Vereinheitlichung und Automatisierung von Backup und Cloning

Christof Gliem
gkv informatik
Lichtscheider Straße 89, 42285 Wuppertal

Schlüsselworte
Backup, Cloning, SAP, NONSAP, Automation, große und kleine Datenbanken, BR*TOOLS, RMAN, 9i, 10g, 11g, Standardisierung

Einleitung

Das Thema „Vereinheitlichung und Automatisierung von Backup und Cloning“ ist aus einer internen Anforderung entstanden, Arbeitsaufwände zu reduzieren und Verfahren zu standardisieren. Zu Beginn wird auf die gesteckten Anforderungen eingegangen. Anschließend werden die Verfahren Online-Sicherung und Cloning mittels Redirected-Restore anhand der Anforderungen dargestellt. Dabei liegt die besondere Schwierigkeit darin, die verschiedenen Oracle Versionen abzudecken und die offiziell supporteten Tools RMAN und BR*TOOLS gleichermaßen zu berücksichtigen. Nach der Lösungsvorstellung werden die Vorteile herausgestellt. Auf die Vorteile beim Datenschutz und Datensicherheit wird danach gesondert eingegangen. Abschließend werden die Probleme bei der Umsetzung der vorgestellten Lösung aufgezeigt und zukünftige Weiterentwicklungen kurz erläutert.

Vereinheitlichung und Automatisierung von Backup und Cloning

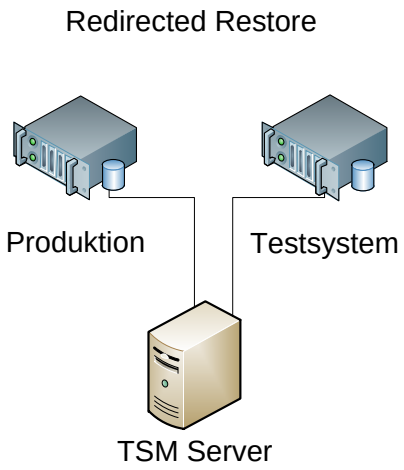
Vor Beginn der Lösungsentwicklung werden die Anforderungen aufgenommen. Dabei ist bei dem Unternehmen gkv informatik ein wichtiger Aspekt, dass die Lösung möglichst kostengünstig ist. Es soll keine neue Hardware oder Software eingekauft werden. Gegeben sind die gängigen kostenlosen Sicherungsstools RMAN und BR*TOOLS. RMAN ist das Tool für NONSAP Datenbanken. BR*TOOLS wird von SAP geliefert und ist demensprechend besonders für SAP Datenbanken geeignet. Weiterhin ist eine 1 Gbit LAN und eine SAN Infrastruktur vorhanden. Die mögliche Lösung soll Oracle Versionen von 9i bis 11g unterstützen und keine Besonderheiten eines Betriebssystems ausweisen. Das entwickelte Skript soll unter Linux genauso wie unter AIX und Solaris funktionieren. Das Automationstool UC4 steuert sowohl die entwickelten Sicherungsjobs als auch die Cloningjobs automatisch ohne manuelles eingreifen. Die Onlinezeiten der produktiven Datenbank dürfen nicht beeinträchtigt werden. Das heißt, dass sowohl die Sicherung als auch das Cloning zur Onlinezeit durchführbar sein soll. In Zusammenarbeit mit der internen Architekturabteilung sind folgende Sicherungs- und Wiederherstellungszeiten entstanden:

Maximale Sicherungsdauer	6 Stunden
Logsicherung	alle 30 Minuten
Rücksicherung aus fachlichen Gründen	< 30 Minuten
Rücksicherung aus technischen Gründen	6 Stunden ± 10%

Voraussetzung ist, dass Wiederherstellungszeiten gleich Sicherungszeiten sind.

