

Datensicherheit und Verfügbarkeit mit der Oracle Standard Edition

Jochen Kutscheruk
Oracle Certified Master
merlin.zwo InfoDesign GmbH & Co. KG
76228 Karlsruhe



Spitzenleistung heißt, sich auf seine Stärken zu konzentrieren.



merlin.zwo

Wir machen Oracle - nur Oracle.
Aus gutem Grund.

www.merlin-zwo.de



Inhalt

- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- Datensicherheit und Verfügbarkeit
- Die Grenzen der Standard Edition
- Bitte nicht so!
- Exemplarische Konfiguration
- Ausfallszenarien
- Zusammenfassung



Datenschutz im Sinne des BDSG

- Mit der Standard Edition ist kein Datenschutz / Datensicherheit im Sinne des BDSG möglich!
- Keine Möglichkeit, Daten nur bestimmten Personen zugänglich zu machen
 - nur bestimmte Zeilen oder Spalten einer Tabelle
 - nur verschleierte Daten anzeigen
 - Datenbankinhalte verschlüsseln
 - Zugriff nur über 4-Augen-Prinzip
- Auch die Überwachung des reinen Zugriffs auf die Daten (select) ist nur mit der Enterprise Edition möglich (FGA).



Inhalt

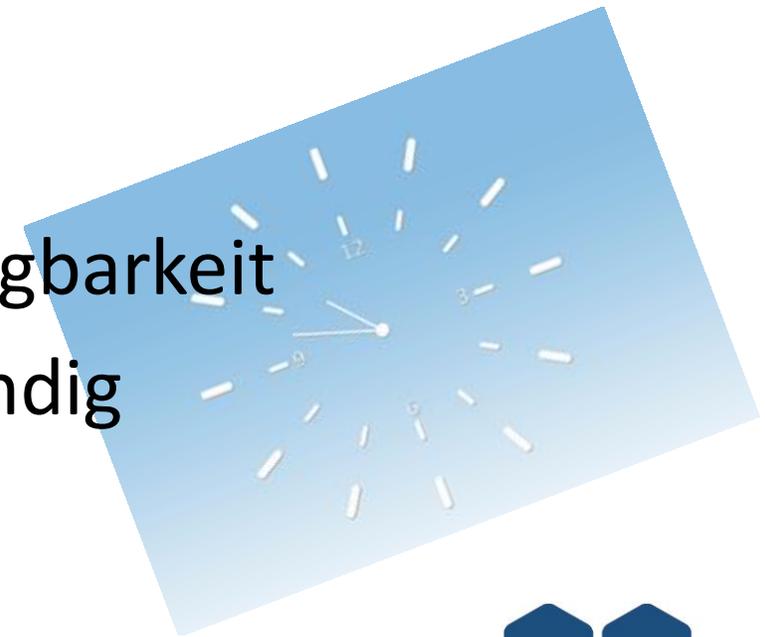
- Vorab: Datenschutz im Sinne des BDSG
- **Ausgangssituation**
- Datensicherheit und Verfügbarkeit
- Die Grenzen der Standard Edition
- Bitte nicht so!
- Exemplarische Konfiguration
- Ausfallszenarien
- Zusammenfassung



Ausgangssituation

Die zentrale Datenbank ist das Herzstück des Unternehmens

- Die Anforderungen an die Datenbank haben sich in den letzten 10 – 15 Jahren drastisch gewandelt
- Konsolidierung an einem Standort
- Alle Werke weltweit abhängig von der Verfügbarkeit
- Verfügbarkeit (fast) rund um die Uhr notwendig
- Ohne Datenbank steht das Unternehmen



Ausgangssituation

Die Sicherungs- und Wiederherstellungsverfahren blieben unverändert

- „Cold Backup“ der Datenbank jede Nacht
- Noarchivelogmodus („kein Platz“ oder „kostet Performance“)
- Sicherung per
 - Filesystem Backup (TAR u.ä.)
 - EXP (die Regel)
 - EXPDP (sehr fortschrittlich)
- „Das Verfahren ist seit 20 Jahren bewährt“
- Im Trend: Snapshots (VM oder Storage)



- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- **Datensicherheit und Verfügbarkeit**
- Die Grenzen der Standard Edition
- Bitte nicht so!
- Exemplarische Konfiguration
- Ausfallszenarien
- Zusammenfassung



Datensicherheit und Verfügbarkeit

Datensicherheit und Verfügbarkeit werden gerne verwechselt

- RAC (Real Application Cluster) = Verfügbarkeit
- DataGuard = Datensicherheit

Ist das die ganze Wahrheit?



Datensicherheit und Verfügbarkeit

RAC schützt **unterbrechungsfrei** vor physischen Fehlern der Server, die Datenbank bleibt erreichbar.

- RAC schützt jedoch nicht vor logischen Fehlern.
- Über 85% der Fehler sind jedoch logische Fehler!
- Eine physisch erreichbare, jedoch logisch korrupte Datenbank, ist nicht verfügbar!



Datensicherheit und Verfügbarkeit

DataGuard schützt vor Datenverlust, jedoch nicht unterbrechungsfrei.

- Physische Fehler bedingen eine kurze Unterbrechung.
- DataGuard schützt auch vor logischen Fehlern.
- **DataGuard gibt es nur in der Enterprise Edition.**



Datensicherheit und Verfügbarkeit

Nur den Schutz vor Unterbrechungen und die Datensicherheit zu betrachten genügt nicht.

Mindestens genauso wichtig sind:

- **Mean time between failure (MTBF)**
- **Mean time to recover (MTTR)**



Inhalt

- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- Datensicherheit und Verfügbarkeit
- **Die Grenzen der Standard Edition**
- Bitte nicht so!
- Exemplarische Konfiguration
- Ausfallszenarien
- Zusammenfassung



Die Grenzen der Standard Edition

Die Kombination von Real Application Cluster und DataGuard ist das Optimum für Datensicherheit und Verfügbarkeit.

- RAC ist Bestandteil der Standard Edition 2 (maximal 2 Server)
- RAC ist eine Zusatzoption für die Enterprise Edition
- DataGuard ist ausschließlich Bestandteil der Enterprise Edition

In der Standard Edition ist kein DataGuard-Mechanismus verfügbar.

Daher muss bei der SE in letzter Konsequenz mit einem Datenverlust gerechnet werden!



Inhalt

- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- Datensicherheit und Verfügbarkeit
- Die Grenzen der Standard Edition
- **Bitte nicht so!**
- Exemplarische Konfiguration
- Ausfallszenarien
- Zusammenfassung



Bitte nicht so!

Original-Zitat eines Softwareherstellers:

„Die Sicherung der Daten kann unterschiedlich erfolgen. Vor dem Einsatz von Archive Logging sollte bedacht werden, dass xxx sehr viele temporäre Daten erzeugt. Diese werden bei Archive Logging ebenfalls Teil des Archive Logs. Insofern sollte Archive Logging nur auf großzügig dimensionierten Systemen eingesetzt werden. Des Weiteren sollte es einen Zuständigen für die Überwachung der Archive Logs geben (sowie eine Urlaubsvertretung!).“

Bei vielen Kunden wird täglich ein ganz normaler Export per Datapump als Backuplösung eingesetzt. In Hinblick auf Nutzen zu Aufwand und verbleibendem Risiko ist dieser Ansatz durchaus akzeptabel.“

