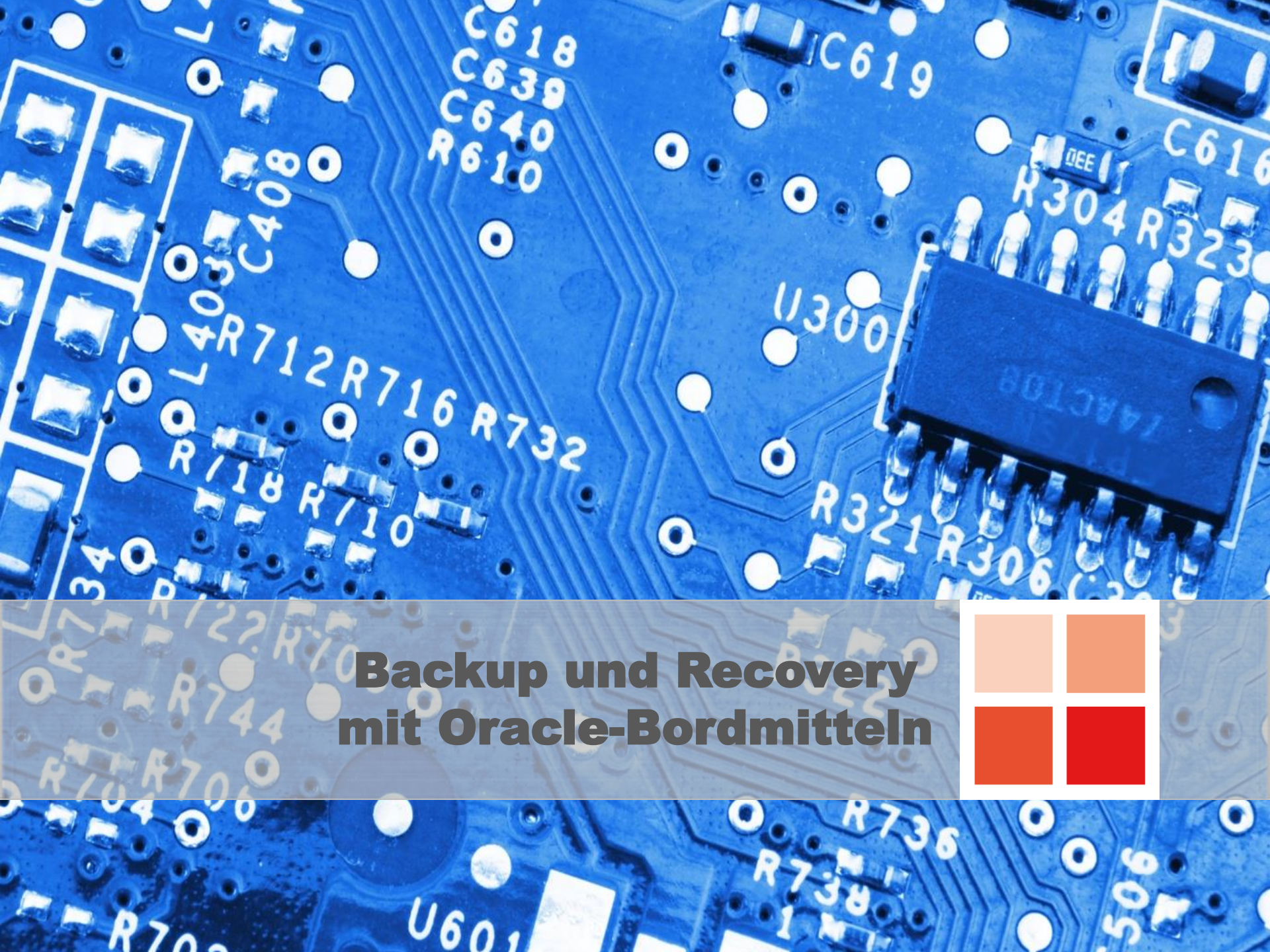


Backup und Recovery mit Oracle-Bordmitteln

Strategische Beratung

Prozesse
DB Struktur
Zukunfts-
sicherheit

Wartung & Support

Wartung
Aktualisierung
Administration
Support

essential BYTES

Oracle Lizenzmanagement

Analyse
Konsolidierung
Management

Projektmanagement

Planung
Koordination
Ausführung
Test & Freigabe

Implementierung

DB Struktur
Dienste
Sicherheit
Verfügbarkeit

Kontakt

Essential Bytes GmbH & Co. KG

Markus Schmidt

In der Spöck 12

77656 Offenburg

mschmidt@essential-bytes.de

http://www.essential-bytes.de

Backup und Recovery

Konzepte, Prozeduren und Strategien um die Datenbank

gegen Datenverlust aufgrund Medien- oder Benutzerfehlern zu schützen

und die Wiederherstellbarkeit im Fehlerfall zu gewährleisten.

Data Protection

- Backup ist Kopie der Daten für die Wiederherstellung von Daten
  - Physikalisches Backup **Essentiell!**
    - „Bitkopie“
    - Datafiles, Controlfiles, Archivelogs, …
  - Logisches Backup **Ergänzend**
    - Logische Kopie
    - Tabellen, Stored Procedures, …

Data Preservation

- Zusammenhang mit Data Protection,
  aber anderer Zweck
- Archival Backup
- Vorhalten von vergangenen Zuständen:
  Stand der DB am Ende des Geschäftsjahres, …
- Meist kein Speicher für Onlinezugriff

Data Transfer

- Backup für die Übertragung der Datenbank an einen anderen Ort
- Meist Export/Import
