



Automatisierung von Datenbank-Backups mit der Zero Data Loss Recovery Appliance

Ralf Zenses und Jan Brosowski, Oracle

Backups sind traditionell ein hochautomatisierter Bereich des Rechenzentrums-Betriebs. Im folgenden Artikel werden Backup-Ansätze mit ihren Vor- und Nachteilen vorgestellt sowie neue Herausforderungen bei der Backup-Automatisierung beleuchtet. Insbesondere wird auf die neue Technologie der Recovery Appliance eingegangen.

Seit vielen Jahren schon werden hierfür Automatismen eingesetzt:

- Scheduler starten automatisch Backup-Vorgänge einzelner Systeme oder Datenbanken.
- Backup-Clients erzeugen Snapshots auf Filesystemen, sie versetzen Datenbanken in Backup-Modus und deaktivieren diese wieder.
- Lifecycle-Management-Systeme sorgen dafür, dass nur notwendige Back-

ups aufgehoben werden und effizient mit Speicherplatz umgegangen wird.

- Band-Überwachungssysteme prüfen die Qualität der eingesetzten Medien und veranlassen bei Bedarf deren Kopie oder sortieren sie aus.
- Nicht zuletzt fahren weltweit Millionen von Robotern automatisch die richtigen Medien zu Bandlaufwerken und sorgen so für den wohl auffälligsten – weil physischen – Teil der Automatisierung von Backup-Tätigkeiten.

All diese klassischen Methoden der Automatisierung sind wohlbekannt und werden immer wieder überarbeitet und verbessert.

Neue Herausforderungen an die Backup-Automatisierung

Diese klassischen Methoden der Backup-Automatisierung sind allerdings vor dem permanenten Wandel, den wir im Betrieb von Datenbanken beobachten, nicht

mehr ausreichend, sie müssen um weitere Automatismen ergänzt werden:

- Die Zeitfenster für die Wiederherstellung und der zulässige Datenverlust (RTO und RPO) werden kleiner: Die Folge sind häufigere Backups und strengere SLAs für die Wiederherstellung. Häufig wird sogar ein maximaler Datenverlust von nahe Null verlangt, was klassische Backup-Umgebungen an den Rand ihrer technischen Möglichkeiten bringt.
- Zudem werden die Fenster für Backup-Aktivitäten geringer. Gerade Netzwerk-Bandbreite wird zu einem knappen Gut in Rechenzentren. Während sich die Datenmengen in den letzten 20 Jahren mehr als vertausendfacht haben (statt weniger Gigabyte pro Datenbank spricht man von wenigen Terabyte pro Datenbank), hat sich die Netzwerkbandbreite gerade mal verzehnfacht (von Gigabit als Quasi-Standard im Jahr 2000 zu 10 Gigabit als Quasi-Standard heute). Das geht mit gewaltigen Bewegungen im Netzwerk einher, insbesondere wenn Full Backups der Datenbanken angelegt werden müssen.

Doch rückt auch die eigentlich wichtigste Funktion des Backups wieder in das Zentrum der Betrachtungen: der Restore. Was nutzt ein angelegtes Backup, wenn man sich nicht sicher sein kann, im Falle der Fälle darauf zurückgreifen zu können, und man statt der angestrebten Stunden Tage und Wochen auf die Wiederherstellung wartet?

Daher werden Funktionen wie eine permanente Prüfung der Backups, Methoden zur Sicherstellung der Restaurierbarkeit und Methoden zur Pflege der gespeicherten Daten zentral. Außerdem rücken Methoden zur Sicherstellung von garantierten Wiederherstellungszeiten in den Fokus.

Datenbanken nehmen dabei eine Sonderstellung ein, die sie von Filesystemen unterscheidet: Sie unterliegen heute meist einem 24/7-Betrieb, in dem es keine lastarmen Zeiten mehr gibt. Zudem speichern sie in vielen Fällen besonders kritische Daten, auf die mit einer Vielzahl von Systemen zugegriffen wird.

Full Backups, Deduplication und Incremental Backups

Im Laufe der Zeit wurden verschiedene Maßnahmen, die sich bei Filesystemen

bewährt haben, auf Datenbanken übertragen. Um diese und ihre Auswirkungen auf Datenbank-Backups zu verstehen, sollen sie hier kurz beleuchtet werden.