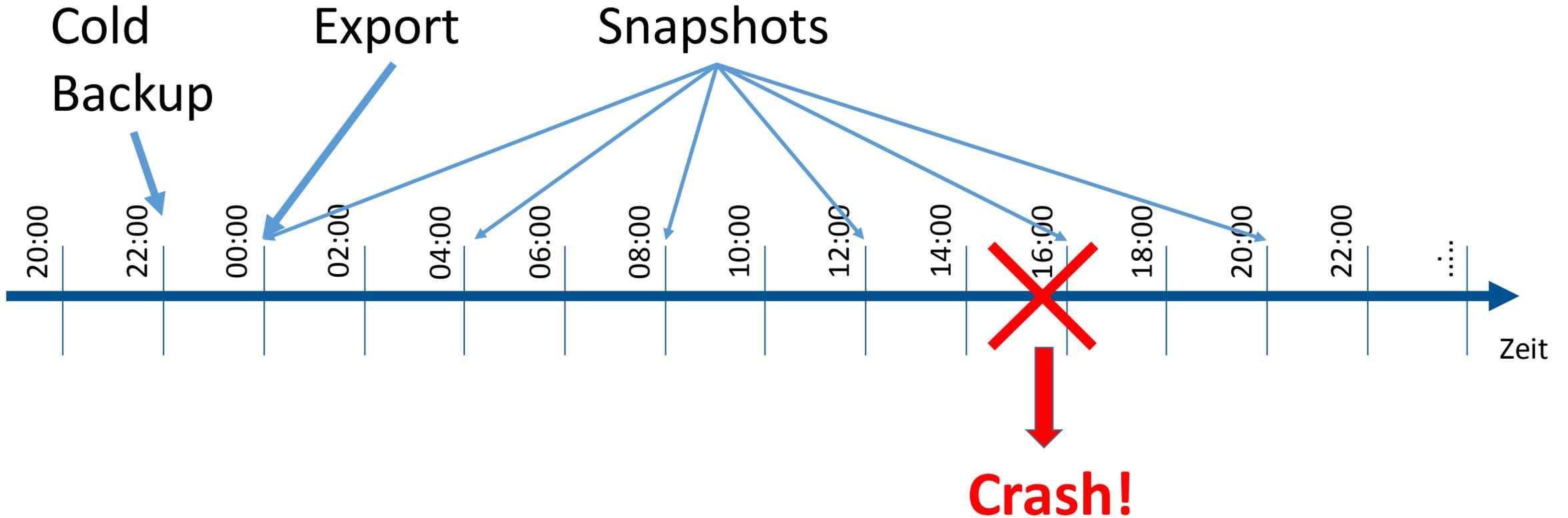


Bitte nicht so!

- Cold Backup der Datenbank jede Nacht
- Noarchivelog-Modus
- EXP oder EXPDP als Sicherungsstrategie
- VM oder Storage Snapshots als Sicherungsstrategie



Bitte nicht so!



Inhalt

- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- Datensicherheit und Verfügbarkeit
- Die Grenzen der Standard Edition
- Bitte nicht so!
- **Exemplarische Konfiguration**
- Ausfallszenarien
- Zusammenfassung



Warum schützt DataGuard vor Datenverlust?



Primärdatenbank

Standby



Alternativ: Manuelle Standby-Datenbank



**Datenverlust
garantiert!**



Exemplarische Konfiguration

- Die Datenbanken laufen im Archivelog-Modus. Punkt!
- Trennen Sie Data Area und Fast Recovery Area
 - Data Area und Fast Recovery Area auf zwei getrennten Storages
 - Storages stehen in getrennten Brandabschnitten und nicht im Keller
 - Controlfiles und Online-Redologs werden von der Datenbank (nicht der Storage!) in der Data Area und Fast Recovery Area gespiegelt
 - Archivelogs liegen in der Fast Recovery Area
 - Halten Sie in der Fast Recovery Area Platz für die Imagecopy der Datenbank bereit
 - Verwenden Sie Oracle Managed Files



Exemplarische Konfiguration

- Für das Datenbank-Backup wird RMAN verwendet
- Die RMAN-Backups werden unabhängig von den beiden Storages (für Data und FRA) abgelegt
- Verwenden Sie nicht Cloud (Grid) Control für das Ausführen der RMAN-Backups
- Verwenden Sie keine Oracle Backup Agents Ihres Sicherungssoftware-Herstellers
- Starten und überwachen Sie die RMAN-Backups über Cron oder Windows Scheduler