- Ergänzung von Recoveryszenarien

Fehler

- Medienfehler
  - Physikalisches Problem:
    Lese/Schreibfehler bei Datenbankdateien
  - Desaster: Ausfall von größeren IT-Strukturen
    Bei Datenbank prinzipiell reduzierbar auf Medienfehler

- Benutzerfehler
  - Hauptgrund für Ausfälle!
  - Fälschliches Verändern oder Löschen von Daten, Tabellen

Oracle Backup- und Recovery-Möglichkeiten

- Recovery Manager RMAN
  - Vielfältige Einsatzszenarien
  - Voll in die DB integriert, CLI oder Enterprise Manager
  - Empfohlenes Werkzeug

- User-managed Backup and Recovery
  - Meist skriptbasiert oder Drittanbieter-Tools
  - Meist für bestimmte Szenarien ausgelegt
  - Meist nicht voll integriert

Archivelogs

- Beinhalten alte Redologs
- Transaktionsinformation
- Wichtige Grundlage für Recovery
- Aus Platzgründen nicht einfach „bereinigen“ !!!
- Datenbanken immer im Archivelog-Mode betreiben
  - Kaum sinnvolle Ausnahmen
    nur z.B. bei flüchtigen oder rekonstruierbaren Datenbeständen

Backup & Recovery mit RMAN (Recovery Manager)

- Mit der DB mitgeliefert, keine Zusatzlizenz nötig
- Konsistente **Online** Backups möglich
- Automatisierung: Erkennen der DB/Ctl/Log-Files
- Effiziente Block-Level Backups
- Integritätschecks während Backup und Recovery
- Testmodus
- Synchronisierung Primär/Standby
- DB-Duplizierung möglich
- Mit Fremdsoftware kombinierbar
- Recovery Catalog