Der klassische Weg des Backups ist der sogenannte Full Backup: Alle Dateien eines File-Systems oder alle Blöcke einer Datenbank werden auf ein Backup-System übertragen. Dies hat einen klaren Vorteil: Das Backup ist vollständig und konsistent. Auch kann es in vorhersagbarer Zeit vollständig zurückgesichert werden. Es hat jedoch zugleich einen großen Nachteil: Es ist sehr groß, insbesondere wenn mehrere Backup-Generationen aufgehoben werden sollen, und seine Übertragung in das Backup-System dauert lange.

Dieser Schwäche begegnete man mit dem Ansatz der Deduplizierung: Auf dem Backup-System nahm man das neue Full Backup entgegen und verglich die Inhalte mit den schon vorhandenen Backups. Waren zwei Blöcke oder Dateien identisch, wurde dieser Block oder diese Datei nur einmal abgelegt und aus mehreren Backups verlinkt. Somit sank zumindest der Speicherplatzbedarf, die Daten mussten dennoch übertragen werden. Heute verliert Deduplizierung immer mehr an Bedeutung, da sie nicht in der Lage ist, mit verschlüsselten Backups umzugehen. Dies ist allerdings gerade bei Cloud-Umgebungen, hochgradig konsolidierten Umgebungen oder bei der Verarbeitung personenbezogener Daten der Quasi-Standard für den Datenbankbetrieb geworden.

Um der Schwäche der zu übertragenden großen Datenmenge zu begegnen, erkannte man früh die Möglichkeit des sogenannten inkrementellen Backups: Statt aller Daten werden nur die Daten übertragen, die sich verändert haben. Bei File-Systemen ist dies ein weitverbreiteter Ansatz, und auch bei Datenbanken hat er sich bewährt. Leider geht er im Falle des Restore bei Datenbanken mit einem sehr unangenehmen Effekt einher. Statt nur eines einzigen Backups müssen mehrere in der richtigen Reihenfolge verwendet werden: Zunächst muss der letzte Full Backup zurückgespielt werden; anschließend müssen alle inkrementellen Backups zwischen dem letzten Full Backup und dem Zeitpunkt der Wiederherstellung angewendet werden. Dies kann eine Wiederherstellung unberechenbar langsam machen.

Daher ist in der Praxis eine Mischform aus regelmäßigen Full Backups (beispielsweise wöchentlich) mit täglichen inkrementellen Backups üblich. Sie kombiniert die Platzersparnis und kurze Laufzeit der inkrementellen Backups mit noch erträglichen Wiederherstellungszeiten, da maximal 6 inkrementelle Backups nach der Wiederherstellung des Full Backups angewandt werden müssen.

In vielen Fällen erreicht diese Strategie schon heute ihre Grenzen, gerade bei steigenden Anforderungen an Verfügbarkeit, bei weiterhin wachsenden Datenbanken und der nicht mitwachsenden Netzwerkbandbreite. Daher ist ein neuer Ansatz notwendig.

Incremental Forever mit Virtual Full Backups

Die Lösung hier ist eine andere Herangehensweise, die Oracle in der Zero Data Loss Recovery Appliance (kurz „Recovery Appliance“) umgesetzt hat. Wichtigstes Element ist hierbei eine gewisse Intelligenz der Recovery Appliance: Sie versteht den Aufbau einer Oracle-Datenbank aus ihren Datenblöcken.

Der erste Teil ist hierbei eine Strategie, die als Incremental Forever bekannt ist. Es wird einmalig ein Full Backup angefertigt und anschließend nur noch Incremental Backups. Somit sind die einzelnen Backup-Fenster kurz, die übertragene Datenmenge gering. Zwei wichtige Ziele sind also erreicht.

