Datensicherheit und Verfügbarkeit mit der Oracle Standard Edition

Jochen Kutscheruk
merlin.zwo InfoDesign GmbH & Co. KG
Karlsruhe

Schlüsselworte

Datensicherheit, Hochverfügbarkeit, Recovery-Zeit, MTTR, Standard Edition, Ausfallzeit

Einleitung

In der Enterprise Edition bietet Oracle mit DataGuard und Real Application Cluster die Möglichkeit, eine Umgebung mit maximaler Verfügbarkeit und Datensicherheit aufzubauen. Diese Möglichkeiten gibt es in der Standard Edition (SE/SE1/SE2) nicht oder nur teilweise.

In diesem Vortrag wird darauf eingegangen, wie die Verfügbarkeit und Datensicherheit auch mit einer Standard Edition (SE/SE1/SE2) zumindest näherungsweise gewährleistet werden kann, welche Einschränkungen dabei in Kauf genommen werden müssen und ab wann der Einsatz einer Enterprise Edition sinnvoll oder notwendig ist.

Die Ausgangssituation

Datensicherheit und Verfügbarkeit der zentralen Datenbank(en) spielen bereits seit Jahren eine immer größere Rolle. Die IT-Abteilungen konsolidieren sinnvollerweise die Unternehmens-Datenbanken an einem zentralen Standort. Dies führt dazu, dass auch die weltweit verteilten Werke oder Niederlassungen von diesem zentralen Standort und der Verfügbarkeit der Datenbanken dort abhängig sind. Falls also z.B. die Datenbank für die Produktion ausfällt, so ist nicht nur ein Werk betroffen, sondern alle Werke weltweit.

Die Verfügbarkeit der zentralen Datenbanken muss daher (fast) rund um die Uhr gewährleistet sein. Und zur Verfügbarkeit gehört selbstverständlich auch die Datensicherheit der vorhandenen Daten – ohne valide Daten ist eine Datenbank nutzlos, selbst wenn sie verfügbar ist.

Datensicherheit im Sinne des BDSG

Datensicherheit im Sinne des BDSG kann mit der Oracle Standard Edition nicht gewährleistet werden. Es gibt datenbankseitige keine Möglichkeit – über das Oracle Rechtekonzept hinaus - Daten nur einem bestimmten Personenkreis zugänglich zu machen, also z.B. nur bestimmte Zeilen oder Spalten einer Tabelle anzuzeigen oder nur verschleierte Daten anzuzeigen oder Datenbankinhalte zu verschlüsseln und den Zugriff nur über ein 4-Augen-Prinzip zu ermöglichen. Dazu wird die Oracle Enterprise Edition und gegebenenfalls zusätzliche Optionen benötigt.

Auch die Überwachung des reinen Zugriffs auf die Daten (select) ist nur mit der Enterprise Edition möglich (Fine Grained Auditing).

Die Wirklichkeit

In unserer täglichen Arbeit treffen wir immer wieder auf Oracle Datenbanken, für die kein brauchbares Sicherungs- und Wiederanlaufkonzept existiert. Datenbanken werden per EXPDP oder

sogar EXP gesichert, Datenbanken laufen im Noarchivelogmodus, Datenbanken werden jede Nacht heruntergefahren und kalt gesichert, Datenbanken werden über einen Snapshot auf der Storage gesichert, ...

Oftmals ist den Kunden dabei nicht bewusst, was Sie damit riskieren. „Das machen wir seit Oracle 8 (oder 7) so, das hat immer funktioniert“. Es wurde jedoch teilweise seit Jahren nicht mehr getestet, wie lange denn ein Neuaufbau der Datenbank mit diesen Verfahren tatsächlich benötigt und wie sich der damit verbundene Datenverlust in der Praxis auswirkt.

Je nach verwendetem Sicherungsverfahren kann selbst die Wiederherstellung einer kleinen Datenbank von 10GB über zwei Stunden in Anspruch nehmen, bei einer Datenbankgröße von 300GB sind es schon mehrere Stunden. Ganz zu schweigen vom Datenverlust: oftmals kann nur der Stand der letzten Nacht wiederhergestellt werden.