Die genannten Anforderungen werden in folgendem Lösungsvorschlag beachtet:
Um die Zeit kleiner 30 Minuten bei einer fachlichen Rücksicherung zu erreichen, wird auf Oracle Flashback Technologie zurückgegriffen. Diese Technologie ist zwar erst ab Version 10g möglich, jedoch werden in der gkv informatik nur Altanwendungen mit unsupporteten Oracle Versionen

betrieben. Produktive Datenbanken mit regelmäßig vielen DML-Statements laufen unter Oracle 11g. Aber auch die Datenbankgröße ist bei Altanwendungen eher gering, sodass man die 30 Minuten auch mittels einer normalen Wiederherstellung einhalten kann. Als Sicherungsverfahren wird sowohl bei SAP als auch bei NONSAP eine Kombination zwischen Online-Vollsicherung und Archivelogsicherungen gewählt. Bei NONSAP Datenbanken wird zusätzlich noch inkrementell gesichert, um das Backupvolumen zu verringern. Die Oracle Softwareinstallation wird mit einer normalen Filesystemsicherung gesichert. Die NONSAP Datenbanken kommunizieren mit dem RMAN Katalog. Dort sind für Datenbanken ab 11g auch Sicherungsskripte hinterlegt. Mithilfe des RMAN Befehls `CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF XX DAYS` wird die Aufbewahrungszeit definiert. Im SAP Bereich werden die Einstellungen im utl-File mit dem Parameter `MAX_VERSIONS` vorgenommen. Vollsicherungen laufen einmal wöchentlich. Täglich findet bei NONSAP Datenbanken eine inkrementelle Sicherung statt. Bei SAP und NONSAP Datenbanken läuft alle 30 Minuten eine Archivelogsicherung inkl. eines erzwungenen Logswitches. Dadurch wird ein Datenverlust größer 30 Minuten vermieden.
Das Cloningverfahren Redirected-Restore setzt das genannte Sicherungsverfahren voraus:



Beim Redirected-Restore wird eine Sicherung der produktiven Datenbank in eine Testdatenbank eingespielt. Durch Mitgabe eines Zeitstempels wird ein Datenbank-Point-In-Time Restore durchgeführt. Dieses Verfahren wird sowohl von BR*TOOLS als auch RMAN unterstützt. Dabei findet automatisch durch die genannten Tools ein Umbenennen der Datenbank inkl. Datenbankdateien statt. Durch eine Wiederherstellung der Sicherungsdaten bleibt das produktive System unangetastet und die Performance wird nicht beeinträchtig. Bei dem Refresh einer Testumgebung müssen zu Beginn verschiedene Vorarbeiten erledigt werden. Unter anderem müssen alte Sicherungen gelöscht und die Sicherungen der produktiven Datenbank der Testdatenbank zugänglich gemacht werden. Die anfangs genannten Sicherungs- und Wiederherstellungszeiten können mithilfe verschiedener Sicherungsziele erreicht werden:

Kleine Datenbanken 0 – 300GB	LAN Sicherung
Mittlere Datenbanken 300GB – 1TB	SAN mittels LANFREE auf DataDomain
Große Datenbanken > 1TB	SAN mittels LANFREE auf Tape Laufwerke - pro Tape 120 MB/s

Die reale Wiederherstellungszeit wird mit dem genannten Cloningverfahren automatisch regelmäßig überprüft. Sollte die Wiederherstellung widererwarten länger dauern, kann die Parallelität der Sicherungskanäle erhöht oder ein neues Sicherungsziel definiert werden. Achtung: Die parallelen

Sicherungskanäle sind eine Option der Oracle Enterprise Edition. Der Automationsprozess sieht vor, dass vor einem Clon eine neue Vollsicherung erstellt wird, damit weniger Archivelogs applied werden müssen. Mithilfe des Automationstools UC4 ist es möglich, den Clonjob automatisch nach Beendigung des Sicherungsjobs laufen zu lassen. Dabei wird der Zeitstempel auf das Ende der Vollsicherung gesetzt. Es gilt zu beachten, dass nach der Vollsicherung noch eine Archivelogsicherung laufen muss, da sonst die Gefahr besteht, dass eine Clonerstellung fehlschlägt, da die erstellte Onlinesicherung unterschiedliche SCN's inne hat.