Exemplarische Konfiguration



Primär

Controlfile
Online Redologs
Datenfiles

Storage 1



Standby

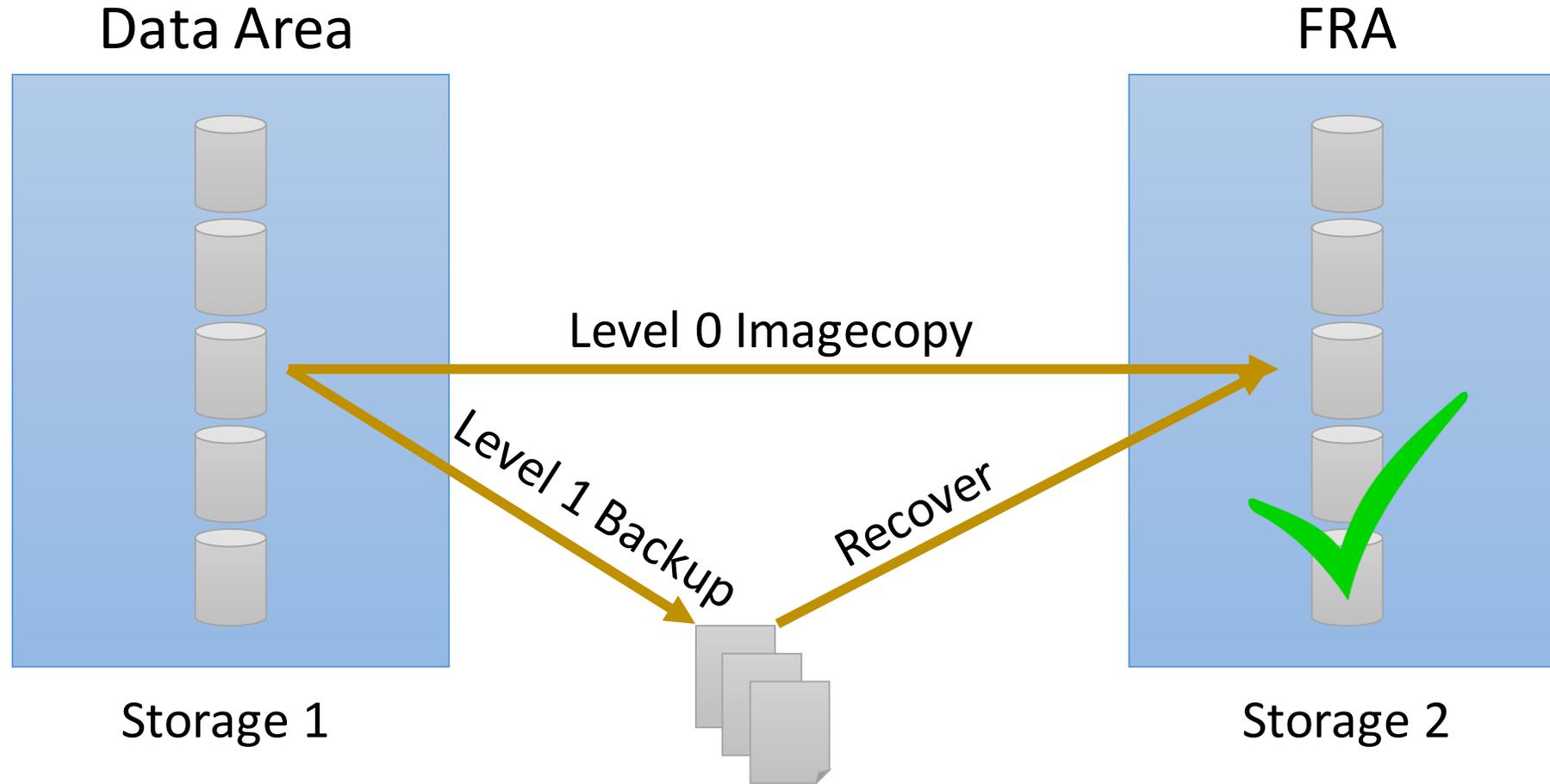
Controlfile
Online Redologs
Archivelogs
Imagecopy