Diese Art der Sicherung ist keinesfalls zeitgemäß.

Welche Datensicherheit und Verfügbarkeit lässt sich mit der Standard Edition erreichen?

Eins vorweg: die Datensicherheit und Verfügbarkeit, die mit einer Enterprise Edition erreicht werden können, lassen sich mit der Standard Edition nicht erreichen.

Beispielsweise existieren folgende nützlichen Features in einer EE nicht: Online Block Repair, Flashback Database, Flashback Table, Flashback Transaction, (Active) DataGuard, ...

Aber auch mit den eingeschränkten Möglichkeiten einer Standard Edition lassen sich garantierte Wiederanlaufzeiten von wenigen Minuten erreichen. Auch der mögliche Datenverlust lässt sich auf einen Zeitraum von 5, 10 oder 15 Minuten begrenzen.

Wie muss die Datenbank für Datensicherheit und Verfügbarkeit aufgebaut sein?

Für eine möglichst gute Datensicherheit und Verfügbarkeit müssen einige Voraussetzungen gegeben sein.

1. Die Datenbank läuft im Archivelog-Modus

Ohne Archivelog-Modus besteht keine Möglichkeit, die Datenbank auf jeden beliebigen Zeitpunkt zu recovern (Point-in-Time Recovery). Und Ausreden in der Art „Ich habe keinen Platz mehr auf der Storage“ oder „beim nächtlichen Datenimport fallen 25GB an Logfiles an, da blieb die Datenbank immer stehen“ sind sträflich. Es handelt sich schließlich um eine Unternehmensdatenbank und nicht die private DVD-Verwaltung.

2. Die Datenbank wird über RMAN gesichert

RMAN ist und bleibt DAS Verfahren, um eine Oracle Datenbank zu sichern. Nur damit kann die Datenbank jederzeit zuverlässig zu jedem beliebigen Zeitpunkt wiederhergestellt werden. Sie benötigen auch keine zusätzlichen Backup-Agenten, um die Datenbank zu sichern, ganz im Gegenteil.

Ebenfalls sollte die Datenbank nicht über CloudControl oder Enterprise Manager DB Console oder einen Scheduler-Job gesichert werden, auch wenn dies eigentlich elegante Wege wären. Der Grund ist einfach: wenn diese nicht laufen, wird keine Sicherung erstellt und es existiert kein Prozess, der eine Warnmeldung verschicken könnte.
Daher ist eine triviale Sicherung über einen Batch-Job mit Skript und Email-Benachrichtigung die zuverlässigste Methode, um Sicherungsprobleme sicher zu erkennen.

3. Nutzen Sie die Möglichkeit der Imagecopy

Ein vollkommen missachtetes Feature des RMAN ist die Möglichkeit, eine Imagecopy der Datenbank zu erstellen und diese inkrementell, z.B. jede Nacht, weiter zu pflegen.

Im Oracle Handbuch ist leider sehr schlecht erklärt, warum eine Imagecopy nützlich sein kann. Es geht primär nicht darum, aus einer Imagecopy schnell wieder eine Datenbank wiederherstellen zu können. Man kann die Datenbank auch einfach innerhalb von Sekunden auf die Imagecopy umschalten und, nachdem diese auf den letzten Stand recovered wurde, mit dieser Imagecopy direkt weiterarbeiten.