Der beschriebe Lösungsvorschlag hat den Vorteil, dass man sehr einfach die Backup und Cloninggeschwindigkeit variieren kann. Je mehr Kanäle man dazuschaltet, desto schneller ist die Sicherung oder die Wiederherstellung beendet. Bei dem Hinzunehmen von weiteren Kanälen sollte die CPU und RAM Auslastung des Systems beobachtet werden, da mehr Kanäle auch mehr Ressourcen benötigen. Das beschriebene Konstrukt, Verwendung von den Standardtools RMAN und BR*TOOLS, bietet weiterhin den Vorteil, dass der TSM als Backendsicherungssoftware leicht ersetzbar ist. Die Kommunikation mit dem TSM findet über eine API Schnittstelle statt, welche auch andere Sicherungstools bieten. Aufkommende Fehler können außerdem wie gewohnt über Metalink analysiert und behoben werden.
Sollte ein Clonversuch fehlschlagen, so ist es mit der beschrieben Lösung ohne weiteres möglich, den Redirected-Restore nochmal zu starten. Außerdem lässt sich der Cloningzeitpunkt auch nach der Vollsicherung noch variieren. Der positive Nebeneffekt des Redirected-Restores ist, dass getestet wird, ob die erstellte Sicherung auch wie erwartet funktioniert. Der automatische Indexrebuild von nologging Indexen bei BR*TOOLS verhindert logische Block Corruption. Um diesem Fehler generell vorzubeugen, empfiehlt sich das Einschalten des Datenbank Parameters `FORCE LOGGING`.
Der Vorteil der beschriebenen Sicherungsziele ist, dass die Sicherungen von großen Datenbanksystemen auf günstigem Tapespeicher liegen. Tapes sind aktuell immer noch ein sehr günstiges Speichermedium.

Neben den technischen Aspekten eines Backup und Cloning Konzeptes sollten auch die rechtlichen Rahmenbedingungen beachtet werden. Erste Empfehlungen liefert das Bundesdatenschutzgesetz (BDSG) in § 9 Nr. 7 Verfügbarkeitskontrolle. Dort werden generelle Sicherungen von Daten verlangt. Die Sicherungen sollten weiterhin ausfallsicher aufbewahrt werden. Dies lässt sich zum Beispiel durch ein Kopieren in ein zweites Rechenzentrum erreichen. Da die gkv informatik ein Unternehmen ist, welches mit Sozialdaten arbeitet, kommt auch das Sozialgesetztbuch (SGB) 10 § 78a zu tragen. § 9 Nr. 8 des BDSG geht auf die Trennung der Daten ein. In dem beschriebenen Konzept werden die Sicherungsdaten im TSM getrennt. Im TSM besitzt jede Datenbank einen eigenen TSM Node. Ein TSM Node ist logisch von anderen Nodes getrennt, ähnlich wie Schemata in einer Oracle Datenbank. Auch in der ISO Norm 270001 A12.3.1 werden Sicherungen inklusive regelmäßiger Wiederherstellungstests gefordert. Eine weitere Institution, die sich mit dem Thema beschäftigt, ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Diese stellen mögliche Gefahren und die dazu passenden Maßnahmen heraus. Nachfolgend werden einige Maßnahmen tabellarisch herausgestellt und Werte der gkv informatik vorgestellt:

BSI 5.7, M6.49 Datensicherung	**Werte der gkv informatik**
Datenvolumen	Aufteilung auf FULL, INCR und ARCH
Maximal verkraftbarer Datenverlust	Maximaler Verlust 30 Minuten bei dem Fall rm –rf /*
Wiederanlaufzeit	Für den Fall rm –rf /* maximal 6 Stunden
Sicherungsmöglichkeiten der Software	Erfolgt über Filesystemsicherung

BSI 5.7, M6.51 Wiederherstellung Prüffragen	Werte der gkv informatik
Gibt es ein Konzept, das die Abläufe einer Wiederherstellung regelt?	Ja, das Cloningkonzept
Wird die Wiederherstellung regelmäßig geprobt?	Ja, durch regelmäßiges Cloning
Wird regelmäßig geprüft, ob genügend Speicherkapazitäten für eine Wiederherstellung verfügbar sind?	Ja, durch regelmäßiges Cloning

Die genannten rechtlichen Rahmenbedingungen und Empfehlungen sind mit dem erarbeiteten Lösungskonzept konform.