Brandabschnitt

Storage 2



Exemplarische Konfiguration



Exemplarische Konfiguration

Erstellen und pflegen einer Imagecopy mit RMAN:

```
RUN {  
  BACKUP INCREMENTAL LEVEL 1 FOR RECOVER OF  
  COPY WITH TAG `imagecopy` DATABASE;  
  
  RECOVER COPY OF DATABASE WITH TAG  
  `imagecopy`;  
}
```

Die Imagecopy wird in der Fast Recovery Area angelegt.

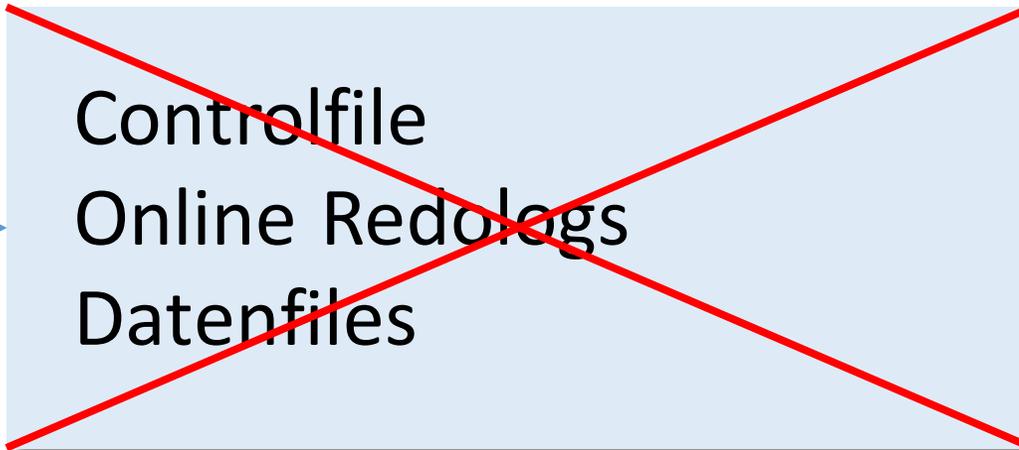


Inhalt

- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- Datensicherheit und Verfügbarkeit
- Die Grenzen der Standard Edition
- Bitte nicht so!
- Exemplarische Konfiguration
- **Ausfallszenarien**
- Zusammenfassung



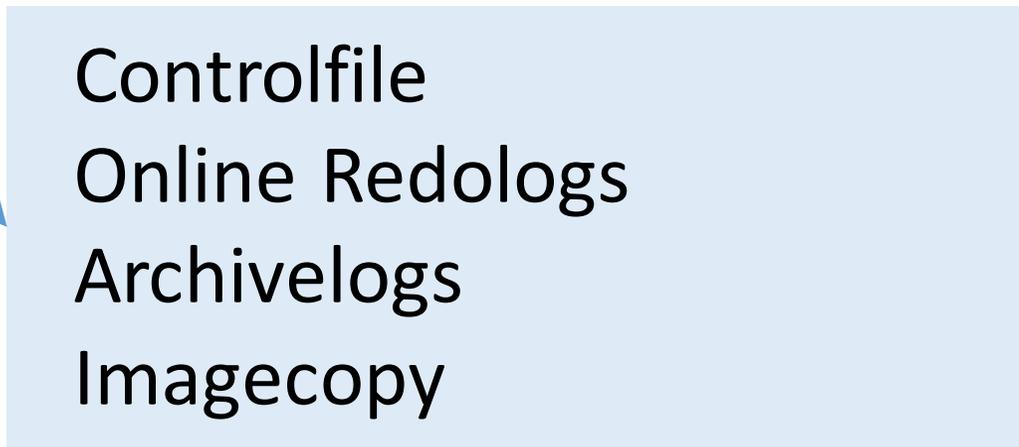
Ausfallszenario (1)