Festplattenlayout für den Server

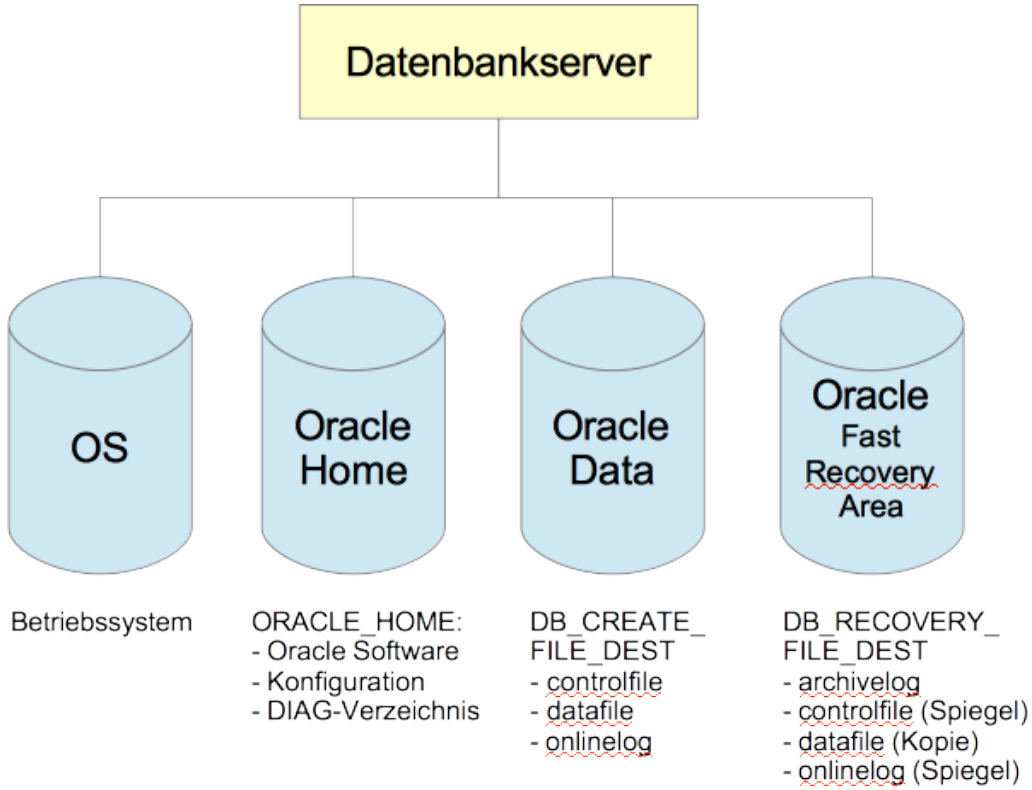

Abb. 1: Festplattenlayout Server

Das Betriebssystem sollte in einem separaten Bereich liegen, ebenso das Oracle Home mit dem DIAG-Verzeichnis. Sollte die Datenbank größere Mengen von Coredumps erzeugen, so läuft zwar das Oracle Home voll, die betrifft dann jedoch nicht das Betriebssystem und nicht den Daten- oder Fast Recovery- Bereich der Datenbank. Die Datenbank wird also weiterarbeiten.

Im Datenbereich befinden sich die Datenfiles, ein Satz Online-Redologs und eine Kopie des Controlfiles.

In der Fast Recovery Area befinden sich ebenfalls ein Satz Online-Redologs, eine Kopie des Controlfiles und die Archivelogs. Zusätzlich liegt hier die Imagecopy der Datenbank mit dem Stand der letzten Nacht.
Aus dieser Imagecopy kann mit Hilfe der Archivelogs, der Online-Redologs und des Controlfiles,

welche sich ebenfalls auf dieser Platte befinden, innerhalb von Minuten wieder eine lauffähige Datenbank erstellt werden.

Die reguläre RMAN-Sicherung sollte sich übrigens überhaupt nicht auf diesem Server befinden sondern auf einem separaten Backupserver, welcher auch unabhängig von einem eventuell verwendeten Storagesystem arbeitet.