Um nun zu vermeiden, im Falle eines Restore alle Incremental Backups nacheinander anwenden zu müssen, ist die Recovery Appliance in der Lage, den Inhalt der Backups zu verstehen und auszuwerten. Dadurch kann sie auf Datenbank-Block-Ebene entscheiden, aus welchen Blöcken ein Full Backup zu einem bestimmten Zeitpunkt bestehen muss. Sie erzeugt dieses sogenannte Virtual Full Backup im Moment des Abrufes aus den Blöcken der vorliegenden Incremental Backups und des initialen Full Backups. Es wird also kein zusätzlicher Speicherplatz belegt, es werden lediglich Pointer angelegt. *Abbildung 1* gibt einen Überblick am Beispiel von 4 nacheinander durchgeführten Incremental Backups einer Datenbank, die aus 5 Blöcken besteht.

An Tag 0 wurde ein Full Backup angelegt, bestehend aus den fünf Blöcken A-E,

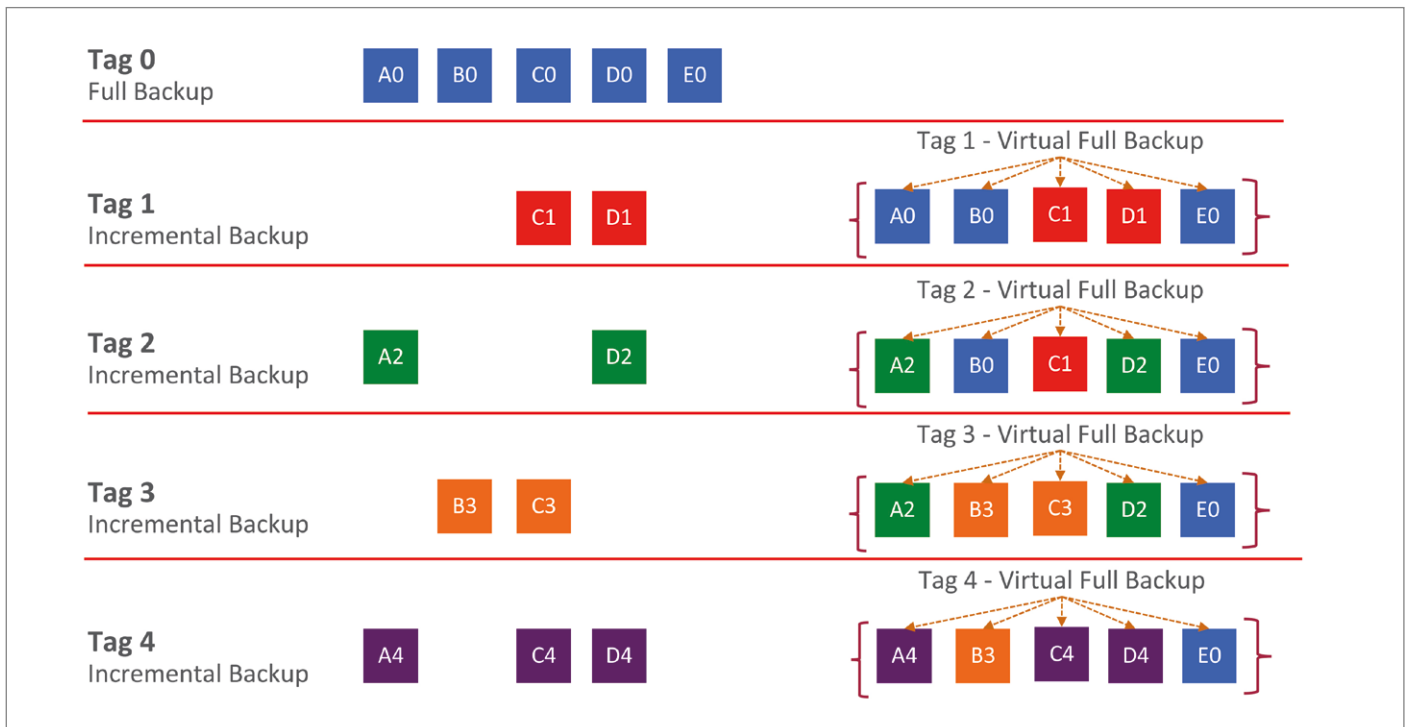


Abbildung 1: Strategie des Virtual Full Backups (Quelle: Ralf Zenses)