RMAN Konfiguration

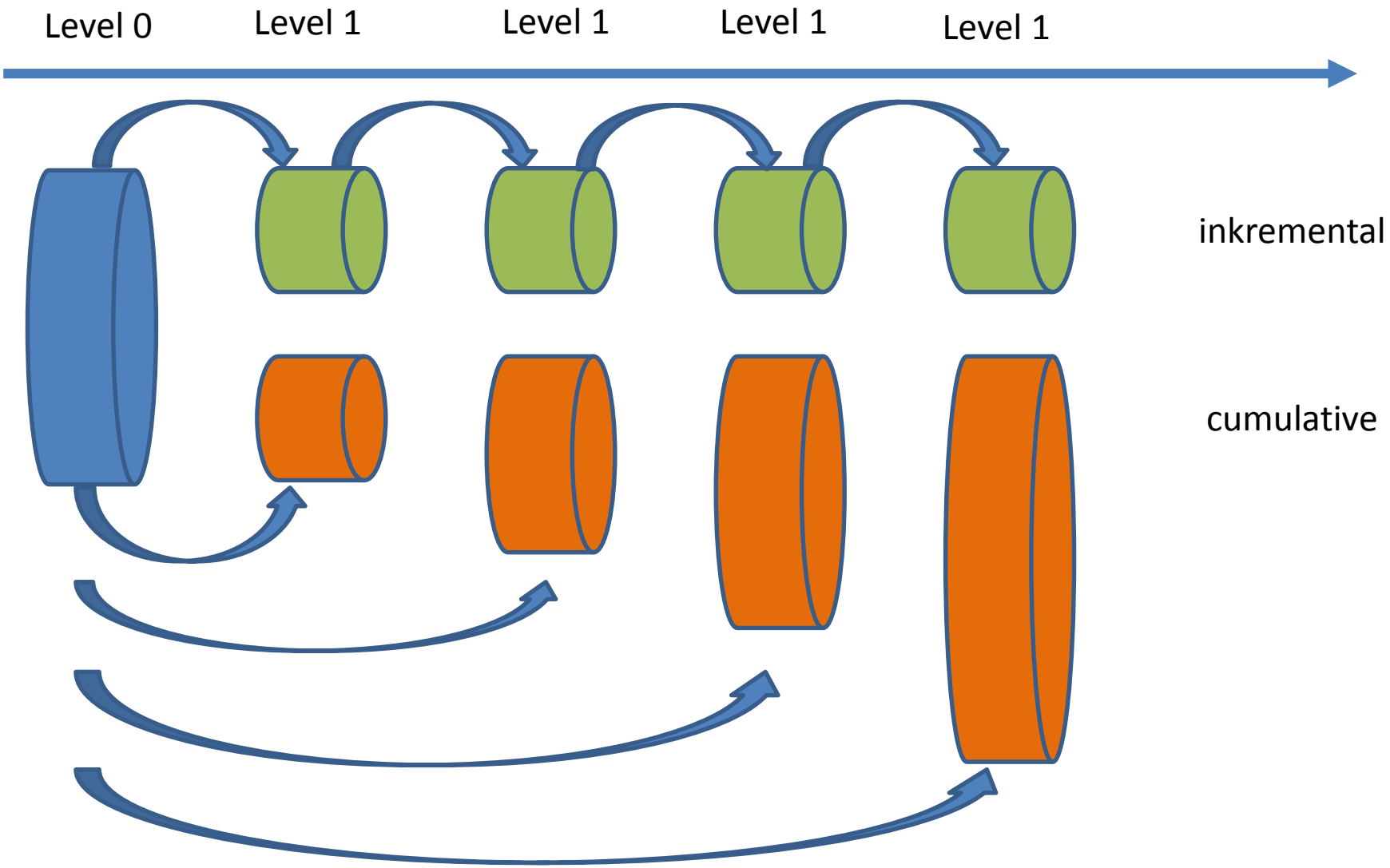
- DB im ARCHIVELOG-Modus !!!
- Faktoren für die Backupfrequenz
  - Recovery Point Objective:
    wie viele Daten dürfen im schlimmsten Fall verloren gehen?
  - Recovery Time Objective:
    wie viel Zeit darf für ein Recovery gebraucht werden?
    Repair Time = Restore Time + Recovery Time
  - Volumen der geänderten Daten
- Backup Retention Policy
  - Anzahl Backups oder Zeitraum
  - Archive-Backups