Storage 1



Brandabschnitt



Storage 2



Ausfallszenario (1)

```
SQL> startup nomount
```

```
SQL> alter system set control_files='ctrl_auf_fra';
```

```
RMAN> alter database mount;
```

```
RMAN> switch database to copy;
```

```
RMAN> recover database;
```

```
RMAN> alter database open;
```

Datenverlust: Keiner!

Ausfallzeit: 15 Minuten



Ausfallszenario (2)



Controlfile
Online Redologs
Datenfiles

Storage 1



Brandabschnitt



~~Controlfile
Online Redologs
Archivelogs
Imagecopy~~

Storage 2



Ausfallszenario (1)

```
SQL> startup nomount
```

```
SQL> alter system set control_files='ctrl_auf_data';
```

```
SQL> alter database mount;
```

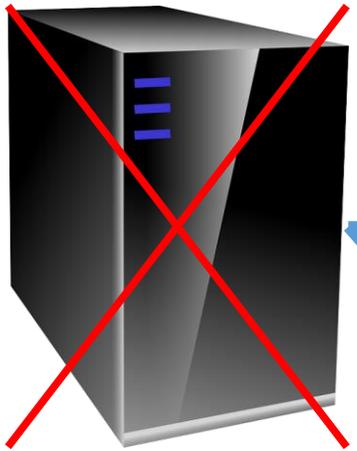
```
SQL> alter database open;
```

Datenverlust: Keiner!

Ausfallzeit: 15 Minuten



Ausfallszenario (3)



Controlfile
Online Redologs
Datenfiles

Storage 1



Brandabschnitt



Controlfile
Online Redologs
Archivelogs
Imagecopy

Storage 2



Ausfallszenario (3)

- Hardware umbauen
- Ersatzserver starten

Datenverlust: Keiner!

Ausfallzeit: 30 Minuten



Inhalt

- Vorab: Datenschutz im Sinne des BDSG
- Ausgangssituation
- Datensicherheit und Verfügbarkeit
- Die Grenzen der Standard Edition
- Bitte nicht so!
- Exemplarische Konfiguration
- Ausfallszenarien
- **Zusammenfassung**



Zusammenfassung

- Datenbank im Archivelog-Modus
- Datenbanksicherung immer über RMAN
 - Verwenden Sie keine Sicherungsagenten
 - Sichern Sie auf einen unabhängigen Sicherungsserver
- Nutzen Sie die Möglichkeit der Imagecopy
 - Dafür wird der doppelte Speicherplatz benötigt!
- Nutzen Sie zwei Storages in verschiedenen Brandabschnitten
 - Stellen Sie in den zweiten Brandabschnitt einen Ersatzserver



Zusammenfassung

- Die Ausfallzeit wird minimiert
- Deutliche Verbesserung der Datensicherheit
- Minimale Mehrkosten (Plattenplatz, evtl. Storage)
- Wiederherstellung ohne Restore
- Klassische Standby ist eine gute Ergänzung
- **Backup ist die „Last line of defense“ und sollte eigentlich nie benötigt werden!**



Zusammenfassung

Die ersten drei wichtigsten Dinge:

Testen, testen, testen

Die zweiten drei wichtigsten Dinge:

Üben, üben, üben



Noch Fragen?



Jochen Kutscheruk
merlin.zwo InfoDesign GmbH & Co. KG

Taglöhnergärten 43
D-76228 Karlsruhe

jochen.kutscheruk@merlin-zwo.de
www.merlin-zwo.de