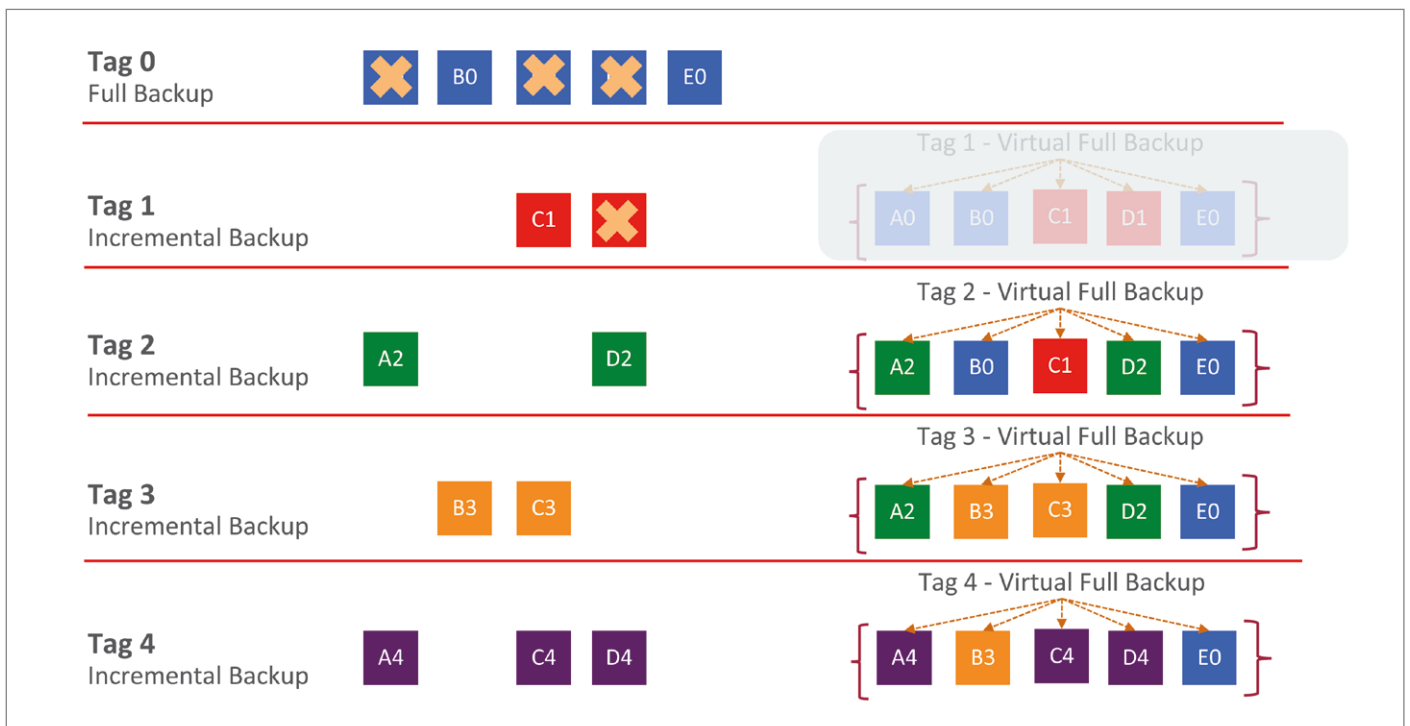


Abbildung 2: Gezieltes Löschen nicht mehr benötigter Datenblöcke (Quelle: Ralf Zenses)

jeweils mit dem Index 0 für Tag 0. An den folgenden Tagen wurden nur Incremental Backups angelegt, die jeweils aus den veränderten Blöcken bestehen (beispielsweise an Tag 3 die Blöcke B und C, jeweils mit Index 3 für den Tag 3).

Aus diesen Blöcken kombiniert die Recovery Appliance dann Virtual Full Backups. Man sieht beispielsweise, dass der

Virtual Full Backup am Tag 3 aus den Blöcken A und D von Tag 2, den Blöcken B und C von Tag 3 sowie dem Block E von Tag 0 besteht.

Durch diese Logik wird auch vermieden, dass man alle Incremental Backups aufbewahren muss. Besteht die Notwendigkeit, den Zustand der drei letzten Tage wiederherstellen zu können, müssen nur

die Blöcke aufbewahrt werden, die an einem dieser drei Tage Bestandteil eines Full Backups wären. Alle übrigen Blöcke können gelöscht werden. In *Abbildung 2* wird dieser Effekt dargestellt.