Konfiguration

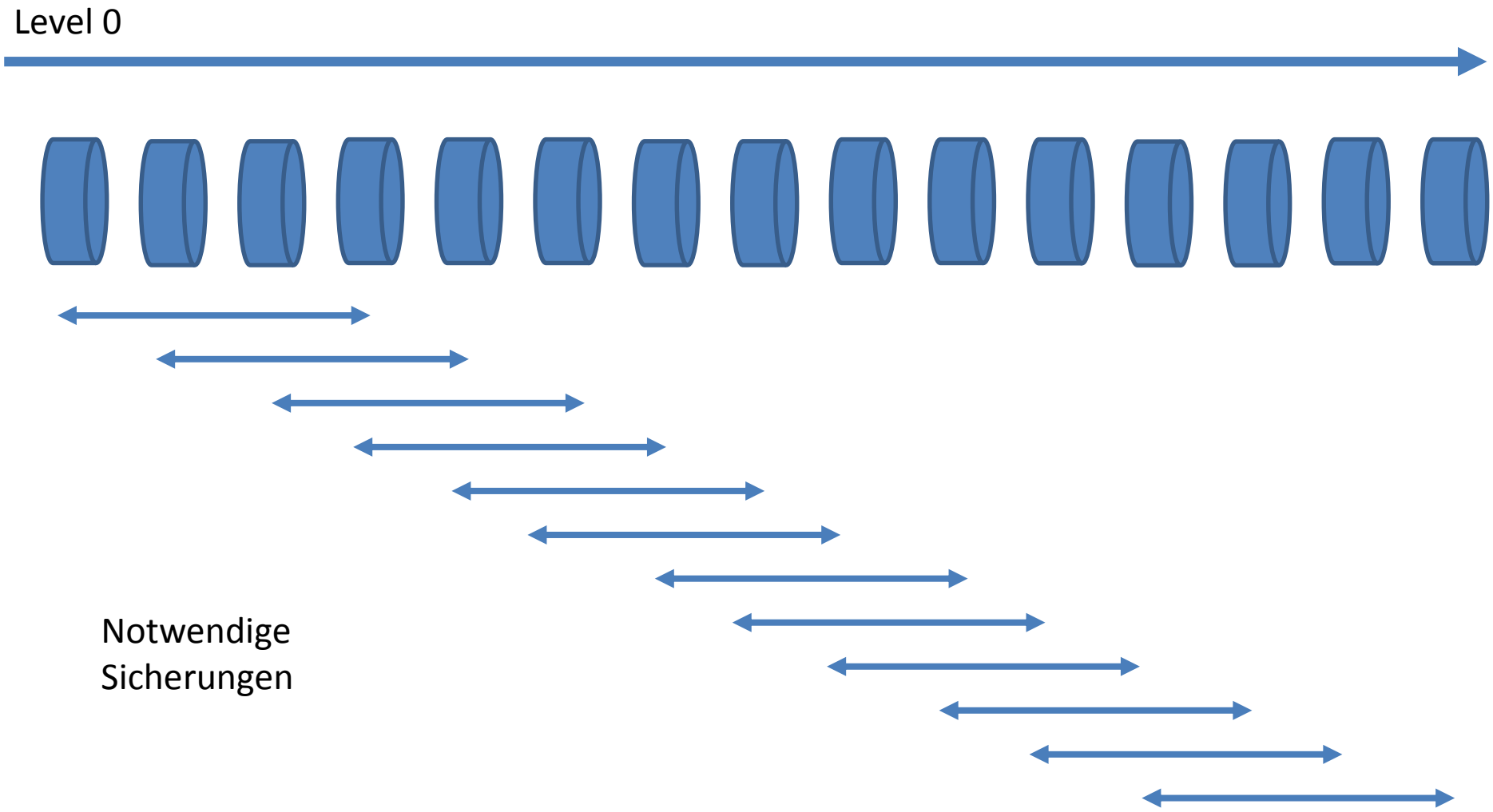
RMAN **show all**

CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF **7** DAYS;
CONFIGURE BACKUP OPTIMIZATION **ON**;
CONFIGURE DEFAULT DEVICE TYPE TO DISK;
CONFIGURE CONTROLFILE AUTOBACKUP **ON**;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/backup/rman/**%F**';
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO **COMPRESSED** BACKUPSET;
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1;
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1;
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/backup/rman/**%d_%U_%t.rman**';
CONFIGURE MAXSETSIZE TO UNLIMITED;
CONFIGURE ENCRYPTION FOR DATABASE OFF;
CONFIGURE ENCRYPTION ALGORITHM 'AES128';
CONFIGURE COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT' OPTIMIZE FOR LOAD TRUE;
CONFIGURE ARCHIVELOG DELETION POLICY TO BACKED UP **2** TIMES TO DISK;
CONFIGURE SNAPSHOT CONTROLFILE NAME TO '/opt/oracle/product/11.2.0.4/dbs/snapcf_mydb.f'; # default