Ausfallszenarien

1. Ausfall des Oracle Datenbereichs

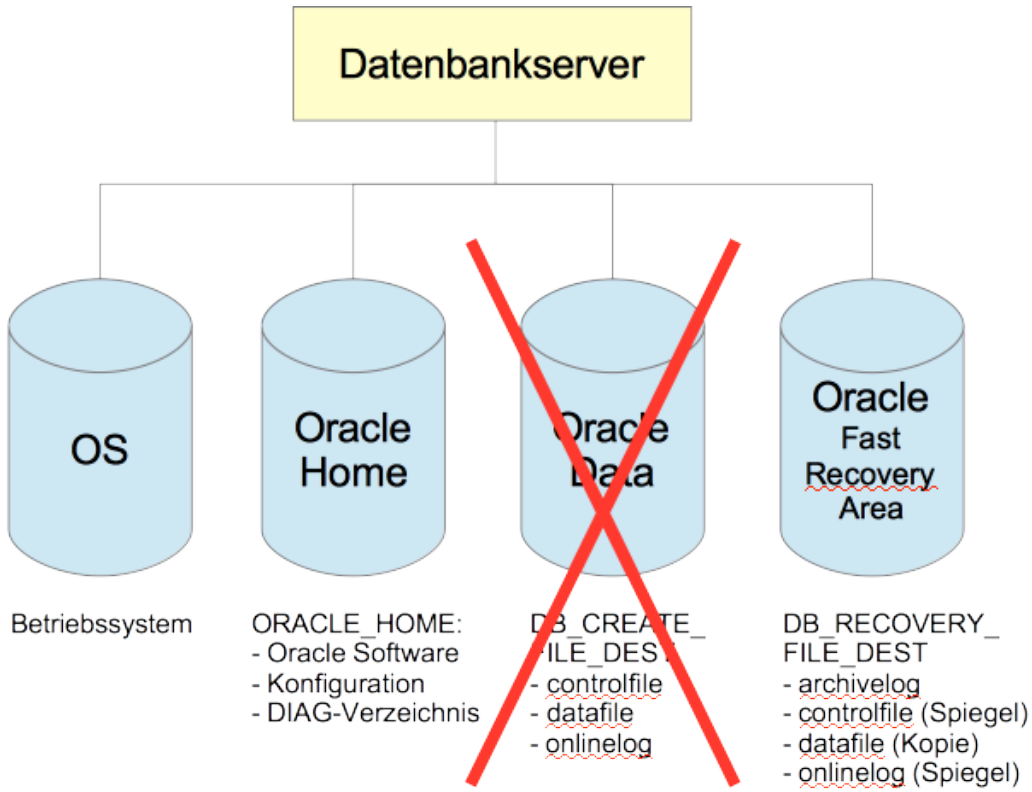

Abb. 2: Ausfall des Oracle Datenbereichs

Notwendige Maßnahmen zum Wiederanlauf:
- control_files im Spfile korrigieren
- Datenbank in den Mount-Status bringen
- Jeweils ein Member aus den Redologgruppen entfernen
- Datenbank auf die Imagecopy umschalten
- Datenbank recovern
- Datenbank öffnen

Ausfallzeit: ca. 15 Minuten
Datenverlust: Keiner

Danach:
- Reparatur des Datenbereichs
- Datenbank im Datenbereich über Imagecopy wiederherstellen

- Bei nächster Gelegenheit Reparatur fertig stellen und wieder auf den Original Datenbereich zurück switchen.