Im Beispiel sieht man, dass nur die Virtual Full Backups der Tage 2 bis 4 benötigt werden. Folglich sind nur die Blöcke, die in diesen Virtual Full Backups enthalten

sind, aufzubewahren. Dies sind die Blöcke A2 und A4, B0 und B3, C1, C3 und C4 und so weiter. Nicht mehr notwendig sind die Blöcke A0, C0, D0 und D1. Sie können gezielt aus den Backups entfernt werden.

Ein wichtiger Aspekt ist hierbei, dass die Blöcke so aufbewahrt werden, dass der jeweils letzte Stand schnell abrufbar ist – mit hoher Wahrscheinlichkeit wird er bei einem Restore benötigt. Daher werden die Blöcke so angeordnet, dass der jeweils aktuelle Zustand der Datenbank repräsentiert wird.

All diese Operationen geschehen automatisch im Hintergrund, die Administratoren brauchen sich um nichts zu kümmern.

Permanente Konsistenz-Überprüfung

Die Recovery Appliance muss durch diese Strategie Datenbankblöcke regelmäßig „anfassen“: Beim Entgegennehmen im Incremental Backup, beim Umsortieren zur Sicherstellung schneller Restore-Zeiten und bei der Analyse, ob Blöcke noch benötigt werden. Bei jedem dieser Schritte überprüft die Recovery Appliance die Konsistenz des Blockes durch Check-Summen. Somit können eventuell später auftretende Restore-Probleme frühzeitig erkannt und auch vermieden werden. Zum einen speichert die Recovery Appliance jeden Block mehrfach ab und kann so den Großteil der Probleme direkt selbst lösen. Sollten alle Kopien des Blocks defekt sein – beispiels-

weise durch Netzwerkfehler während des Incremental Backups – kann sie den Block erneut bei der Datenbank anfordern.

Somit werden automatisch die größten Probleme und größten Risiken eines fehlerhaften Restore ausgeschlossen und die Qualität des gesamten Prozesses deutlich erhöht.

Zero Data Loss

Der vollständige Name der Recovery Appliance besagt, dass es einen weiteren, ebenfalls automatisierten Baustein gibt, der die Zeit zwischen dem letzten Incremental Backup und dem Moment des Zusammenbruchs einer Datenbank abdeckt – nur dann kann man von einem Restore ohne Datenverlust sprechen.

Bei klassischen Verfahren sichert man zu diesem Zweck die sogenannten Archive Logs der Datenbank gesondert ab, da man mit diesen die Änderungen im genannten Zeitraum „nachziehen“ kann. Durch permanentes Sichern der Archive Logs sind so kürzere RPOs möglich, die sich aber immer noch weit von Null entfernt befinden.

Die Recovery Appliance nutzt hier eine Technologie namens Delta, über die Datenbanken permanent alle Schreib-Tätigkeiten an die Recovery Appliance replizieren. Dieser Datenstrom von Änderungen wird innerhalb der Recovery Appliance aufgezeichnet und es werden virtuelle Archive Logs daraus generiert. Diese können – ebenso wie die echten Archive Logs

– für ein Nachziehen der Änderungen seit dem letzten Incremental Backup genutzt werden. Sie sind jedoch deutlich aktueller als die Archive Logs einer Datenbank, da sie annähernd synchron zum Datenbank-Betrieb mitgeführt werden.

Auch dieser Prozess ist vollständig automatisiert. Administratoren schalten ihn in der sogenannten Backup-Policy ein, die gesamte weitere Konfiguration wird automatisch durchgeführt.

Steuerung und Überwachung mittels Policies

Dies leitet zu einem wichtigen Bestandteil der Recovery Appliance über: der Steuerung und Überwachung der beschriebenen Mechanismen. Heute sind in Unternehmen Hunderte, wenn nicht Tausende von Oracle-Datenbanken im Einsatz; daher müssen nicht nur die Mechanismen selbst, sondern auch deren Einsatz und die Überwachung hochgradig automatisiert sein.