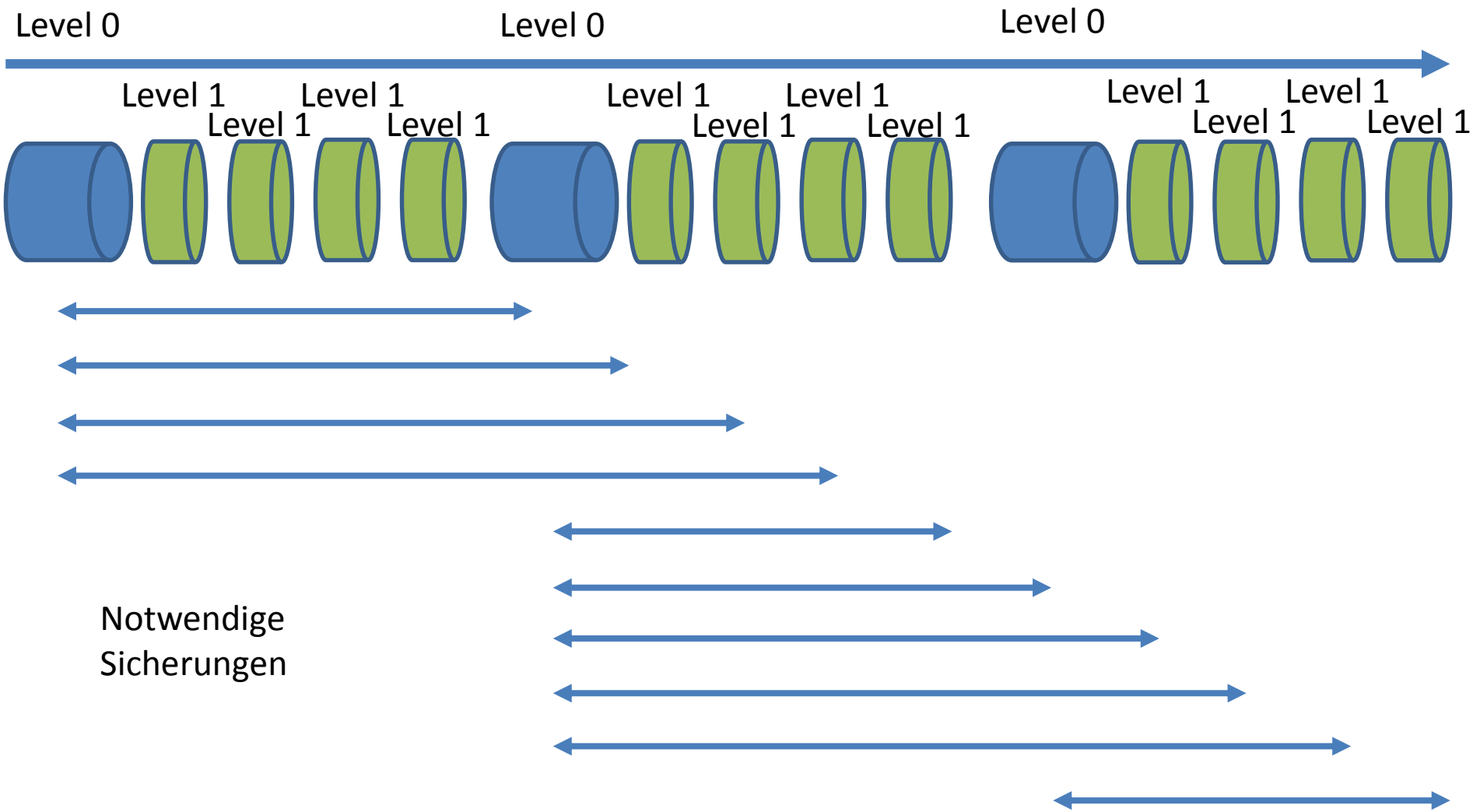
Level 0/1


Level 0
Level 1
Level 1
Level 1
Level 1
inkremental
cumulative

Bsp: Retention Window 3 Tage



Bsp: Retention Window 3 Tage



Recovery Szenarien

- „Zurückholen“ der DB:
  - Einzelne Files
  - Komplett
  - Media-Recovery
- Zurücksetzen auf Zeitpunkt vor Benutzerfehler
  - DBPITR – DB Point in Time Recovery
  - TSPITR – TS Point in Time Recovery
- Reparatur von Blöcken
- Testen von Backups auf anderen Servern
- Aufbau von Testsystemen
- Aufbau von Standbysystemen