2. Ausfall der Fast Recovery Area

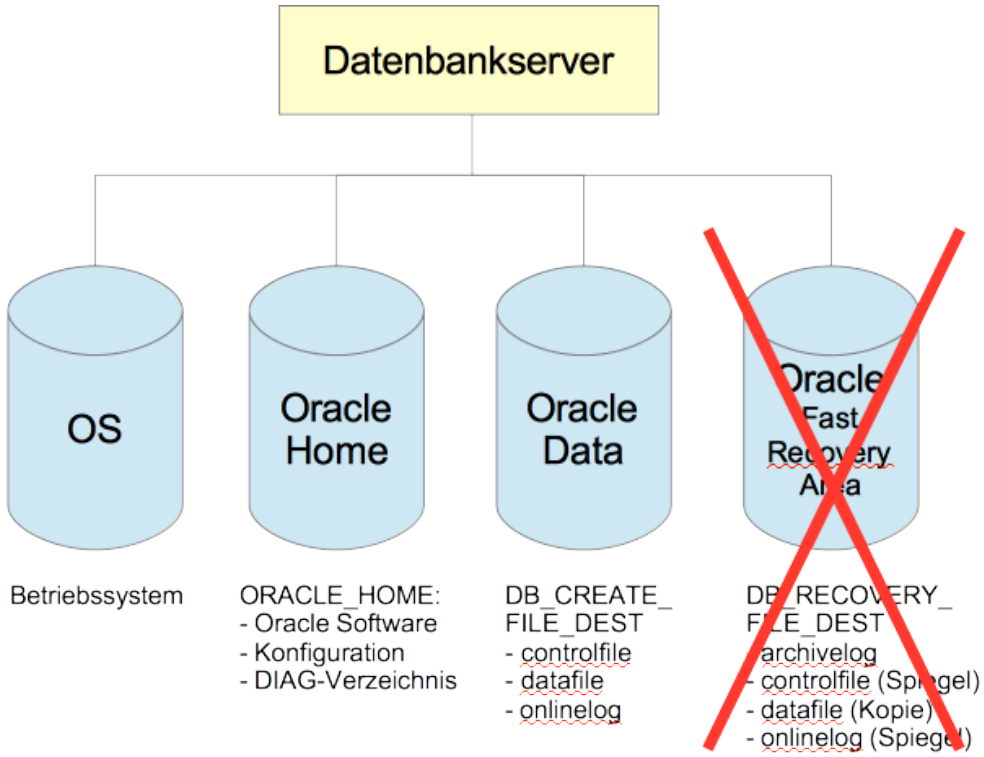

Abb. 3: Ausfall der Fast Recovery Area

Notwendige Maßnahmen zum Wiederanlauf:
- control_files im Spfile korrigieren
- Datenbank in den Mount-Status bringen
- Jeweils ein Member aus den Redologgruppen entfernen
- Fast Recoery Area temporär auf eine andere Platte legen
- Datenbank öffnen

Ausfallzeit: ca. 15 Minuten
Datenverlust: Keiner

Danach:
- Reparatur der Fast Recovery Area
- Fast Recoery Area auf den Originalbereich zurückstellen
- Imagecopy wieder erzeugen
- Bei nächster Gelegenheit Reparatur fertig stellen (Controlfile, Redolog-Member)