Bei der Umsetzung der Lösung sind verschiedene Probleme aufgetaucht. Ein großes Problem ist gewesen, dass die Differenz zwischen praktischer und theoretischer Performance sehr groß war. Dies hat verschiedene Gründe.
Der Parameter `Multiplexing` war nicht korrekt gesetzt. Der Parameter ist bei großen Datenbanken besonders spürbar, wenn sich folgende Konstellation ergibt:
Die Datenbank wird mit sechs Kanälen gesichert. Der Parameter `Multiplexing` steht auf eins. Der theoretische Wert liegt bei 120 MB/s pro Kanal. Im ungünstigen Fall liegen sechs Datendateien auf der gleichen physikalischen Disk. Es ist aber nicht möglich, diese Disk mit 6x120 MB/s zu lesen. Daher sinkt die Sicherungsperformance. Wenn man den Parameter auf den Wert acht setzt, verringert dies die Wahrscheinlichkeit solcher ungünstigen Konstellationen.
Ein weiteres Problem ist die automatische Komprimierung des Backupendclients. Wenn die Komprimierung eingestellt ist, wird nur ein Bruchteil der Tapegeschwindigkeit erreicht.
Fehlkonfigurationen, die bewirken, dass Sicherungen über LAN statt über SAN gehen, sind auch aufgetreten. Wenn zu viele Kanäle geöffnet oder zu viele Sicherungen parallel auf einem System laufen, sinkt die Geschwindigkeit, da das System zu startk ausgelastet ist. Das Optimum zu finden, gelingt oft nur durch ausprobieren.
Beim Cloning ist das Problem aufgetreten, dass eine Rücksicherung nicht möglich war. Die normale Sicherung hat zwar funktioniert, aber der TSM Server konnte aufgrund von fehlkonfigurierten SAN Pfaden die Sicherung nicht zur Datenbank senden.
Neben den Performanceproblemen sind auch diverse Schwierigkeiten mit dem RMAN Katalog aufgetaucht. Zum einen sollten DBID's innerhalb eines Unternehmens eindeutig sein. Der RMAN Katalog benutzt diese als Primärschlüssel für die Sicherungsmetadaten. Sollten zwei Datenbanken die gleiche DBID besitzen, so werden Sie intern im RMAN Katalog als Inkarnationen geführt.
Nicht mehr aktive Datenbanken haben den Katalog zusätzlich unnötig aufgebläht. Mit dem SQL-Statement

```
select db_name, min(completion_time) from
RC_BACKUP_CONTROLFILE group by db_name
having min(completion_time) < sysdate-40;
```

lassen sich Datenbanken finden, welche seit 40 Tagen kein Controlfilebackup mehr erstellt haben. Anschließend können die Datenbanken mit dem Katalog Package `dbms_rcvcat.unregisterdatabase` entfernt werden. Wenn der Resync der Datenbanken zu lange läuft, empfiehlt sich Doc ID 1600112.1 Dort wird ein Hinweis gegeben, wie die Tabelle `ROUT` frühzeitiger bereinigt wird. Diese ist oft der Grund für einen lang laufenden Resync.

Die Zukunft der Sicherungen bei der gkv informatk sieht folgendermaßen aus:
Alle Datenbanksicherungen gehen über ein 10 Gbit LAN auf einen TSM Disk Pool, welcher auf dem verteilen Filesystem GPFS angelegt ist. Die Deduplizierung ist am effektivsten, wenn der Parameter `FILESPERSET` auf eins gesetzt ist. Dann finden sich mehr gemeinsame Blöcke zwischen den

Backupsets der Vollsicherungen. Außerdem empfiehlt es sich, die RMAN Komprimierung ausgeschaltet zu lassen. Dies spart Performance auf dem Client Server ein und die Komprimierungsrate auf dem TSM Server ist nahezu genauso effektiv. Der Vorteil dieses Konstruktes ist, dass man auf keine physikalischen Ressourcen wie Bandstationen angewiesen ist und mit sehr vielen Clients gleichzeitig in den großen Sicherungspool schreiben kann. Durch das verteilte Filesystem bietet der Pool auch genug I/O Durchsatz.

Kontaktadresse:
Christof Gliem
gkv informatik
Lichtscheider Straße 89
D-42285 Wuppertal

Telefon: +49 202 6958-1249
E-Mail christof.gliem@gkvi.de
Internet: www.gkvi.de