RMAN-Empfehlungen

- Catalog verwenden
  - Controlfile kann u.U. nicht alle Informationen halten
  - Kann Metadaten für viele DBs speichern
  - Backup-Offloading bei Standby-Konfigurationen
- Backups in NOCATALOG Mode, dann RESYNC
- Block Change Tracking verwenden (EE)
- Autobackup für Control und SPFile
- Offloading Backup auf Standby-Seite

Best Practices

- Optimierung Recoveryzeit
  - DB Copy / Incremental Backup mit Recovery auf Copy
    -> kein Restore, nur Recovery mit Archivelogs und Switch
- Optimierung Platzbedarf
  - Level 0 Backup
  - Cumulative Incremental Level 1
  - Differential Incremental Level 1
- Optimierung Ressourcenbedarf
  - Einsatz der Recovery Appliance / ZDLA ☺
  - Block Change Tracking

Best Practices

- Read Only TS nutzen wenn möglich
- Komprimierung nur dann, wenn Daten nicht komprimiert
- 12c: Section Size bei Big File Datafiles
- Data Recovery Advisor nutzen
- Regelmäßige Prüfung auf korrupte Daten
- Regelmäßig die Recovery-Prozeduren testen
- Catalog sichern
- Dateisystem-Backup

Scripting

$ rman target / cmdfile CMDFILE

```
# Backup database
backup incremental level 0 database;
backup incremental level 1 database;

# Backup of archivelogs
backup archivelog all;
# Remove unneccessary archivelogs
delete noprompt archivelog all;

# Validate
restore database validate;
restore controlfile validate;
restore spfile validate;
```

User Managed Backups

- Eigene Skripte nötig
  - Bestimmen der Datafiles und Controlfiles
  - Backup-Implementierung
  - Konsistenzsicherung, Metadatenverwaltung

User Managed Backup

- Closed DB Backup
  - SHUTDOWN NORMAL/IMMEDIATE/TRANSACTIONAL
  - Betriebssystemkopie der Datafiles, Controlfiles, SPFile etc.
  - STARTUP
- Backup Offline TS
  - TS offline setzen
    - nicht SYSTEM oder bei TS mit offenen UNDO-Segmenten
    - Vorsicht bei Abhängigkeiten zwischen TS (Bsp: Data/Index)
  - Betriebssystemkopie der OFFLINE Datafiles
  - TS online setzen mit TS-Recovery
  - Redologs sichern

User Managed Backup

- Backup im Backup-Modus
- Schreibvorgänge fließen in die Redologs
- Vorgehen:
  - Datafiles des TS identifizieren (auch mehrere möglich)
  - ALTER TABLESPACE … BEGIN BACKUP
    (warten, bis Befehl abgeschlossen!)
  - Betriebssystemkopie der Datafiles
  - ALTER TABLESPACE … END BACKUP
  - Redologs sichern
- Read-Only TS kann direkt kopiert werden

User Managed Backups

- Archivelogs: einfach kopieren
- Controlfile:
  ALTER DATABASE BACKUP CONTROLFILE TO TRACE | ‚file‘
- SUSPEND / RESUME Feature
  - IO wird angehalten
  - Storage-Kopie
  - IO wird fortgesetzt

Recovery

- Nicht alle Szenarien können recovered werden
- Ohne Archivelogs evtl. nicht wiederherstelltbare Szenarien
- Verfahren: Zurückkopieren der Sicherung und anschließendes Recovery