3. Ausfall OS-Platte oder Oracle Home

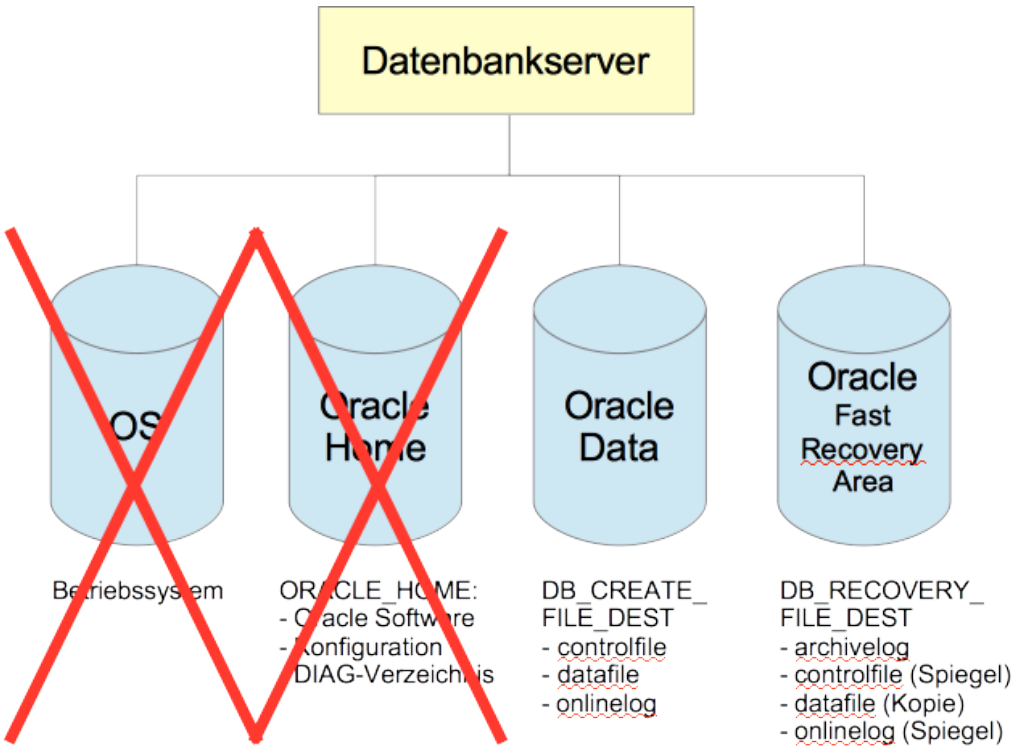

Abb. 3: Ausfall OS-Platte oder Oracle Home

Notwendige Maßnahmen zum Wiederanlauf
- Es sind noch alle Daten vorhanden
- Entweder das Betriebssystem / Oracle Home auf einem anderen Server wieder herstellen oder den Testserver verwenden.

Ausfallzeit: > 1 Stunde
Datenverlust: Keiner

In diesem Fall ist mit einem längeren Ausfall zu rechnen.
Daher muss insbesondere für dieses Szenario ein Plan erstellt werden, wie mit diesem Problem umgegangen wird.

Ergänzung: die klassische Standby-Datenbank

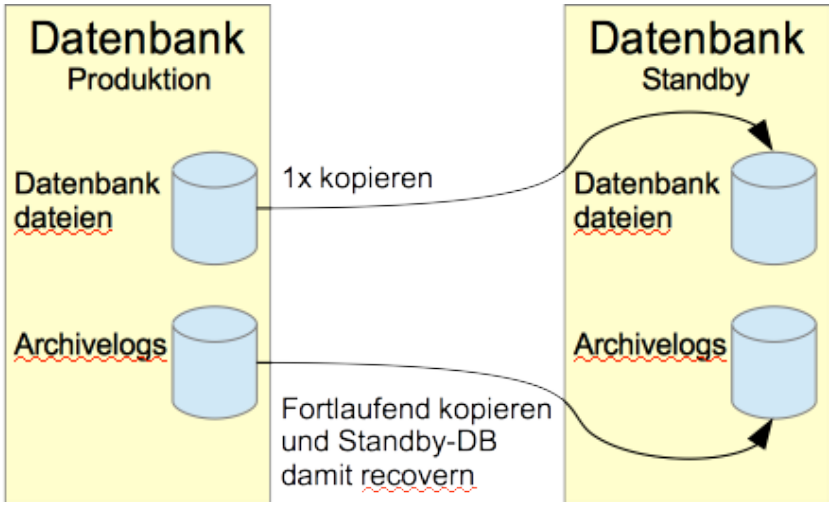

Abb. 4: Klassische Standby-Datenbank

Auf einem zweiten Server wird eine Kopie der Produktionsdatenbank erstellt. Diese Datenbankkopie wird in den Mount-Status gebracht und permanent mit den von der Produktionsdatenbank erzeugten Archivelogs recovered.