Daher nutzt die Recovery Appliance hier einen Policy-basierten Ansatz. Administratoren definieren einmal einen Satz von Regeln (Policies) dafür, welche Parameter bei Backup und Restore eingehalten werden sollen (RPO und RTO), sowie daraufhin, ob ein kontinuierliches Backup erfolgen soll. Diese Regeln bekommen eigene Namen (beliebt: Platin, Gold, Silber, Bronze. Andere Namen sind natürlich möglich).

Dann werden Datenbanken diesen Policies zugewiesen. Alle weiteren Konfigu-

	Klassische Full Backups in Standard-Backup-Umgebungen	Wöchentliche Full- + tägliche Incremental-Strategien in Standard-Backup Umgebungen	Virtual Full + Incremental Forever auf Recovery Appliance
Sicherungsvorgang	Sehr langsam: gesamte Datenbank wird bei jedem Backup übertragen	Überwiegend schnell: Beim wöchentlichen Full Backup langsam, bei Incrementals schnell	Schnell: nur beim ersten Backup wird ein Full Backup angefertigt, dann nur noch schnelle Incremental Backups
Last auf dem Netzwerk beim Sicherungsvorgang	Hoch	Beim wöchentlichen Full Backup hoch	Niedrig, außer beim initialen Backup
Recovery-Vorgang	Schnell: ein Full Backup wird zurückgesichert	Langsam, da alle Incrementals nacheinander übertragen und angewendet werden müssen	Schnell: ein Virtual Full Backup wird zurückgesichert.
Speicherplatzbedarf	Sehr hoch, insb. bei verschlüsselten Daten	Gering	Sehr gering
Recovery-Garantie	Keine Prüfung der Konsistenz durch die Backup-Umgebung	Permanente Prüfung des Backups	
Zero-Data-Loss-Strategie	Ansatzweise möglich durch regelmäßige Sicherung von Archive Logs. Datenverlust reduziert in den Bereich von Minuten-Stunden	Teil des Konzepts durch Delta-Push. Datenverlust im Bereich Null bis wenige Sekunden	

Tabelle 1

rationen übernimmt dann die Recovery Appliance, sodass ein Administrator nur wenig machen muss.

In der Folge sieht der Administrator dann, wie die Einhaltung der Policies funktioniert: Er kann so frühzeitig erkennen, ob unter Umständen zusätzlicher Storage-Bedarf besteht oder ob es technische Probleme bei einzelnen Backups gibt.

Zusammenfassung

Ein neues Backup-Konzept wie das der Recovery Appliance mag auf den ersten Blick ungewohnt sein, doch bietet es durch seine hohe Automation deutliche Vorteile gegenüber traditionellen Ansätzen. Durch das Incremental Forever Backup werden wertvolle Zeit und Netzwerk-Ressourcen im Alltag gespart und durch die innovativen Virtual Full Backups wird das Rücksichern einer Datenbank deutlich beschleunigt und vereinfacht. Vielfäl-

tige Automatisierungen helfen dem Administrator, das Backup einfacher, aber auch sicherer zu gestalten. *Tabelle 1* fasst die wichtigsten Merkmale zusammen.

Eine letzte Besonderheit sei zum Abschluss noch genannt: die Integration mit RMAN. Datenbankadministratoren sind es gewohnt, mit RMAN zu arbeiten. Gerade in stressigen Situationen – wie dem Zurücksichern einer Datenbank aus dem Backup – ist es zentral, durch eine neue Technologie wie die Recovery Appliance keine zusätzlichen Stress-Auslöser einzuführen. Daher wurde die Recovery-Appliance so in RMAN integriert, dass sich die Befehle für die Administratoren nicht verändern. Die gesamte „Magie“ der Recovery Appliance, die das Backup auf eine qualitativ neue Stufe hebt, wird in solch stressigen Situationen vollständig verborgen und läuft automatisiert ab. So können sich die beteiligten Menschen auf ihre Tätigkeiten konzentrieren.



Ralf Zenses
Ralf.Zenses@Oracle.com



Jan Brosowski
jan.brosowski@oracle.com

Eventpartner: **AUG** **SUG** swiss oracle user group **IUG** Verbund **ORACLE**

2019
DOAG
Konferenz + Ausstellung
19. - 22. November in Nürnberg

EARLY BIRD
BIS ZUM
30. SEPT.



2019.doag.org