierte Prüfsummen in echten Storage-Arrays behoben wird.

Mit einem echten Storage-Array wird die Datenintegrität durch die Verwendung von Prüfsummen auf mehreren Ebenen gesichert. Wenn Daten in einem IP-basierten Netzwerk beschädigt sind, weist die TCP-Schicht (Transmission Control Protocol) die Paketdaten zurück und fordert eine erneute Übertragung an. Das FC-Protokoll umfasst Prüfsummen sowie eingekapselte SCSI-Daten. Nachdem es sich auf dem Array befindet, verfügt ONTAP über RAID- und Prüfsummenschutz. Es kann zu einer Beschädigung kommen, aber wie in den meisten Enterprise-Arrays wird sie erkannt und korrigiert. In der Regel fällt ein ganzes Laufwerk aus, was zu einer RAID-Neuerstellung führt, und die Datenbankintegrität bleibt davon unberührt. Seltener erkennt ONTAP einen Prüfsummenfehler, was bedeutet, dass die Daten auf dem Laufwerk beschädigt werden. Das Laufwerk ist dann ausgefallen, und die RAID-Wiederherstellung beginnt. Auch hier bleibt die Datenintegrität erhalten.

Die Architektur der Oracle-Datendatei- und des Wiederherstellungsprotokolls wurde auch für höchste Datenintegrität entwickelt, selbst unter extremen Bedingungen. Auf der einfachsten Ebene enthalten Oracle-Blöcke Prüfsumme und grundlegende logische Prüfungen mit fast jedem I/O Wenn Oracle nicht abgestürzt ist oder einen Tablespace offline genommen hat, sind die Daten intakt. Der Grad der Datenintegritätsprüfung ist einstellbar und Oracle kann auch zur Bestätigung von Schreibvorgängen konfiguriert werden. Dadurch können fast alle Crash- und Ausfallszenarien wiederhergestellt werden. Im äußerst seltenen Fall einer nicht wiederherstellbaren Situation wird eine Beschädigung umgehend erkannt.

Die meisten NetApp-Kunden, die Oracle-Datenbanken einsetzen, beenden die Nutzung von RMAN und anderen Backup-Produkten nach der Migration zu Snapshot-basierten Backups. Es gibt nach wie vor Optionen, mit RMAN Recovery auf Blockebene mit SnapCenter durchgeführt werden kann. Allerdings werden RMAN, NetBackup und andere Produkte täglich nur gelegentlich verwendet, um monatliche oder vierteljährliche Archivkopien zu erstellen.

Einige Kunden wählen zu laufen `dbv` Regelmäßige Integritätsprüfungen der vorhandenen Datenbanken durchführen. NetApp rät von dieser Vorgehensweise ab, da dadurch unnötige I/O-Last erzeugt werden. Wie oben erwähnt, wenn die Datenbank zuvor keine Probleme hatte, die Chance von `dbv` Das Erkennen eines Problems ist nahezu gleich null, und dieses Dienstprogramm erzeugt eine sehr hohe sequenzielle I/O-Last auf dem Netzwerk und dem Speichersystem. Es sei denn, es gibt Grund zu der Annahme, dass Korruption vorhanden ist, wie die Offenlegung eines bekannten Oracle-Fehlers, gibt es keinen Grund, ausgeführt zu werden `dbv`.

Grundlagen von Backup und Recovery

Oracle-Datenbanken und 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 NetApp FlexVol 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 NetApp FlexVol 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 FlexVol 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.

Schnelles Recovery von Oracle Database mit 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 von Oracle Datenbanken

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.

Oracle Database 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 das Management und die Automatisierung von Oracle Datenbanken

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.