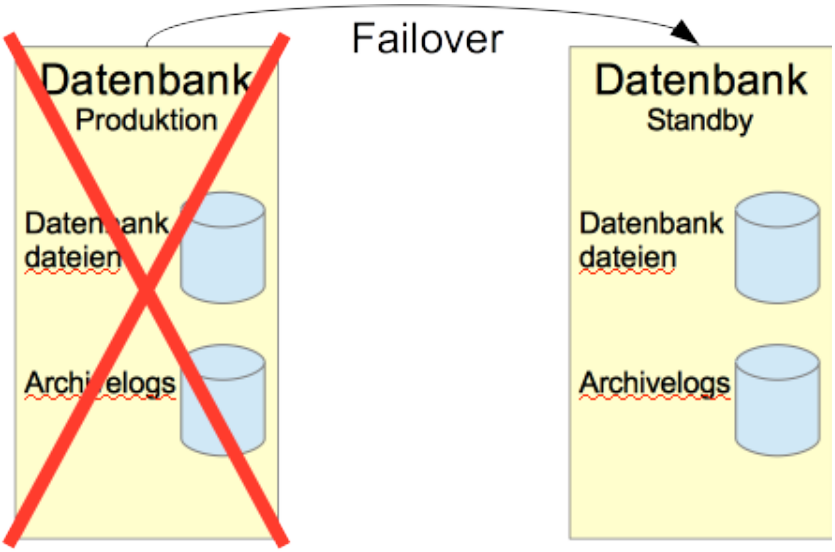

Abb. 5: Ausfall des Produktionsservers

Im Fall, dass der Produktionsserver verloren geht, kann ein Failover auf die Standby-Datenbank erfolgen. Sollte sich von der Produktionsdatenbank nicht mehr das letzte Online-Redolog retten lassen, so muss in diesem Fall mit einem Datenverlust von 5 bis 15 Minuten gerechnet werden (je nach Einstellung des archive_lag_target).

Ausfallzeit: ca. 30 Minuten
Datenverlust: 5 – 15 Minuten

Last Line of Defense: Restore der RMAN-Sicherung

Erst wenn alle anderen Maßnahmen fehlgeschlagen sind und sowohl der primäre Datenbankserver wie auch der Standby-Server verloren gegangen sind muss auf die „klassische“ RMAN-Sicherung zurückgegriffen werden. Wie Sie inzwischen sicherlich erahnen können muss bis dahin jedoch richtig viel in Ihrem Rechenzentrum kaputt gegangen sein. Umso wichtiger, dass Ihre RMAN-Sicherung außerhalb dieses Rechenzentrums gelagert wurde – ansonsten ist sie wahrscheinlich ebenfalls verloren. Dies muss bei einem Notfallkonzept unbedingt beachtet werden.

Und erst, wenn Sie an diesem Punkt angekommen sind, haben Sie ein wirkliches Problem. Und Ihr Notfallkonzept sollte so aufgebaut sein, dass Sie diesen Punkt niemals erreichen werden.

Zusätzliche Sicherungen unabhängig von RMAN

1. Regelmäßiger Export der Datenbank

Das können Sie gerne machen, sofern Sie den Platz und ein passendes Zeitfenster für den Export haben. Aus einem Export können Sie sehr viel eleganter als aus einer RMAN-Sicherung einzelne Tabellen oder auch Packages wiederherstellen. Hierfür eignet sich ein Export hervorragend. Nicht jedoch als alleinige Sicherungsstrategie für die Datenbank.

2. Snapshot des Datenbankservers über Storage-Mechanismen

Sehr gut geeignet, um schnell wieder die Betriebssystem- oder Oracle Home Festplatte herstellen zu können (siehe Ausfallszenario 3). Für die Datenbanksicherung jedoch nur bedingt geeignet – Sie müssen auf jeden Fall mit einem Datenverlust rechnen.

3. Backup der Datenbank über das Betriebssystem

Damit gemeint ist die Sicherung einer heruntergefahrenen Datenbank mit Betriebssystemmitteln (TAR- oder Robocopy oder ähnliches). Dieses Verfahren ist definitiv veraltet, der Datenverlust ist immanent und nicht notwendig.
Bitte verwenden Sie kein solches Verfahren mehr.

Kontaktadresse:

Jochen Kutscheruk

merlin.zwo InfoDesign GmbH & Co. KG

Taglöhnergärten 43

D-76228 Karlsruhe

Telefon: +49 (0) 7052-50898-40

Fax: +49 (0) 7052-50898-58

E-Mail jochen.kutscheruk@merlin-zwo.de

Internet: www.merlin-zwo.de