Export, logisches Backup

- Daten werden in Datei geschrieben
- EXPDP nutzen
- „Recovery“: zurückspielen der Daten in DB
  - Meist Neuaufbau der Grundstruktur (DB) nötig → Zeit, Aufwand!
  - Meist kein aktueller Stand
- Nutzung als Data Transfer- oder Archiving-Verfahren
- Als „letzte Rettung“ bei Komplettverlust und Fehlschlagen der RMAN-Sicherungen
- Niemals als alleinige Strategie einsetzen

Backuptechniken

Feature	RMAN	User-managed	Data Pump
Closed DB Backup	Ja	Ja	Nein
Open DB Backup	Ja	Ja	Ja
Incremental Backups	Ja	Nein	Nein
Corrupt block detection	Ja	Nein	Ja
Automatisches Erkennen von Datafiles etc.	Ja	Nein	-
Backup Catalog	Ja	Nein	Nein
Backup zu Medien-Managern	Ja	Ja	Nein

Flashback

- Diverse Möglichkeiten, um auf alte Daten zuzugreifen
- Einsatz bei Benutzerfehlern
  - Flashback Query
  - Flashback Version Query
  - Flashback Transaction Query
  - Flashback Transaction
  - Flashback Table
  - Flashback Drop
  - Flashback Data Archive
  - Flashback Database

Best Practices - Storage

- ASM für Datenbank verwenden
  - SAME-Konzept, Stripe And Mirror Everything, Redundanzlevel
  - Schutz vor Medien- und SAN-Fehler
  - Hohe Performance, automatisches Balancing
  - Flexibel bei Rekonfiguration
  - Clusterfähig, Oracle Restart möglich
- Storage RAID nutzen
- Multipathing nutzen
- Parameter anpassen:
  FAILGROUP_REPAIR_TIME, DISK_REPAIR_TIME,
  ASM_POWER_LIMIT

essential BYTES

Best Practices - Datenbank

- Archivelog-Mode
  - Force Logging auf DB oder TS-Level
- Redolog:
  - min. 3 Gruppen mit identischer Filegröße auf schnellen Medien
  - in High Redundancy oder mit Multiplexing in Normal Redundancy Diskgroups
- Fast Recovery Area nutzen
  - DB_RECOVERY_FILE_DEST, DB_RECOVERY_FILE_DEST_SIZE
  - Primäre Quelle für Recovery, schnell verfügbare Backups
- Flashback Database nutzen
  - Recovery von logischen Fehlern
  - DB_FLASHBACK_RETENTION_TARGET
- Recovery bei Instanzencrash beschleunigen
  - FAST_START_MTTR_TARGET setzen, Dauer für Recovery in Sekunden
- Datenkorruption vermeiden und erkennen
  - DB_BLOCK_CHECKSUM=FULL, DB_BLOCK_CHECKING=FULL, DB_LOST_WRITE_PROTECT=TYPICAL

Vorüberlegung

- Wie wichtig sind die Daten für den Betrieb?
- In welchem Umfang kann ein Verlust toleriert werden?
- Welche Ausfallzeit kann toleriert werden?
- Was kostet ein Ausfall?
- Können die Daten aus anderen Quellen rekonstruiert werden?
- Mit welchem Aufwand kann rekonstruiert werden?
- Ist Archivierung nötig?
- Volumen, Speicherbedarf

Ansatz: Vermeide Recovery

- Speicherredundanzen nutzen
  - ASM, RAID etc. nutzen um Ausfällen vorzubeugen
- Failoverszenarien in Betracht ziehen
  - Cluster-Systeme
  - Standby-Systeme
  - Storage-Spiegel
- VM-Snapshots
- Nicht darauf verlassen, dass Redundanz ausreicht
  - Logische Fehler sind auch redundant vorhanden
  - Komplettverlust immer noch möglich
- Sinnvoll als Ergänzung, evtl. schnellerer Wiederanlauf

Fazit

- User Managed Backups sind anfällig und aufwändig
  - Konsistenz, Pflege
  - DBA muss Verfahren beherrschen, weil viele Fehlerquellen
- RMAN einfacher und konsistent
- Vollständiger Schutz der DB
- Vielfältige Einsatzmöglichkeiten
- Mit RMAN starten und eigene Skripte erzeugen
  - Backup L0, L1, Arc, Bereinigung, Validation
- Das Testen der Sicherungen nicht vergessen!